Department of Information and Communications Engineering

Secret Key Generation for Ambient Backscatter Communication

Jari Lietzén

Aalto University

DOCTORAL THESES

Aalto University publication series
DOCTORAL THESES 83/2023

Secret Key Generation for Ambient Backscatter Communication

Jari Lietzén

A doctoral thesis completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Electrical Engineering, at a public examination held at the lecture hall TU1 of the school on 30 June 2023 at 12:00.

Aalto University
School of Electrical Engineering
Department of Information and Communications Engineering
Communications Theory

Supervising professor
Professor Olav Tirkkonen, Aalto University, Finland

Thesis advisor
Doctor Roope Vehkalahti, University of Jyväskylä, Finland

Preliminary examiners
Professor Lorenzo Mucchi, Universita degli studi Firenze, Italy
Doctor Eva Lagunas, Université du Luxembourg, Luxembourg

Opponent
Professor Doctor Aarne Mämmelä, VTT Technical Research Centre of Finland, Finland

Aalto University publication series
DOCTORAL THESES 83/2023

ISBN 978-952-64-1296-2 (printed)
ISBN 978-952-64-1297-9 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-64-1297-9

Unigrafia Oy
Helsinki 2023

Finland

NORDIC SWAN ECOLABEL
Printed matter
4041-0619

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

Author
Jari Lietzén

Name of the doctoral thesis
Secret Key Generation for Ambient Backscatter Communication

Publisher School of Electrical Engineering

Unit Department of Information and Communications Engineering

Series Aalto University publication series DOCTORAL THESES 83/2023

Field of research Communications Engineering

Manuscript submitted 18 January 2023 **Date of the defence** 30 June 2023

Permission for public defence granted (date) 24 March 2023 **Language** Finnish

☐ **Monograph** ☒ **Article thesis** ☐ **Essay thesis**

Abstract

The interest in wireless Internet of Things (IoT) devices and Ambient Intelligence has increased significantly in recent years. The security of IoT devices has become a concern, as IoT has made it possible for things and people to interact with each other anytime and any place. Therefore, sufficient protection against active eavesdropping or confusing devices with other users' devices is an essential requirement. Due to the embedded nature of these devices, they are often limited in their computational, communication and power resources. Ambient backscatter communication (AmBC) is seen as a viable solution for resource limited devices, as the wireless nodes are communicating without any active RF components. However, the interference from the ambient transmitter remains a major challenge, as the ambient signal is present at the receiver together with the backscattered signal.

This thesis contributes to secure IoT device communication in an AmBC setting. The contributions are a two-way secret key agreement protocol and a backscatter device design. We developed a novel secret key agreement protocol that uses an advantage distillation method to collect secret key from error corrected parity bits. Our protocol provides complementary performance compared to protocols known in the literature. We have analysed the performance of the key agreement protocol in two different operating scenarios, in a quantum key distribution setting and in a satellite setting. The second contribution is a backscatter device design that introduces polarization conversion between the direct and scattered path signals and exploits that at the dual polarization receiver antenna to substantially decrease the interference from the ambient transmitter. We showed that in an anechoic RF chamber, our proposed set-up could achieve more than 25 dB isolation between the backscattered component, and the ambient component for narrowband signals.

In this thesis, we analyse secret key generation between ambient backscatter devices where the channel between an ambient transmitter and the backscatter devices is used as a source of randomness. We show that even in non-line-of-sight channels the distance from legitimate users to an eavesdropper being larger than a few wavelengths is not alone a sufficient security guarantee. This is in contrast with previous secret key generation methods where the distance is assumed to prevent the eavesdropper from having any information about the key prior to error correction. Our simulations show that a distance based approach is too optimistic, and there is a possibility that the eavesdropper still knows a substantial part of the final key.

A working solution is based on a two-way key agreement protocol, and assuming that the eavesdropper's error rates are k times that of the legitimate users, with $k < 1$. This method gives the legitimate users the freedom to trade off between achievable key rate and the eavesdropper's knowledge of the final key.

Keywords Ambient backscatter, IoT, physical layer security, polarization conversion, secret key generation

ISBN (printed) 978-952-64-1296-2 **ISBN (pdf)** 978-952-64-1297-9

ISSN (printed) 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2023

Pages 181 **urn** http://urn.fi/URN:ISBN:978-952-64-1297-9

Tekijä
Jari Lietzén

Väitöskirjan nimi
Salausavaimen kehittäminen takaisinheijastusta käyttäville laitteille

Julkaisija Sähkötekniikan korkeakoulu

Yksikkö Informaatio- ja tietoliikennetekniikan laitos

Sarja Aalto University publication series DOCTORAL THESES 83/2023

Tutkimusala Tietoliikennetekniikka

Käsikirjoituksen pvm 18.01.2023 **Väitöspäivä** 30.06.2023

Väittelyluvan myöntämispäivä 24.03.2023 **Kieli** Suomi

☐ **Monografia** ☒ **Artikkeliväitöskirja** ☐ **Esseeväitöskirja**

Tiivistelmä

Kiinnostus langattomia esineiden internet -laitteita (IoT) ja älykästä ympäristöä kohtaan on kasvanut merkittävästi viime vuosina. IoT-laitteiden turvallisuudesta on tullut huolenaihe, sillä IoT on mahdollistanut laitteiden ja ihmisten vuorovaikutuksen ajasta ja paikasta riippumatta. Olennaiseksi vaatimukseksi on noussut riittävä suoja aktiivista salakuuntelua vastaan tai laitteiden sekoittamista muiden käyttäjien laitteisiin. IoT-laitteiden sulautetun luonteen vuoksi niiden laskenta- ja viestintäkapasiteetti, sekä käytettävissä oleva teho ovat usein rajallisia. Ympäristössä olemassa olevan signaalin takaisinheijastukseen perustuva kommunikaatio (AmBC) nähdään käyttökelpoisena ratkaisuna resursseiltaan rajoitetuille laitteille, koska nämä eivät tarvitse tiedonsiirtoon aktiivisia RF-komponentteja. Alkuperäisen signaalin aiheuttama interferenssi on kuitenkin edelleen suuri haaste, sillä vastaanotin näkee sen yhdessä takaisinheijastetun signaalin kanssa.

Väitöskirjan tulokset auttavat turvaamaan IoT-laitteiden tiedonsiirtoa AmBC-ympäristössä. Väitöskirjan kontribuutioita ovat kaksisuuntainen salausavaimen generointiprotokolla ja AmBC-modulaattori. Kehitetty salausavaimen generointiprotokolla kerää salaista avainta virheenkorjatuista pariteettibiteistä. Tunnettuihin protokolliin verrattuna kehittämämme ratkaisu tarjoaa paremman suorituskyvyn. Protokollan toimivuutta on analysoitu kahdessa eri toimintamallissa, kvanttiavainjakelussa ja satelliittimallissa.

Toinen kontribuutio on AmBC-modulaattori, joka tekee polarisaatiomuunnoksen suoran ja takaisinheijastetun signaalin välillä. Vastaanotin käyttää hyväkseen kahden polarisaation vastaanotinantennia, jolla vähennetään merkittävästi alkuperäisen lähettimen aiheuttamaa interferenssiä. Ehdotettu järjestelmä saavuttaa kaiuttomassa RF-kammiossa yli 25 dB:n vaimennuksen kapeakaistaisen takaisinheijastetun signaalin ja alkuperäisen signaalin välillä.

Tässä väitöskirjassa analysoidaan salausavaimen kehittämistä AmBC-laitteiden välillä, kun laitteiden välistä radiokanavaa käytetään satunnaisuuden lähteenä. Osoitamme, että ilman näköyhteyttä olevilla kanavilla muutamaa aallonpituutta suurempi etäisyyskään salakuuntelijan ja käyttäjien välillä ei takaa riittävää turvallisuutta. Aiemmin on oletettu pelkän etäisyyden estävän salakuuntelijaa saamasta mitään tietoa salausavaimesta ennen virheenkorjausta. Simulaatiomme osoittavat, että etäisyyteen perustuva lähestymistapa on liian optimistinen, ja on mahdollista, että salakuuntelija tietää vielä merkittävän osan lopullisesta salausavaimesta.

Käyttökelpoinen ratkaisu perustuu kaksisuuntaiseen salausavaimen generointiprotokollaan olettaen, että salakuuntelijan virhesuhde on k-kertainen käyttäjien virhesuhteeseen verrattuna, kun $k < 1$. Tämä menetelmä antaa käyttäjille vapauden tasapainotella saavutettavissa olevan avaimen määrän ja salakuuntelijan tiedon välillä lopullisesta avaimesta.

Avainsanat Fyysisen kerroksen tietoturva, IoT, polarisaatiomuunnos, salausavaimen kehittäminen, takaisinheijastukseen perustuva kommunikaatio

ISBN (painettu) 978-952-64-1296-2 **ISBN (pdf)** 978-952-64-1297-9

ISSN (painettu) 1799-4934 **ISSN (pdf)** 1799-4942

Julkaisupaikka Helsinki **Painopaikka** Helsinki **Vuosi** 2023

Sivumäärä 181 **urn** http://urn.fi/URN:ISBN:978-952-64-1297-9

Preface

The research work for this doctoral thesis was carried out at the Department of Communications and Networking (ComNet) in the School of Electrical Engineering at Aalto University. That was a truly inspiring and amazing community to do research work.

I would like to thank my supervisor Professor Olav Tirkkonen for giving me this opportunity and his thorough support throughout my work. My advisor, Doctor Roope Vehkalahti, I would like to thank for his meaningful guidance and valuable contribution to my work. Doctor Kalle Ruttik was always willing to discuss various ideas and in doing that he helped me to better understand the problems at hand.

I would like to thank all my co-authors for their respective contributions to the research work. Viktor Nässi gave me valuable support whenever I needed to use the facilities at the laboratory. In addition, I am thankful for the meaningful discussions with all my colleagues at ComNet.

Special thanks to my wife Tarja, family members and friends. You have all supported me during this work.

Lohja, April 11, 2023,

Jari Lietzén

Contents

List of Publications

This thesis consists of an overview and of the following publications which are referred to in the text by their Roman numerals.

I Behnam Badihi, Aleksi Liljemark, Muhammad Usman Sheikh, Jari Lietzén and Riku Jäntti. Link Budget Validation for Backscatter-Radio System in Sub-1GHz. In *IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakech, pp. 1-6, Apr. 2019.

II Jari Lietzén, Roope Vehkalahti and Olav Tirkkonen. A Two-way QKD Protocol Outperforming One-way Protocols at Low QBER. In *IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, pp. 1106-1111, Jun. 2020.

III Jari Lietzén, Aleksi Liljemark, Ruifeng Duan, Riku Jäntti and Ville Viikari. Polarization Conversion-Based Ambient Backscatter System. *IEEE Access*, Vol. 8, pp. 216793 - 216804, Dec. 2020.

IV Le Nguyen, Stephan Sigg, Jari Lietzén, Rainhard Dieter Findling and Kalle Ruttik. Camouflage learning: Feature value obscuring ambient intelligence for constrained devices. *IEEE Transactions on Mobile Computing*, pp. 781 - 796, Jun. 2021.

V Jari Lietzén, Olav Tirkkonen and Roope Vehkalahti. Secret Keys from Parity Bits in the Satellite Setting. In *IEEE International Symposium on Information Theory (ISIT)*, Espoo, pp. 2672-2677, Jun. 2022.

VI Jari Lietzén and Olav Tirkkonen. Secret Key Generation between Ambient Backscatter Devices. *IEEE Access, Early access*, pp. 1-13, Feb. 2023.

Author's contributions

Publication I: "Link Budget Validation for Backscatter-Radio System in Sub-1GHz"

The author designed the backscatter modulator used in the experiments and wrote the corresponding analysis of the modulator.

Publication II: "A Two-way QKD Protocol Outperforming One-way Protocols at Low QBER"

The author participated in formulating the research problem and the theoretical analysis. The author had a leading role in the modelling and writing the paper.

Publication III: "Polarization Conversion-Based Ambient Backscatter System"

The author had a leading role in formulating the research problem, and invented the concept of polarization conversion system. The author derived the theoretical results, and designed and made the backscatter modulator and the corresponding receiver antenna construction, and wrote most of the paper.

Publication IV: "Camouflage learning: Feature value obscuring ambient intelligence for constrained devices"

The author designed the backscatter modulator used in the experiments and wrote the corresponding analysis of the modulator. The author de-

signed and made the semidirectional antennas used in the experiments, and wrote the corresponding parts of the paper.

Publication V: "Secret Keys from Parity Bits in the Satellite Setting"

The author participated in formulating the research problem and the theoretical analysis. The author had a leading role in the modeling and writing the paper.

Publication VI: "Secret Key Generation between Ambient Backscatter Devices"

The author had a leading role in formulating the research problem, and the system model. The author produced and analysed the results, and wrote the paper.

List of Figures

List of Tables

Abbreviations

3GPP	3rd Generation Partnership Project
6G	Sixth Generation of Mobile Networks
ADC	Analogue-to-Digital Converter
AmBC	Ambient Backscatter Communication
ASK	Amplitude Shift Keying
BCBCS	Bistatic Collocated Backscatter Communication System
BDBCS	Bistatic Dislocated Backscatter Communication System
BER	Bit Error Rate
BPSK	Binary Phase-Shift Keying
BSC	Binary Symmetric Channel
D2D	Device-to-Device
DLI	Direct-link Interference
DMC	Discrete Memoryless Channel
DSC	Distributed Source Coding
IoT	Internet of Things
IRS	Intelligent Reflecting Surfaces
LDPC	Low-Density Parity Check
LHCP	Left-Hand Circular Polarization
LOS	Line-of-sight
LUT	Lookup Table

MAQ Multibit Adaptive Quantization

MBCS Monostatic Backscatter Communication System

ML Maximum Likelihood

MTC Machine-Type Communications

OFDM Orthogonal Frequency Division Multiplexing

OOK On-Off Keying

OTP One-Time Pad

PAM Pulse Amplitude Modulation

PCP Parity-Check Protocol

PKI Public Key Infrastructure

PSK Phase Shift Keying

QBER Quantum Bit Error Rate

QKD Quantum Key Distribution

QuaDRiGa QUAsi Deterministic RadIo channel GenerAtor

RFID Radio-Frequency Identification

RF Radio Frequency

RHCP Right-Hand Circular Polarization

RSSI Received Signal Strength Indicator

SPDT Single Pole Double Throw

TPPR Two-way Protocol with Parity bit Reconciliation

VNA Vector Network Analyzer

Symbols

B	Path-blockage loss
B_{BC}	Backscatter link path-blockage loss
B_f	Forward link path-blockage loss
c	Speed of light
C_A	Binary symmetric channel for Alice
C_B	Binary symmetric channel for Bob
C_E	Binary symmetric channel for Eve
C_{T}	Diode capacitance
$D(X\|\|Y)$	Relative entropy between X and Y
$erf(x)$	Error function
$\mathbb{E}(X)$	Expected value
F_{BCBCS}	Bistatic dislocated fade margin
F_{BDBCS}	Bistatic dislocated small-scale fading loss
f_c	Center frequency
f_{in}	Fraction of sifted bits
f_m	Doppler spread
F_{MBCS}	Monostatic backscatter fade margin
G_{BC}	Load-matched free-space gain for backscatter antenna
G_R	Load-matched, free-space gain of receiver
G_T	Load-matched, free-space gain of transmitter

G_{TR}	Load-matched free-space gain for transmitter antenna
$h(p)$	Binary entropy function
$I(X;Y)$	Mutual information between X and Y
k	Error rate estimation factor
M	Modulation factor
$\mathcal{N}$	Set of error corrected parity bits
N_{sif}	Number of sifted bits
p	Transition probability
p_{col}	Collision probability
p_{in}	Incoming error rate
p_{out}	Outgoing error rate
P_R	Received modulated backscatter power
P_T	Unmodulated carrier transmitter power
$Q(x)$	Quantizer function
r	Distance between backscatter device and reader or receiver
r_{BC}	Backscatter path, from device to receiver
r_f	Forward path, from transmitter to the device
R_{f}	Forward resistance
R_{OW}	One-way protocol key rate
r_s	Distance between collocated antennas
S	Secret key
T_c	Coherence time
$\mathcal{T}$	Set of terminated parity bits
v	Speed of the user
W	Message
X	Polarization mismatch
X_{BC}	Backscatter link polarization mismatch
X_f	Forward link polarization mismatch

x_{in}	Incoming collision probability
x_{out}	Outgoing collision probability
Z_0	Characteristic impedance
Z^n	Signal carrying the message
β	Bit error rate between Alice and Bob
ϵ	Information leakage parameter
ϵ_A	Alice's error probability
ϵ_B	Bob's error probability
ϵ_E	Eve's error probability
η	Bit error rate between Bob and Eve
γ	Bit error rate between Alice and Eve
Γ	Complex Reflection Coefficient
λ	Wavelength
Θ	On-object gain penalty

1. Introduction

1.1 Motivation

In recent years, the interest in wireless Internet of Things (IoT) and Ambient Intelligence has increased significantly [1]. There are more and more applications for embedded or wearable sensing devices forming a personal area network. For example, the sensing devices could be monitoring the environment, like the temperature, humidity or the level of lighting, or are gathering information about the vital statistics of the user, like the heart rate, body temperature or respiration rate. Due to the embedded nature of these devices, they are often limited in their computational, communication and power resources [1, 2]. Therefore, ambient backscatter communication (AmBC) is seen especially effective in addressing the communication and energy consumption issues for low-power IoT devices [3, 1]. In backscatter communication, wireless nodes are communicating without any active radio frequency (RF) components. Instead of generating the RF signal at the node itself, the devices are capable of reflecting the incoming RF signal back to the receiver, effectively becoming a modulator by changing the amount of reflection [4, 5]. However, a major challenge is the presence of the ambient signal at the receiver which interferes with the backscattered signal.

Ambient Intelligence is based on collecting and using data from distributed sensing devices. While IoT has made it possible for things and people to interact with each other any time and any place, at the same time the security of IoT devices has become a concern [6, 7]. As the devices are communicating with each other or to some coordinator, it is important that the devices can trust each other. There should be sufficient protection against confusing with other users' devices or active eavesdropping.

The use of cryptographic methods in order to enforce security for the connected devices is the conventional method. Due to the limitations in electrical and computational power, this makes it difficult to implement

and use complex security methods. Traditional security schemes are based on public key cryptography to support confidentiality, data integrity and authentication [8, 9, 10]. Public key cryptographic methods are asymmetric as they use a public key to encrypt messages and a private key to decrypt them [11]. Asymmetric cryptography has high energy and implementation costs, as these methods rely on computational hardness to provide security [12, 9].

A symmetric encryption method uses the same key for encryption and decryption, but this raises the question of key distribution, as both parties must have the same key [13]. Preconfiguring the secret keys, for example, at the time of manufacturing the devices, does not scale well; adding and removing devices may require updating the existing keys. Another solution is to use a configuration system to deliver the keys to the devices, but this approach is vulnerable to eavesdropping during the configuration phase [14]. Due to the broadcast nature of wireless channels, this is especially problematic for wireless IoT devices.

Alternatively, the secret key is distilled from the environment, e.g. using the wireless channel as a source of randomness for secret key generation. As wireless channels change in time, exploiting the randomness of the fading channel provides information-theoretic security [15, 9, 2]. The information for creating secret keys is extracted from random spatial and temporal variations of the reciprocal wireless channel [10]. Even if the eavesdropper has unlimited computational power, the same randomness of the radio channel limits the information that an eavesdropper can get at the bit level [9, 13].

1.2 Objectives and Scope

The scope of this thesis is on secure communication between IoT or personal area network devices. Motivated by the importance of the security of connected devices, this thesis studies both secret key agreement between the connected devices and enhancing robustness of the communication link in an AmBC setting. The aim is to investigate and develop a backscatter device that mitigates the interference from the ambient transmitter and to develop a method for secret key agreement that is suitable for IoT devices.

The building blocks forming the scope of this thesis are shown in Fig. 1.1. The legitimate users use *a key agreement* protocol to obtain a shared secret key, or they can use *a learning based* data obfuscation method to conceal their communication. The secret key is obtained using *wireless channel* as a source of randomness for *key distillation* and the users are using *backscatter communication* when communicating with each other. The figure is revisited in later chapters when each building block is discussed in more detail.

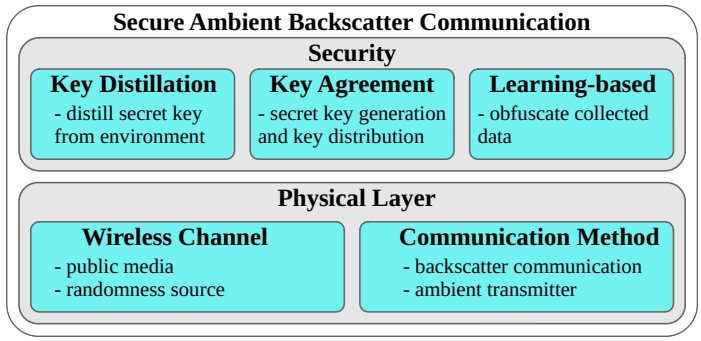


Figure 1.1. The scope of this thesis and the corresponding building blocks.

1.3 Contributions and Structure of the Thesis

This thesis contributes to secure IoT device communication in an AmBC setting. The contributions are a novel two-way secret key agreement protocol, which provides complementary performance compared to protocols known in the literature and a backscatter device design that decreases substantially the direct path interference from the ambient transmitter. In contrast to similar protocols known in the literature, the secret key is gathered from error corrected parity bits, and not from legitimate users' original bit strings. We analyse secret key generation between ambient backscatter devices and show that the distance from legitimate users to an eavesdropper is not alone a sufficient security guarantee. This is in contrast with previous secret key generation methods where the distance is the only safeguard and privacy amplification removes any information that the eavesdropper overheard during the error correction phase.

The thesis is organized as follows. Chapter 2 provides an overview of backscatter communications and introduces the corresponding modulator and receiver components. Chapter 3 discusses secret key agreement and key growing protocols and defines perfect and information-theoretic security for one-way and two-way protocols. In addition, two common key agreement models are discussed as well, the satellite setting and the quantum key distribution (QKD) setting. The use of a wireless channel as a source of randomness, and how to extract raw key material from channel measurements are reviewed in Chapter 4. Furthermore, the properties of a wireless channel which enable the randomness extraction are also discussed in Chapter 4.

Chapter 5 presents the author's backscatter device designs. Chapter 6 presents a novel two-way secret key agreement protocol and the corresponding secret key rate analysis both in the satellite setting and in the QKD setting. All building blocks from Fig. 1.1 are tied together to secure IoT communication in AmBC setting in Chapter 7. Finally, conclusions and potential avenues for future work are given in Chapter 8.

1.4 Summary of the Publications

This thesis consists of an introductory part and six original publications. In **Publication I** the link budget of a backscatter radio system is analysed and **Publication III** proposed a method to substantially decrease the direct path interference signal from the ambient transmitter. In **Publication II** we introduced a new secret key agreement protocol and analysed its performance in the QKD setting. The same protocol is analysed in the satellite setting in **Publication V**. **Publication IV** proposed a distributed machine learning scheme to address the security aspects of distributed sensing devices using AmBC. In **Publication VI** we proposed and analysed a secret key agreement method for ambient backscatter devices.

Publication I conducts a comprehensive study including measurements in different propagation environments, and a thorough simulation to validate backscatter radio system's link budget. The measurements were done in an anechoic chamber, indoors in a corridor, and outdoors in a parking lot using our own backscatter modulator. The results confirm the link budget equations in a backscatter system with trivial error between measurements and simulation.

In **Publication II** we proposed a new two-way secret key agreement protocol based on advantage distillation, and collecting secret key from parity bits. Two-way protocols are known to provide secret key rates for considerably higher quantum bit error rates (QBER) than one-way protocols. However, when QBER is low, only modest key rate gains have been achieved, and this has been one of the major obstacles to using two-way protocols. Under the assumption that the eavesdropper can only perform individual symmetric attacks, our protocol achieves a secret key rate that is higher than the information-theoretical bound limiting the performance of any one-way protocol.

Publication IV investigates the performance of the machine learning based distributed data obfuscation scheme with respect to communication range, impact on challenging communication environments, power consumption, and the backscatter hardware prototype. The author's contribution to **Publication IV** was to design the backscatter devices and antennas used in the experiments.

In ambient backscatter communications, the direct signal from the ambient transmitter can be several orders of magnitude stronger than the backscattered one. In **Publication III** we proposed a polarization-conversion based method to substantially decrease the direct path interference from the ambient transmitter. The backscatter device changes the polarization of the ambient signal from linear to circular. The receiver antenna is a circularly polarized patch antenna with a 180°-hybrid to obtain the difference between the left- and right-hand polarized fields. Ideally, this receiver antenna and 180°-hybrid combination would completely re-

move the linearly polarized direct path and reflected components. We showed that in an anechoic RF chamber, our proposed set-up could achieve more than 25 dB isolation between the backscattered component, and the ambient component for narrowband signals.

The secret key agreement protocol introduced in **Publication II** is considered in the satellite setting in **Publication V**. In the satellite setting the legitimate users and an eavesdropper each decode bits from noisy signals received from a source in their environment. A key agreement protocol in the satellite context could be used to provide secret keys to IoT type devices, which are often limited in computational or electric power. We analysed the mutual information acquired by the eavesdropper from exploiting the original eavesdropped information together with the information leaked during the distillation protocol, as well as the achieved key rate. Comparing with the Parity-Check Protocol (PCP) known in the literature, our protocol provides complementary performance.

In **Publication VI** we analysed secret key generation between ambient backscatter devices where the channel between an ambient transmitter and the backscatter devices is used as a source of randomness. We analysed the eavesdropper's mutual information based on fundamental principles, and we used state-of-the-art wireless channel models from the 3rd Generation Partnership Project (3GPP) to model the radio channel between an ambient transmitter and the backscatter devices. We show that even in non-line-of-sight channels the distance from legitimate users to an eavesdropper being larger than a few wavelengths is not alone a sufficient security guarantee. This is in contrast with previous secret key generation methods, where the distance is assumed to prevent the eavesdropper from having any information about the key prior to error correction. Our simulations show that a distance based approach is too optimistic, and there is a possibility that the eavesdropper still knows a substantial part of the final key. We show how the legitimate users can estimate the eavesdropper's knowledge, and trade off between the achievable key rate and the eavesdropper's knowledge of the final key.

2. Backscatter Communications

2.1 Introduction

In backscatter communication wireless nodes are communicating without active RF components [3]. This concept was first introduced by Stockman in 1948 [16]. It has since been studied and used in low-power and short-range wireless communication systems, for example in radio-frequency identification (RFID) technology. The principal idea in backscatter communication is to modulate the incoming RF signal and reflect it back to the receiver instead of generating the RF signal locally [4, 5]. Detecting the backscattered signal at the receiver may be a challenging task as the backscattered signal levels are usually very low and the signal source whose signal is backscattered is present at the receiver causing interference.

The lack of active RF components decreases the number of components which in turn decreases costs and energy consumption. The decreased energy consumption makes energy harvesting methods a viable solution to power the devices. Backscatter communication is therefore an appealing physical layer communication building block for low power IoT devices, as shown in Fig. 2.1.

2.2 Backscatter Communication Systems

Three types of different backscatter communication system configurations are considered in the literature [17], [1]. These configurations are *monostatic*, *bistatic collocated* and *bistatic dislocated* backscatter communication systems.

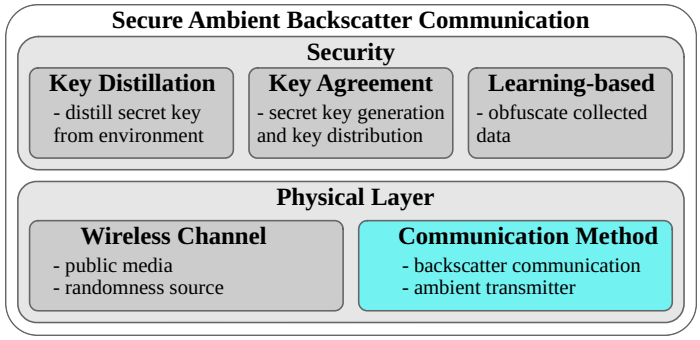
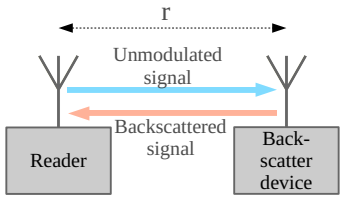
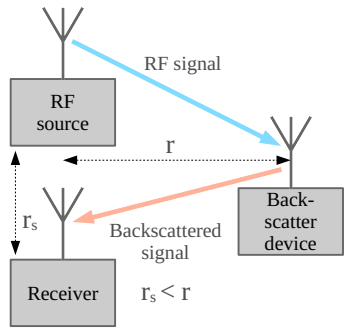


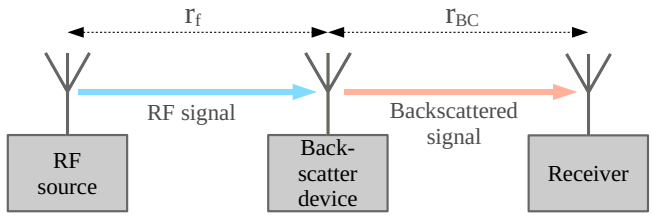
Figure 2.1. Backscatter communication as a physical layer communication method in the scope of secure AmBC.



(a) The monostatic backscatter configuration (MBCS).



(b) The bistatic collocated backscatter configuration (BCBCS).



(c) The bistatic dislocated backscatter configuration (BDBCS).

Figure 2.2. Three main configurations of backscatter communication system.

2.2.1 The Monostatic Backscatter Communication System

The transmitter and the receiver share a common antenna in the monostatic backscatter communication system (MBCS). This architecture has two main components: a backscatter device, and a reader as shown in Fig. 2.2, part (a). The backscatter device modulates the received RF signal from the reader and reflects the modulated signal back to the reader. As the link from the RF source to the device, and the link from the device back to the reader are identical paths, the slow fading phenomena may cause severe path loss to the received signal. The received modulated backscatter power P_R at the reader is given by a linear-scale link budget [17]:

$$P_R = \frac{P_T G_{TR}^2 G_{BC}^2 \lambda^4 X^2 M}{(4\pi r)^4 \Theta^2 B^2 F_{MBCS}}, \tag{2.1}$$

where P_T is the power of the unmodulated carrier transmitted from the reader, G_{TR} and G_{BC} are the load-matched free-space gains of the full-duplex antennas of the reader and the backscatter device. The polarization mismatch is X, M is the modulation factor, Θ implies the on-object gain penalty of the backscatter device, B indicates the path-blockage loss, F_{MBCS} is the monostatic backscatter fade margin, and r is the distance between the reader and the backscatter device.

While this configuration has a drawback of self-interference, the MBSC architecture is predominantly used in commercial RFID readers. The monostatic configuration suffers also from round-trip path loss [18], and if the backscatter device is located far from the reader, it experiences higher outage probability due to signal loss between the reader and the backscatter device [1].

2.2.2 The Bistatic Collocated Backscatter Communication System

The transmitter and the receiver are separated in the bistatic collocated backscatter communication system (BCBCS). This configuration is shown in Fig. 2.2, part (b). The antenna for transmitting and receiving are collocated within a few wavelengths apart, marked as distance r_{s} in Fig. 2.2, part (b). As the forward link and backscatter link are slightly dissimilar, BCBCS can improve round-trip path loss compared to MBSC. The linear-scale link budget in BCBCS configuration for the received modulated backscatter power, P_R is given by [17]:

$$P_R = \frac{P_T G_T G_R G_{BC}^2 \lambda^4 X^2 M}{(4\pi r)^4 \Theta^2 B^2 F_{BCBCS}}, \tag{2.2}$$

where G_T and G_R stand for the load-matched, free-space gains of transmitter and receiver antennas, respectively, and F_{BCBCS} indicates the bistatic dislocated fade margin. Considering equations (2.1) and (2.2), two main

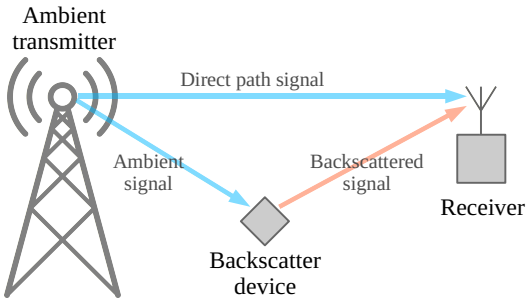


Figure 2.3. Ambient backscatter communication system operating principle.

differences are observed. The antenna gains for the transmitter and the receiver can be different as they are separated, and since the small scale fading on forward and backscatter paths are different in comparison with the monostatic case, the bistatic fade margin F_{BCBCS} is applied in this configuration.

2.2.3 The Bistatic Dislocated Backscatter Communication System

The transmitter and receiver are freely located in the bistatic dislocated backscatter communication system (BDBCS). This configuration is shown in Fig. 2.2, part (c). The linear-scale link budget in BDBCS for the received modulated backscatter power is calculated by:

$$P_R = \frac{P_T G_T G_R G_{BC}^2 \lambda^4 X_f X_{BC} M}{(4\pi)^4 r_f^2 r_{BC}^2 \Theta^2 B_f B_{BC} F_{BDBCS}}, \tag{2.3}$$

where r_f is the forward path from the transmitter to the device and r_{BC} is the backscatter path from the device to the receiver. X_f and X_{BC} indicate forward link and backscatter link polarization mismatches, respectively, and B_f and B_{BC} are the forward link and backscatter link path-blockage losses. F_{BDBCS} symbolizes the bistatic dislocated small-scale fading loss. In (2.3), G_{BC} is calculated as the average RF device gain. The reason being, the angle-of-arrival and angle-of-departure are dissimilar for a wave entering to the device and leaving the device [17].

2.2.4 The Ambient Backscatter Communication System

In MCBS and BCBCS backscatter systems, the device usage and coverage area are limited by the requirement that the backscatter device needs to be near the RF source [1]. As the conventional backscatter systems operate passively, a backscatter device can transmit only when the backscatter receiver is inquiring it, and this also limits the communication performance.

AmBC systems can effectively address these limitations [19]. In AmBC

systems, the backscatter devices utilize the surrounding signals from ambient RF sources, e.g. terrestrial TV or FM radio transmitters, cellular mobile stations, or wireless local area network access points [1]. A backscatter device modulates the ambient signal that is impinging its antenna and the receiver sees the message on top of the ambient signal, as illustrated in Fig. 2.3. In this case, the backscatter system does not need a dedicated RF signal source. Therefore, the AmBC system can be seen as an extension to the bistatic system. It is challenging to detect the backscattered signal at the receiver because the signal levels are usually very low and the signal from the ambient transmitter is present at the receiver as well, causing interference. However, as the backscattered signal is superimposed to the ambient signal, it is important that the backscattered signal is not causing interference for the original users [1].

2.3 The Backscatter Modulator

As the backscatter devices do not have any active RF components, they need some other method in order to transmit information. The devices are capable of reflecting the incoming RF signal back to the receiver, effectively becoming a modulator by changing the amount of reflection. The modulators are said to be passive, if the modulator draws the energy it needs to operate from the RF signal it receives or is using some other energy harvesting method to power itself. A semi-passive modulator is using a battery to provide all or some additional power to the modulator [1].

One possible modulator implementation uses a switch connected to an antenna. Depending on the position of the switch the incoming RF signal is either absorbed in a terminating resistor or the switch is short-circuiting the antenna, resulting in a total reflection of the incoming RF signal. In general, this type of modulator selects one complex impedance out of a set of predetermined impedances. In the case of a matched impedance and a short circuit, this produces on-off-keying (OOK) modulation. More complex modulations, including phase and amplitude modulations, are possible with a suitable choice of complex impedances. Assuming the antenna is matched to characteristic impedance Z_0, then the complex reflection coefficient Γ is [20, p.57]

$$\Gamma_{\mathrm{A}} = \frac{Z_{\mathrm{A}} - Z_0}{Z_{\mathrm{A}} + Z_0} \,, \tag{2.4}$$

where Z_{A} is the selected impedance. In case of two different impedances Z_{A} and Z_{B}, the modulation factor M in (2.1), (2.2), and (2.3) is [17]

$$M = \frac{1}{4}|\Gamma_{\mathrm{A}} - \Gamma_{\mathrm{B}}|^2 \,. \tag{2.5}$$

If the impedance $Z_{\mathrm{A}} = Z_0$, and $Z_{\mathrm{B}} = 0$, i.e. a short circuit, then $\Gamma_{\mathrm{A}} = 0$ and $\Gamma_{\mathrm{B}} = -1$, correspondingly. In this ideal case, the modulation factor

$M = 0.25$. The maximum value for M is 1, that is achieved when $\Gamma_{\mathrm{A}} = 1$ and $\Gamma_{\mathrm{B}} = -1$, corresponding an open circuit and a short circuit.

Antennas also have a structural mode in addition to the antenna mode [21]. The structural mode does not cause currents at the antenna feed and thus are rescattering the incoming signals. This rescattering is not part of the signal modulated by the backscatter modulator, but rather appears as a constant background backscattered signal at the receiver.

A diode was used as a switching element in [17], realizing a single pole switch. A diode acts as a current controlled switch, a current flowing through the diode sets it in a conducting state [20, pp.530-532]. However, the current required to keep the diode conducting could be relatively high, e.g. around 1 mA. For a passive modulator this amount of current consumption is usually too high. Several works are using an integrated RF switch component instead of a diode [19, 22, 23, 24]. In [22] ADG919 RF switch was used, requiring less than 1 μA to operate [25]. An M-PSK modulation method was proposed in [23] and a 4-PSK modulator was implemented using a four pole RF switch. A backscatter modulator using a quarter-wavelength transmission line as a delay element with switches at both ends to realize binary phase shift keying (BPSK) modulation is used in [26].

In [27] the authors used pulse shaping to generate the modulating waveforms, instead of selecting between predetermined impedance values. Using continuously variable antenna load instead of switching e.g. between two discrete values, significantly decreases the required bandwidth per backscatter modulator. Out-of-band emissions are also suppressed with the use of pulse shaping and this in turn helps to meet regulatory limitations [27]. This method was further utilized in [28], where a single RF transistor connected to a microstrip antenna array was used to modulate a 24-28 GHz millimetre-wave signal. The authors demonstrated that it is possible to achieve high-order modulations, e.g. 16-QAM, and data rates up to 2 Gbits/s using only a single transistor even at very high frequencies.

The modulator can utilize multiple polarizations and change antenna polarization according to the modulating message. A modulator that is using four different polarization directions is proposed in [29].

A semi-passive modulator is proposed in [30] that uses a reflection amplifier instead of a load resistor. A battery powered microcontroller biases a tunnel diode to modulate and amplify the incoming RF signal. A substantial 34 dB return gain is reported when reflecting back a 5.45 GHz signal while using only 45 μW power.

2.4 The Ambient Backscatter Receivers

Receiving and demodulating the transmitted data at the AmBC receiver is a challenging task for two reasons. The backscattered signal is weak and it is received together with the unknown modulated ambient signal, and the ambient signal also contains information of its own [19, 31]. The ambient signal appears as direct-link interference (DLI) at the AmBC receiver, as shown in Fig. 2.3. Compared with RFID systems where the DLI signal is an unmodulated carrier frequency, in AmBC systems the removal of DLI signal is more complicated [31].

In cooperative AmBC, the receiver is able to acquire information about the ambient signal before the signal detection, and therefore the receiver can cancel the ambient signal prior detecting the backscattered symbols [32]. In non-cooperative model the AmBC receiver has very limited amount of information about the ambient signal, or none at all [32]. Several methods have been proposed to mitigate the effect of the DLI signal. In [33] the receiver has two antennas and the ratio of the received signals is used to cancel DLI out. The repeating structure of an orthogonal frequency division multiplexing (OFDM) signal is used to tackle the DLI problem in [34].

The receiver can work either in a coherent or non-coherent mode when it is decoding the received symbols. In coherent mode the phase information of the received pulse is available at the receiver, whereas in non-coherent detection it is not [35, Ch. 10.3, 10.11]. Comparing BPSK and amplitude shift keying (ASK) modulations, ASK needs 3 dB more pulse energy than BPSK for the same performance [35, p. 521]. Decoding BPSK or any other modulation that uses phase information requires the use of coherent detection. However, non-coherent detection only needs a filter matched to the RF pulse, an envelope detector, sampler and a comparator for making the detection decision [35, p. 581].

The use of a coherent receiver would require a pilot assisted channel estimation and coordination between the ambient and backscatter system [31]. Therefore, to eliminate the complex task of channel estimation, a non-coherent receiver has been proposed in a number of works [19, 36, 37, 38, 39, 40, 41, 42]. Because the phase information is not available when using non-coherent detection, this results in a performance loss compared with coherent detection [32]. Furthermore, if the backscatter devices are communicating with each other in a device-to-device (D2D) manner, the backscattered information should be decodable without using power or computationally hungry components, such as analogue-to-digital converters (ADCs) or oscillators [19].

2.5 Receiver implementations

The original idea behind the first AmBC receiver was that if the information rate of the backscatter device is lower than that of the ambient signal, the receiver can use averaging to extract the backscattered information [19]. The adjacent samples in the ambient signal are more uncorrelated than the corresponding samples in the backscattered signal. Therefore, averaging the received signal over multiple samples of the ambient signal removes the wideband variations, as the ambient signal is treated as noise [19, 33]. The drawback of this method is that it requires digital samples from an ADC and some digital signal processing in order to work, which can use a large amount of power. As an alternative, an analogue envelope detector and averaging circuit together with a threshold circuit and a comparator are used instead to generate output bits from the received signal in [19]. The averaging also limits the transmit rate of the backscatter device. If the receiver averages the ambient signal over one millisecond, then the maximum rate would be 1 kbps [33].

The authors in [33] used two receiving antennas, individual envelope detectors, and an analogue divider to have a fraction representing two different levels, depending on whether the backscatter device was reflecting or absorbing the ambient signal. This method is named as μmo Decoding, and it does not use any digital computation nor does it need channel estimation. A backscatter device using differential modulation was used in conjunction with a maximum likelihood (ML) detector in [43, 36]. A complete analogue backscatter device and sensor design is used to modulate FM broadcasts and the resulting signal can be received by any off-the-shelf FM receiver [22].

The backscatter symbol period is matched to the OFDM symbol period of the ambient transmitter in [34]. The backscatter device either makes a state change in the middle of an OFDM symbol or keeps the state, corresponding to information bits 1 and 0. This signal detection method is able to cancel out DLI by exploiting the repeating cyclic prefix structure [34]. This approach requires that the backscatter device knows the timing of OFDM symbols and can time its own transmission accordingly.

The backscatter device is also synchronized to the ambient OFDM signal in [40]. The backscatter device shifts the spectrum of the backscattered signal to null subcarriers of the OFDM signal when the transmitted bit is 1. Therefore, an energy detector can be used at the receiver to listen to the null subcarriers to decode the backscattered signal [40].

An ML detector which does not require a priori knowledge about the channels or ambient symbols is presented in [31]. A backscatter transmitter and receiver pair suitable for D2D communication is presented in [23]. The devices use M-PSK modulation in order to increase the data rate.

The bit error rate (BER) is enhanced by the use of transmission repe-

Table 2.1. Reported transmission rates and ranges.

Rate	Range	Frequency	Modulation	Reference
1 kbps	0.76 m outdoor 0.46 m indoor	539 MHz	ASK	[19]
1 Mbps	25 m	539 MHz	ASK	[33]
20 kbps	0.76 m	539 MHz	4-PSK	[23]

titions that also helps to filter out WiFi carrier fluctuations in [44]. The joint detection of both ambient and backscattered signal from a low-density parity-check (LDPC) encoded transmission is considered in [45].

Achieved transmission rates and ranges are presented in Table 2.1 for three cases that are reasonably simple to implement and are suitable for D2D communication.

2.6 Intelligent Reflecting Surfaces

Intelligent reflecting surfaces (IRS) can be used to enhance the communication between users [46]. An IRS is made from many small and low-cost reflecting units that are able to reflect the incoming RF signal with an adjustable phase shift. Like backscatter communications, the IRS does not need active RF components, but it needs a controller that is working in conjunction with either the transmitter or receiver [47]. The signal from the transmitter is reflected by an IRS and can add constructively or destructively with the direct signal at the receiver, either enhancing the wanted signal or suppressing the unwanted signal [46]. Unlike backscatter communications, an IRS is only assisting the signal transmission, it does not usually send any information of its own [47].

However, an IRS is used to aid backscatter communications in [48], where the transmitted signal is split in two. The first part is the message signal and the second part is an unmodulated carrier signal. In addition to suppressing unwanted signals at the receiver, such as DLI, an IRS can be used to put an eavesdropper at a disadvantage compared to legitimate users [46]. This is done by causing the signal power seen by the eavesdropper to decrease. While IRS is a somewhat similar technique compared to backscatter communications, it does have added complexity as it needs a separate controller to operate. Therefore, backscatter communications is better suited for D2D applications. A comprehensive survey towards smart wireless communications using IRS is presented in [49].

3. Secret Key Agreement and Key Growing Protocols

3.1 Introduction

If two parties, say Alice and Bob, want to communicate in the presence of an eavesdropper Eve, Alice and Bob need to use some cryptosystem to make it as hard as possible for Eve to get information about the messages. Several cryptosystems have been developed and are in use, but according to Kerckhoffs' principle, the security of the cryptosystem should only rely on the secrecy of the key and not the secrecy of the algorithm [50, p.16]. Perfect secrecy is achievable in the form of the one-time pad (OTP), but it requires that a key is used only once, and that the key is at least as long as the message [50, pp.16-17]. Even if Alice and Bob are not seeking perfect secrecy, they still need a method in order to distribute the secret key between themselves.

Secret key agreement protocols address the key distribution problem by letting Alice and Bob generate and agree on secret keys when needed without involving any third party to distribute the keys. This is a useful approach for devices that are limited in computational or electric power, or they lack a method in order to communicate with a third party. Therefore, secret key agreement and key growing protocols are an integral part of secure ambient backscatter communication, as illustrated in Fig. 3.1 in the scope of this thesis.

3.2 Perfect Secrecy

Perfect secrecy introduced by Shannon in 1949 is the strongest security scheme [51]. It requires that the message W and the signal Z^n carrying the message and possibly observed by an eavesdropper are statistically independent,

$$\forall w \in \mathcal{W}, \forall z^n \in \mathcal{Z}^n \; p_{WZ^n}(w, z^n) = p_W(w) p_{Z^n}(z^n), \text{ i.e., } I(W; Z^n) = 0 \quad (3.1)$$

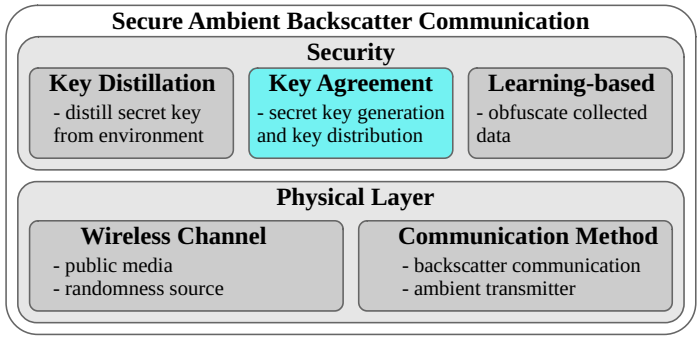


Figure 3.1. Secret key agreement as an integral part of secure AmBC.

where $I(W; Z^n)$ is the mutual information between the message and the signal [52]. If (3.1) is written as $p_{W|Z^n}(w|z^n) = p_W(w)$ it shows that an eavesdropper cannot do better than guess the message at random according to p_W. Perfect secrecy also ensures that every message induces the same statistical distribution of the eavesdropper's observation, as shown when (3.1) is written as $p_{Z^n|W}(z^n|w) = p_{Z^n}(z^n)$ [52]. Some randomization is required for perfect secrecy to hold, as W cannot be a function of Z^n [52]. The aforementioned OTP offers perfect secrecy. However, for practical settings perfect secrecy is not easily achieved, as it requires a new key for each message exchange.

3.3 Information Theoretic Security

Information-theoretic security aims to offer a framework in which the security of information flows can be measured and enforced by using signalling and coding mechanisms [52]. By controlling the rate of information leakage, secure communication is possible through noisy channels, first proven in Wyner's original wiretap channel model [53]. The eavesdropper Eve observes the communication between the honest parties, Alice and Bob, through a wiretap channel, that is degraded in comparison with the original channel. Controlling the information *leakage rate* is referred to *weak secrecy* [52]. The wiretap model and the results were later generalized by Csiszár and Körner [54] and in [55] the eavesdropper was allowed to select which subset of the original message to observe. In all these models, secure communication is possible only if Eve is at a disadvantage compared with Alice and Bob.

3.3.1 Weak Secrecy

By controlling the rate of information leakage, perfect secrecy (3.1) is replaced by Wyner's weak secrecy [53]

$$\frac{1}{n} I(W; Z^n) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \tag{3.2}$$

The relative entropy $D(p_{WZ^n} \parallel p_W p_{Z^n})$ [56, p.250] between the joint distribution p_{WZ^n} and the product of marginals $p_W p_{Z^n}$ can be used to express the mutual information in (3.2). Weak secrecy is a measure of information leakage rate, measuring how many bits about the message W are leaked per symbol of the signal Z^n [52]. It is therefore possible to achieve weak secrecy and to leak many bits of information regardless of how small the parameter $\epsilon > 0$ is [57].

3.3.2 Strong Secrecy

Strong secrecy, introduced by Maurer [58], measures the amount of leaked information instead of the information leakage rate, strengthening the security guarantee [52]. Weak secrecy (3.2) is strengthened by dropping the normalization $\frac{1}{n}$, resulting

$$I(W; Z^n) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \tag{3.3}$$

Writing (3.3) as $\mathbb{E}_W(D(p_{Z^n|W} \parallel p_{Z^n})) \leq \epsilon$ shows that strong secrecy is dependent on the message distribution p_W [52]. It is still possible that some messages are poorly protected even if $D(p_{Z^n|W=w} \parallel p_{Z^n})$ is large while $p_W(w)$ is small [52].

3.3.3 Semantic Secrecy

Semantic secrecy requires that strong secrecy holds regardless of the distribution of the message p_W. Semantic secrecy is named after semantic security known in standard cryptography [59].

$$\max_{p_W} I(W; Z^n) \leq \epsilon \text{ for some suitably small } \epsilon > 0. \tag{3.4}$$

Under semantic secrecy, an eavesdropper cannot do better than randomly guess any function of the message W [59]. Semantic secrecy can be made even stronger by making ϵ disappear with n [52].

3.3.4 Universally Composable Security

Cryptographic protocol settings were traditionally considered in a model where a single execution of the protocol is taking place and the only involved parties are those using the protocol. Allowing relatively concise

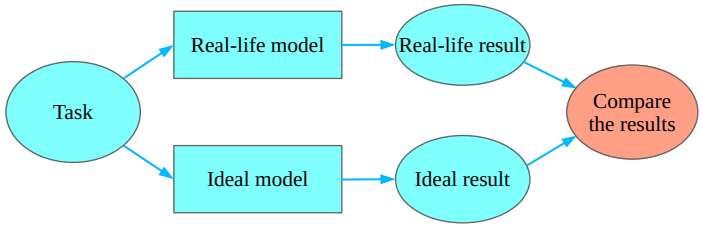


Figure 3.2. Principle of composable security.

problem statements and simplifying the design and analysis of protocols, this model does not necessarily capture the present-day security requirements of cryptographic protocols in networked environments [60]. Instead of stand-alone execution, these protocols may run concurrently with any number of copies of itself or in combination with any other protocols. The protocols may be executed by the involved parties or other parties and the local outputs of a protocol may be used in an unforeseen way [60].

Canetti proposed the *universally composable security framework* that is a general purpose model for the security analysis of cryptographic protocols [61]. A protocol proven secure in the universally composable framework is guaranteed to maintain its security even when multiple copies of it are used in multi-party, and multi-protocol environments, a guarantee provided by a general composition theorem [60, 61].

In the universally composable framework, a real-life model is first created to represent the process of protocol execution in a real-life environment. The next step is to formulate a corresponding ideal process to carry out the same task. The protocol under examination is said to securely realize the ideal task if running the protocol in real-life model produces the same result as running the ideal task [61]. This is illustrated in Fig. 3.2 where the same task is the input to both real-life and ideal models and the results are compared afterwards. The universal composition theorem states that running the protocol in the real-life modes has the same effect as running the protocol in an ideal model [61].

A secret key is considered secure if the difference between the key produced in real-life environment and a perfect key from an ideal process is smaller than some predetermined ϵ. Therefore, the maximum probability that the produced key differs from a perfect key is ϵ [62]. The secret key can now be securely used in any arbitrary context.

3.4 Source and Channel Models in Secret Key Agreement

Two main models exist for secret key agreement: *source model* and *channel model* [63, 64, 52]. In the source model Alice and Bob have the n i.i.d symbols of random variables X and Y while Eve observes the n i.i.d.

symbols of a random variable Z. It is assumed that these random variables are distributed according to a joint probability mass function $p_{\mathrm{XYZ}}(x, y, z)$, i.e. these random variables are dependent, for $x \in \mathcal{X}$, $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, where $\mathcal{X}, \mathcal{Y}$, and $\mathcal{Z}$ are finite sets [52]. Alice and Bob exchange public messages $F_{1,\mathrm{k}}$ over an authenticated channel in order to be able to extract a secret key S. The key should be the same for Alice and Bob with high probability while Eve's information $(Z^n, F_{1,\mathrm{k}})$ should be as small as possible. Applying the weak secrecy constraint (3.2) to source model

$$\frac{1}{n} I(S; Z^n, F_{1,\mathrm{k}}) \leq \epsilon \, . \tag{3.5}$$

The secret key rate is defined as $R_{\mathrm{S}} = \frac{1}{n} H(S)$ and the supremum of all achievable key rates is defined as the secret key capacity $S(X; Y \parallel Z)$ for the source model. The secret key capacity is upper and lower bounded as follows [63], [64]

$$I(X;Y) - \min\{I(X;Z), I(Y;Z)\} \leq S(X;Y \parallel Z) \leq \min\{I(X;Y), I(X;Y|Z)\} \, . \tag{3.6}$$

The key rate capacity is lower bounded by using one-way communication. There are two lower bounds as it is possible to communicate in two different directions [52].

In the channel model either Alice or Bob can control the sequence X^n that is the input to a discrete memoryless channel (DMC). The other user observes Y^n and Eve observes Z^n. The sequence X^n does not have to be i.i.d, as in the source model. A public, authenticated channel is available to Alice and Bob like in the source model. The channel model can then be regarded as a wiretap channel [53] with an additional public channel [52]. Using the same secrecy and reliability constraints with the channel model that were used for the source model the channel model achieves the same secret key rates as the source model [52]. This is because the channel model is more general than the source model. Similar upper bounds can be found for the channel model as for the source model, but due to the generality of the channel model, finding the secret key capacity for it will be harder [52].

To achieve strong secrecy from weak secrecy requires three main steps: *advantage distillation*, *information reconciliation*, and *privacy amplification* [52]. These steps are discussed next.

3.5 Advantage Distillation

If Alice and Bob use multi-round communications, they can gain an advantage over Eve. Even if Eve originally has a better channel than Alice and Bob, they can concentrate their efforts to those parts of X and Y they both received reliably [52]. *Advantage distillation* allows Alice and

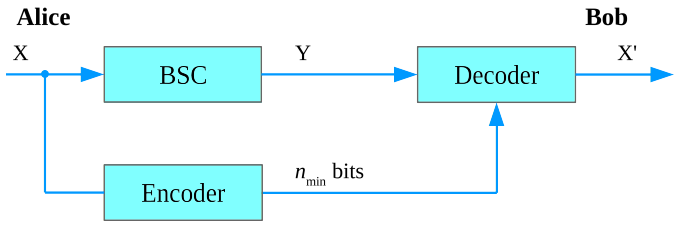


Figure 3.3. Principle of source coding with side information.

Bob to achieve non-zero secret key rates that would be impossible with one-way communication only [63]. Feedback is used to improve the secret key rate [52].

3.6 Information Reconciliation

Let us now assume that Alice has a sequence of bits x of length n and Bob has a possibly erroneous version y. Even without knowing Bob's codeword, Alice can send some information to Bob through the error free channel, so that Bob can correct his errors. This problem can be seen as an example of *source coding with side information* as illustrated in Fig. 3.3, where X is the source, Y is the side information the decoder has and $n_{\min}$ is the amount of error correction information that Alice sends to Bob.

The Slepian-Wolf Theorem [65] considers lossless compression of two correlated data streams, which is a form of distributed source coding (DSC) problem [65]. As a special case, Slepian-Wolf also considers the question of source coding with side information. Let us assume that X is length n i.i.d random binary sequence and Y its image received through a binary symmetric channel (BSC). Slepian-Wolf theorem then tells us that if the decoder knows Y perfectly then given any ϵ there exists an n_0 such that for all $n > n_0$ we only need to send $H(X|Y)$ bits to the decoder so that it can recover X with error probability less than ϵ. This can be achieved even when the encoder does not know Y, but only the transition probability between X and Y. In the case where X is i.i.d with equal probabilities for 1 and 0, we have that $H(X|Y) = nh(p)$, where h is the binary entropy function and p is the transition probability

$$h(p) = -p \log_2 p - (1-p) \log_2 (1-p) \, . \tag{3.7}$$

When we let n become arbitrarily large, the probability that all errors in Bob's word will be corrected with $n_{\min} = nh(p)$ bits will approach 1. Hence, if Y' is Bob's random sequence after the error correction, then $P(X \neq Y')$ can be pushed arbitrarily close to zero.

3.7 Privacy Amplification

After the information reconciliation phase the errors in Bob's key string are corrected or Alice and Bob have otherwise obtained a common key string. However, the key string cannot be used as a secret key before Eve's information about that key string is removed. Privacy amplification is used to distil secret shared information from a larger, partially secret body of shared information [66, 62]. Alice and Bob have a random variable W, an n-bit string of which Eve knows a correlated random variable V. Eve knows at most $t < n$ bits of information about W, i.e. $H(W|V) \geq n - t$. The probability distribution P_{WV} is usually not known to Alice and Bob, but they may know P_W. Classical privacy amplification was first introduced by Bennet, Brassard and Robert [67] and further analysed in [66]. The privacy amplification is performed using either universal hash functions or randomness extractors [67, 66, 68, 69].

3.7.1 Universal Hash Functions

Alice and Bob can use a universal hash function $g : \{0,1\}^n \rightarrow \{0,1\}^r$ where $n > r$ from a class $\mathcal{G}$ of functions to produce a secret key $K = g(W)$ of which Eve should have as little information as possible, given V and the choice of g [62, pp.40-41].

Given two finite sets $\mathcal{A}$ and $\mathcal{B}$, a class $\mathcal{G}$ of functions $\mathcal{A} \rightarrow \mathcal{B}$ is universal if for any distinct x_1 and x_2 in $\mathcal{A}$, the probability that $g(x_1) = g(x_2)$ is at most $1/|\mathcal{B}|$ when g is chosen uniformly at random from $\mathcal{G}$ [70]. Furthermore, the notation *2-universal* is used to emphasize that this definition constrains the behaviour of class $\mathcal{G}$ to only *pairs* of elements of $\mathcal{A}$ [70]. For example $\mathcal{A} = GF(2)^m$ and $\mathcal{B} = GF(2)^n$ where $m > n$ $\mathcal{G}$ is the space of all linear mappings between $\mathcal{A}$ and $\mathcal{B}$.

3.7.2 Randomness Extractors

A randomness extractor is a function that generates a highly random and independent output U from a partially secret source X of length n together with a short uniformly distributed random string Y of length d [68, 71].

A function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ is a strong (k, ϵ)-extractor if for every X with minimum entropy k and independent and uniform random string Y on $\{0,1\}^d$ [69, Definition 1.2],

$$(\mathsf{Ext}(X, Y), Y) \approx_\epsilon (U_m, Y) \; . \tag{3.8}$$

Even if Eve learns Y, the output of the strong extractor is close to uniform [69].

3.8 One-way and Two-way protocols

A *one-way protocol* begins with an error correction phase. At the beginning Alice has a length L bit vector x and Bob has a possibly erroneous version y of x. Alice and Bob then communicate through an authenticated and error free channel, correcting the errors in Bob's vector y. Eve can listen, but not alter, this communication. After the error correction phase, Bob's codeword can be modelled as a random sequence Y', where $P(X \neq Y') < \epsilon$, for some predetermined ϵ. Based on the observed error probabilities and the amount of information leaked during the error correction phase, Alice and Bob can now estimate how much information Eve has of X. In order to erase this information Alice and Bob execute a privacy amplification protocol. They use a randomly selected *2-universal* hash function [50, p.88], to map their sequences X and Y' to length L_{fin} bit-sequences K and K', where K is a binary i.i.d sequence with equal probabilities of 1 and 0. The probability density function after the error correction and privacy amplification protocols is $p'(K, K', Z')$. Here Z' represents Eve's original random variable Z and all the additional data she has managed to acquire during the execution of the error correction and privacy amplification protocols, including the choice of the hash function. The constant L_{fin} was selected such that $I(K; Z') < \epsilon$.

A key distribution protocol achieves a key rate S if for every ϵ we can find $L(\epsilon)$ so that for all $L > L(\epsilon)$ we have that

$$\begin{aligned} P(K \neq K') &< \epsilon\,, \\ I(K; Z') &< \epsilon\,, \text{ and} \\ \frac{n_{fin}}{n} &\geq S - \epsilon\,. \end{aligned} \tag{3.9}$$

The secret key rate of a *two-way protocol* is defined similarly, but the process does not begin with an error correction phase. Instead, Alice and Bob use two-way classical communication and agree on keywords k and k' so that the corresponding random variables satisfy

$$\begin{aligned} P(K \neq K') &< \epsilon\,, \\ I(K; Z') &< \epsilon\,, \text{ and} \\ I(K'; Z') &< \epsilon\,. \end{aligned} \tag{3.10}$$

General upper and lower bounds for a secret key rate are given by ([72, Lemma 1] and [63, Theorem 2]). This definition corresponds to the *strong secrecy* key rate. Remarkably, weak and strong secrecy are equivalent under two-way communication [73]. For any finite probability distribution

$P(X, Y, Z)$ we have the secret key rate bounds

$$\begin{aligned} I(X;Y) - \min(I(X;Z), I(Y;Z)) &\leq S(Z;Y|Z) \\ &\leq \min(I(X;Y), I(X;Y|Z)) \ . \end{aligned} \tag{3.11}$$

Here the lower bound is a result of one-way communication. However, the achievable key rates for two-way protocols seem to be less well-known.

3.9 Satellite Setting

The satellite setting [63] is an example of the *source model* secret key agreement method [52], where a source is broadcasting a signal in the form of a sequence of uniformly distributed random bits U. This is a method of secret key agreement using two-way communication over a public channel, starting from some correlated information [74, 63]. Alice, Bob, and Eve receive these bits through three independent BSCs C_A, C_B and C_E, with corresponding error probabilities ϵ_A, ϵ_B, and ϵ_E [63]. The error probabilities depend on the quality of reception and while Alice and Bob may have fixed sized antennas, nothing prevents Eve having a better antenna than Alice or Bob. Therefore, Eve's error probability ϵ_E may be much lower than Alice's or Bob's error probabilities. Even if Eve's channel is better originally than Alice's or Bob's, they can use *advantage distillation* to concentrate only on those bits that they both received reliably and throwing away the rest. The parity-check protocol (PCP) by Maurer is one such protocol using the advantage distillation method to collect secret key [63, 72].

In order to get meaningful results, one has to assume that Eve's resources are somehow limited, and she cannot receive the bits from the satellite without errors [72]. It is also assumed that Eve is a passive adversary. She cannot alter the bits that Alice and Bob are receiving, and she cannot tamper with their communication. If Alice and Bob start with a short shared secret key, they can authenticate their communication and prevent Eve from interfering [72]. The satellite setting is illustrated in Fig. 3.4 showing the independent channels from the satellite to Alice, Bob, and Eve and the public channel between Alice and Bob.

Let X be Alice's bit string, Y Bob's, and Z is Eve's bit string received through the channels C_A, C_B and C_E, respectively. The probability distribution $P_{X_i Y_i Z_i}$ is defined in [63] as

$$P_{X_i Y_i Z_i|U} = P_{X_i|U} \ P_{Y_i|U} \ P_{Z_i|U}, \tag{3.12}$$

where

$$P_{X_i|U}(x,u) \ = \begin{cases} 1-\epsilon_A, & \text{if } \ x = u \\ \epsilon_A, & \text{otherwise}, \end{cases}$$

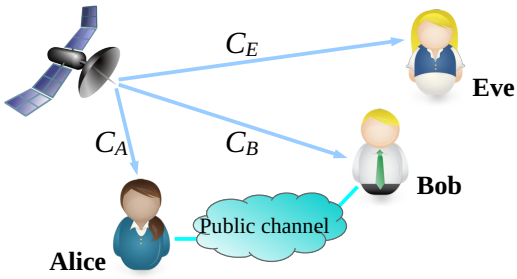


Figure 3.4. Principle of satellite setting showing three independent channels from the satellite source and an untamperable public channel between legitimate users.

$$P_{Y_i|U}(y,u) = \begin{cases} 1-\epsilon_B, & \text{if } y=u \\ \epsilon_B, & \text{otherwise,} \end{cases}$$

$$P_{Z_i|U}(z,u) = \begin{cases} 1-\epsilon_E, & \text{if } z=u \\ \epsilon_E, & \text{otherwise.} \end{cases}$$

Due to the independence of the channels C_A, C_B and C_E, the knowledge of the positions of bits reliably received by Alice and Bob does not give Eve any information about the values of these bits [63].

Following [63], after N consecutive uses of the satellite channel Alice has a length N i.i.d binary sequence with equal probabilities for 1's and 0's and Bob's sequence Y is X received through a BSC with crossover probability

$$\beta = \epsilon_A(1-\epsilon_B) + (1-\epsilon_A)\epsilon_B \ . \tag{3.13}$$

The random variables of Alice, Bob and Eve then satisfy the following conditions:

1. X is a random sequence with i.i.d binary random variables with equal probabilities for 1 and 0,
2. Random sequence Y corresponds to X received through a BSC with transition probability β,
3. Z is a sequence of independent identical random variables and for every x, y and z, $P(x,y,z) = \prod_{i=1}^{n} P(x_i,y_i,z_i)$, and
4. For every coordinate i of X, Y and Z the corresponding pdfs $P(X_i,Y_i,Z_i)$ are identical.

3.10 Quantum Key Distribution

In QKD Alice and Bob try to generate a shared secret key using a private quantum channel and an authenticated error free classical channel as

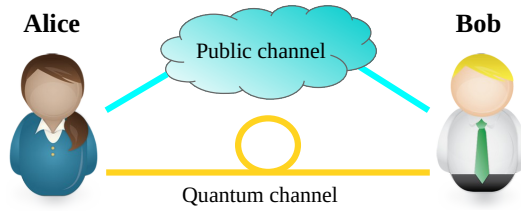


Figure 3.5. Channels between Alice and Bob in quantum key distribution.

illustrated in Fig.3.5, while Eve is eavesdropping both of these channels. The aim is to generate the keys of a priori unknown bits in absolute secrecy. The security is guaranteed by laws of nature, not based on the hypothesis on problem hardness [62, p.14]. The security in QKD is based on collapsing the wave function during a measurement, and the no-cloning theorem [62, p.13]. In order to get hold on the information, one has to make a measurement. The no-cloning theorem states that an unknown quantum state cannot be cloned and then measured. Therefore, if Eve wants to spy on the quantum channel, she has to make measurements, and doing so she inevitably collapses the measured wave functions. The stages in QKD are:

1. generate raw keys
2. sifting phase, Alice and Bob agree on common measurement base
3. information reconciliation, discussed in Section 3.6
4. privacy amplification, discussed in Section 3.7

In the first, and most used, QKD protocol BB84 named after the authors Bennet and Brassard [75], Alice generates a random bit sequence and sends it to Bob through the quantum channel. Eve may perform quantum attacks on this communication. There are other similar protocols such as the Ekert protocol [76], the B92 [77], the six-state protocol [78], and the SARG protocol [79]. For this work, the BB84 key arrangement protocol is of interest because it is a well-tested, robust and well-established protocol, and there are several commercial products using the BB84 protocol [80, 81].

3.10.1 BB84 Protocol

At the beginning of the BB84 protocol, Alice measures the polarizations of n photons in a randomly selected base, rectilinear ($\updownarrow$, $\leftrightarrow$) or diagonal ($\nwarrow\!\!\searrow$, $\swarrow\!\!\nearrow$) and sends the photons to Bob. Bob measures the polarization of each received photon in a randomly selected base. If Bob measures a photon in the same basis as Alice, Bob gets the same result as Alice, otherwise the result is random. These steps are illustrated in Table 3.1. Alice and Bob

Table 3.1. BB84 protocol steps, starting from raw key and ending up to sifted key bits.

Alice's polarization	↔	↙↗	↙↗	↕	↔	↖↘	↕	↕	↖↘	↕
Alice's bits	1	0	0	0	1	1	0	1	1	0
Bob's polarization	↔	↔	↕	↕	↖↘	↖↘	↕	↖↘	↖↘	↕
Bob's bits	1	1	0	0	1	1	0	1	1	0
Basis	✓	×	×	✓	×	✓	✓	×	✓	✓
Sifted key	1			0		1	0		1	0

then compare the basis they have chosen and discard the measurements that were done in a different basis. This step is called *sifting phase*. Alice and Bob can now form an estimate for the QBER between their bit strings, e.g. comparing some number of sifted bits in public and discarding them afterwards. Based on the nature of the quantum channel and the estimated QBER, Alice and Bob can estimate how much information Eve has gained during the quantum phase. Using this knowledge and their corresponding bit strings Alice and Bob will use the classical authenticated channel to generate a shared secret key of which Eve should have very little information.

A number of effective key generation protocols and error correction algorithms to be used with BB84 have been developed [82, 83, 84, 85, 86]. Most schemes belong to the category of one-way protocols, which are used in most practical applications. A one-way protocol takes Alice's sifted bit string as a raw key and the differences in Bob's sifted bit string are corrected as the protocol is run. In principle, only one-way communication is needed for error correction and key distillation in these protocols. While protocols like CASCADE [87] do use two-way classical communication they are still logically one-way protocols as the aim is to correct the errors in Bob's bit string. In a two-way protocol, instead of correcting the errors in Bob's sifted key, Alice and Bob agree on a common bit string based on message exchanges using two-way post-processing.

3.10.2 Attack Models in Quantum Key Distribution

Finding protocols with a high secret key rate is one of the primary problems in QKD. The secret key rate of a given protocol may depend on the model we use for Eve's attacks on the quantum channel. Typically, the more general attacks we assume, the lower the achievable secret key rate is going to be. However, as the set of all possible attacks is hard to analyse, it is common to divide the attacks into three classes [82, 86]:

- individual attacks,
- collective attacks, and

- coherent attacks.

The smallest class contains individual attacks, where Eve is only interacting separately with each of the quantum bits sent by Alice. If Eve is allowed to wait with her measurements until the protocol has ended, the attack belongs to the collective attacks class. Coherent attacks constitute the most general class of attacks. This class includes all attacks allowed by the laws of quantum physics [86]. For any QKD protocol the final goal is to provide key rate guarantees under the assumption that Eve can perform coherent attacks.

3.10.3 Key Rates

Unlike in the case of classical communication channels much is unknown about the achievable key rates of QKD protocols assuming coherent quantum attacks, even the exact achievable key rate of one-way algorithms is not known. The best known lower bound is given in [88]. Assuming that we can also perform classical pre-processing, the highest reported key rate is given in [86]. The key rate of all one-way protocols is upper bounded by a general information-theoretic bound [89, p.184]. This bound also proves that no one-way protocol can produce secret key beyond QBER 14.6%.

The performance of two-way protocols is not limited by these key rate bounds. In particular a number of works [90, 91, 92] have considered the problem of extending the QBER region by using two-way post-processing. In [91] and [92] the authors demonstrate that a two-way protocol can achieve a positive key rate even when QBER is 20%. However, when the QBER is low these protocols have a very low key rate, which hinders their applicability for practical QKD.

Only a few work on two-way protocols have concentrated on maximizing the key rate for the whole range of QBERs, including small values. In [93], the authors demonstrate a two-way protocol that achieves a higher key rate than the best one-way protocol [86]. However, the improvement in the key rate is moderate, and does not break the one-way protocol bound [89] at low QBER. In general, the achievable key rate of the best possible two-way protocol is not known [82].

4. Wireless Channel as a Source of Randomness

4.1 Introduction

It is difficult to shield transmitted signals from unintended recipients due to the broadcast nature of wireless communications, making them less secure than systems using wired communications [13]. In wired communications a physical connection to the wires, or a very close one, is required for an eavesdropper to succeed in overhearing the communication. A wireless transmission can be heard within the coverage area of the transmitter [15].

Traditional security schemes are based on public key cryptography or public key infrastructure (PKI) to support confidentiality, data integrity and authentication [8, 9, 10]. Public key cryptographic methods are asymmetric as they use a public key to encrypt messages and a private key to decrypt them [11]. Asymmetric cryptography has high energy and implementation costs, as these methods rely on computational hardness to provide security [12, 9]. As wireless IoT devices are often limited in electrical and computational power, this makes it difficult to implement and use complex security methods [2].

A symmetric encryption method uses the same key for encryption and decryption. Considering the limitations in electrical and computational power, symmetric encryption methods are preferred, but this raises the question of key distribution [13]. It is not practical to preconfigure the keys, for example at the time of manufacturing the devices. Dynamic updating and pairing devices and keys requires a trusted third party to operate the key distribution [12]. Instead of using a fixed infrastructure for key distribution, it would be more practical to generate the keys automatically when needed [8, 12]. The radio channel between two wireless devices can be used to provide the basis for creating a shared secret for the devices [8, 94, 15, 95, 96, 9, 97, 98, 10, 13, 12, 2]. As wireless channels change in time, exploiting the randomness of the fading channel provides information-

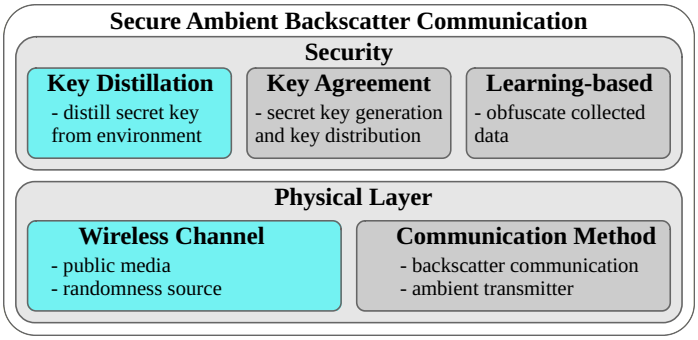


Figure 4.1. Secret key distillation using wireless channel as a source of randomness.

theoretic security [15, 9, 2], as discussed in Section 3.3.

The raw key material from which the final secret key is obtained, is based on measuring the channel response between the users and then extracting secret bits from the measurements. The information for creating secret keys is extracted from random spatial and temporal variations of the reciprocal wireless channel [10]. On the other hand, the same randomness of the radio channel also limits the information that an eavesdropper can get at the bit level, even if the eavesdropper has unlimited computational power [9, 13]. In addition to using the wireless channel as to be the source of the secret key, the problem of key distribution is also solved and the keys can be renewed as needed [97]. In Fig. 4.1 the use of a wireless channel as a source of randomness and the key distillation procedure are shown in the scope of securing ambient backscatter communication.

A notable exception for using public key cryptography to produce and distribute secret keys is QKD [95, 96, 10], and Section 3.10. In QKD, the non-orthogonal states of a quantum system provide the correlated observations of randomness for end users [96]. The wireless fading channel provides another comparable source of secrecy that can be used to provide information-theoretically secure keys [99, 96].

4.2 Fading Wireless Channel

The wireless environment with multipath propagation is typical in wireless scenarios and is characterized by a fading channel response. Relative movement between the user equipment and the environment leads to random amplitude and phase fluctuations of the received signal [96, 9]. The radio channel acts as a time and space-varying filter. The filter's response at any point in time is the same from location A to location B, and vice versa [95, 10]. The short term fading process is hard to predict and is best modelled stochastically [96].

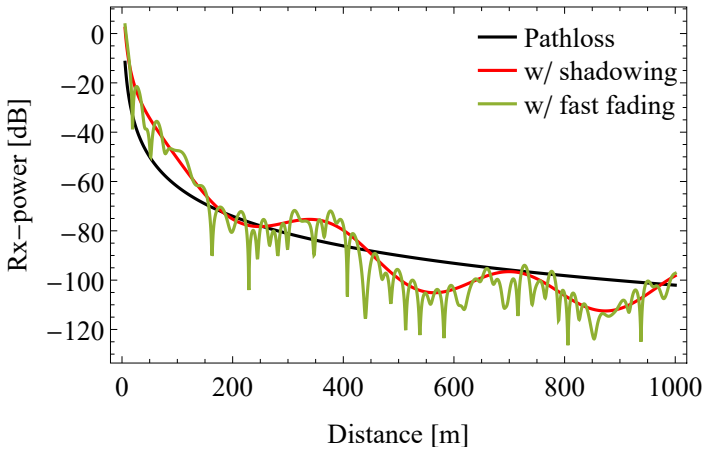


Figure 4.2. An example of wireless channel fading response.

An example of a wireless channel fading response as a function of distance is presented in Fig. 4.2 when the user is moving away from the transmitter. The figure is showing the three main components affecting the channel's fading process [100, Ch. 4.2]:

- path loss,
- shadowing, and
- fast fading.

Path loss represents the attenuation of the received signal as the distance from the transmitter increases. In free space, the attenuation is proportional to the square of distance and the more large scale obstacles there are between the transmitter and the receiver causing reflections, absorption, and scattering, the larger the path loss exponent gets [101, Ch. 3.2].

Shadowing shows the long-term fluctuations in the received signal level. These fluctuations are caused by signals reflected or scattered from the environment, e.g. buildings or terrain, and thus forming separate signal paths from the transmitter to the receiver [100, Ch. 4.2].

Fast fading is a similar phenomenon to shadowing and is caused largely by the same mechanisms, but the time interval is much shorter. A zoomed out portion of the wireless channel fading response is shown in Fig. 4.3, where the nature of fast fading is clearly visible. The received signal level changes rapidly and there can be very large changes in the received signal power, as much as 30 to 40 dB [101, Ch. 3.1].

The security of using the physical layer as a source of random bits relies on the reciprocity principle. The channel is unique between communicating parties as the multipath propagations are highly correlated, symmetric and sufficiently random in their nature [8, 94, 12, 2]. The legitimate users can obtain strongly correlated channel measurements, and since the

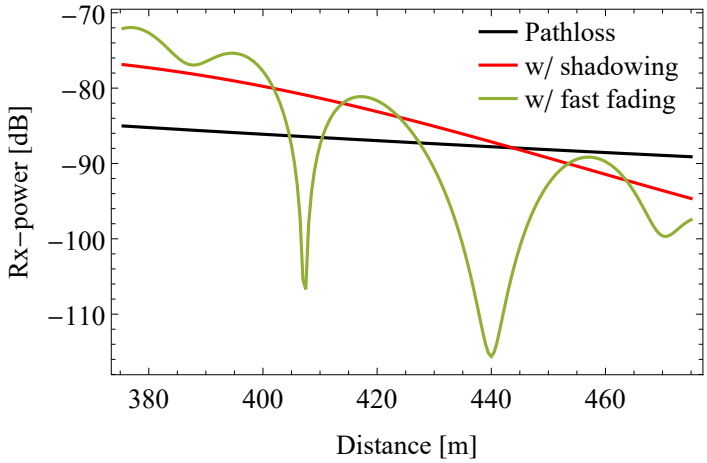


Figure 4.3. A zoomed portion from example wireless channel fading response [PV].

channel fluctuations are spatially specific in multipath radio environments, an eavesdropper cannot get similar channel responses [99, 94, 102, 2]. In multipath-rich environment, channel responses are rapidly decorrelating both in time and space [15].

The three basic properties of fading wireless channels that are utilized as basis for key generation are temporal variation, spatial variation, and channel reciprocity [95, 9]. Based on these properties, several methods are proposed and used to extract bits from wireless channels for secret key generation. Patwari *et al.* [95] lists the following methods:

- send two nonmodulated continuous wave signals in both directions and measure phase differences,
- measure time delay and gain from the channel,
- measure the channel's impulse response,
- estimate channel gains and delays from narrowband cellular signals,
- measure amplitude or channel gain, and
- measure angle-of-arrival.

The most common method is to use the amplitude or channel gain as a source for key generation, as amplitude or received power is relatively easy to measure. The angle-of-arrival is not reciprocal itself, but the channel gain can be measured with steerable antennas [95].

It should be noted that while the radio channel is reciprocal, the measurements are not. The main reasons are [95]:

- different additive noise at the endpoints,
- different transceiver hardware at the endpoints, even if they are the same make and model, causing e.g. gain variations
- measurements at both ends are not typically simultaneous, and
- interference power at the endpoints is not symmetrical.

Therefore, the measurements at the endpoints of a wireless channel are not exactly the same.

An exception to this channel model is presented in [103] where two wireless devices measure the signal originating from an ambient transmitter, such as a local TV broadcast. Now there is no reciprocal channel between the devices, but if the devices are close to each other, the channels from the ambient transmitter to the devices are correlated and the measurements can be used as a source of randomness. Given ambient signal carrier wavelength λ, [103] assumes the devices to be located within 0.1λ distance from each other, and the eavesdropper needs to be at least 0.4λ away from either one of the legitimate devices in order to reliably derive a secret key.

4.3 Channel Measurements

To make use of the most common bit extraction method from Section 4.2, measuring the amplitude or channel gain, the received signal strength indicator (RSSI) value measurements are used for generating secret keys [9, 10]. For example, Alice sends a probe to Bob and Bob sends immediately an acknowledgement back to Alice. In general, probes and acknowledgements are just packets that the users are sending to each other and are measuring the RSSI values of those packets [10, 98]. The basic steps taken when using RSSI values are [9]:

- probing the channel, i.e. measure RSSI,
- use some method to quantize RSSI values and convert them to bits, and
- use error correction to obtain a shared key.

As the wireless environment is changing continuously, providing the necessary randomness, there is a *channel coherence time* during which the channel does not change significantly. As an example, in Fig. 4.3 the channel stays relatively stable in the timescale of moving a few metres, between large changes in the received signal power caused by the fast

fading phenomenon. The coherence time window makes it possible to obtain correlated measurements [9]. The coherence time T_{c}

$$T_{\mathrm{c}} \sim \frac{1}{f_m} \,, \tag{4.1}$$

where $f_m = \frac{v \cdot f_c}{c}$, c is the speed of light, v is the speed of the user and f_c is the centre frequency of the transmitter [101, Eqn. 4.40.a]. Equation (4.1) suggests a time duration during which the channel is essentially invariant [101]. The extracted bits need to be separated in time by at least a coherence time interval (4.1) to ensure that successive bits are almost independent [8]. Therefore, extracting bits from channel measurement at a rate that is greater than $1/T_{\mathrm{c}}$ cannot produce random bits. Short coherence time yields high randomness and e.g. vehicular environments usually have very short channel coherence times [98]. Therefore, the packets that are used for channel measurements should be small so that the users have time to send the packets and make measurements inside the coherence time window. However, these continuous changes in channel properties makes it harder for an eavesdropper to experience the same RSSI variations [10].

The mean RSSI value needs to be filtered out of the measured RSSI values, as the mean is closely related to the distance between users, corresponding the path loss component shown in Fig. 4.2. Otherwise, an eavesdropper could use the knowledge of the distance between users to predict parts of the secret key [10]. The RSSI values are easily available, but they are not a very accurate means to characterize channel properties [98]. The use of RSSI measurements usually leads to quite low key rates [9]. If the bit-rate requirements are low, the key generation procedure can piggyback channel sampling during normal communications, thus saving energy and computations [12]. In order to produce a secure key, the elimination of dependency among measured samples is a crucial step. Correlation between measurements leads to correlation between bits in the secret key [95, 98].

The key rate starts to suffer, if there is mismatch between Alice and Bob's measurements, decreasing the correlation between their raw key bits. The time delay between measurements is the dominant source of the observed channel mismatch [12]. As many wireless transceivers are half duplex, this immediately leads to sampling delay and will decrease the mutual information between Alice and Bob [102]. The key generation is also limited in slowly varying wireless environments [97] and in general the secret key generation does not work in free space, i.e. there is no multipath propagation [95].

4.4 Quantization

A quantizer is used to convert the measured RSSI values to bits, which are further processed to obtain the secret key. The RSSI measurements for Alice and Bob are $X = (x_1, x_2, ..., x_n)$ and $Y = (y_1, y_2, ..., y_n)$. X and Y are called raw data or raw readings [98]. Each reading of X is mapped to a temporary bit using level crossing quantizer Q [96]

$$Q(x) = \begin{cases} 1, & \text{if } x > q_+ \\ 0, & \text{if } x < q_- \\ e, & \text{otherwise.} \end{cases} \tag{4.2}$$

The thresholds q_+ and q_- are adaptive

$$\begin{aligned} q_+ &= \text{mean}(X^n) + \alpha \cdot \sigma(X^n) \\ q_- &= \text{mean}(X^n) - \alpha \cdot \sigma(X^n) \,, \end{aligned} \tag{4.3}$$

where $\alpha \geq 0.2$ and estimates between q_+ and q_- are dropped [96, 10]. The quantizer is applied to blocks, their size n being an adjustable parameter. Alice and Bob can use those values they both quantized to bits, discarding positions where either one of them got an e. The level crossing method does not necessarily produce a random bit string [98].

Alice and Bob can also identify excursions in temporary bits, e.g. find the locations of three bits that are the same. Then the positions of excursions are shared between Alice and Bob, and each common excursion is encoded to a bit [98].

However, the simple level crossing method produces only one bit per raw data reading. More bits per one raw data reading is produced when using multilevel quantization. An equiprobable quantizer is introduced in [99] where all outputs from the quantizer are equally probable. The quantizer takes a unit-variance Gaussian distribution and divides it into intervals $(-\infty, \bar{q}_1], (\bar{q}_1, \bar{q}_2], \ldots, (\bar{q}_{i-1}, \infty)$, where $\bar{q}_i$ is determined as [99]

$$\int_{-\infty}^{\bar{q}_i} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx = \frac{i}{v} \,, \tag{4.4}$$

where i is the interval and v is the total number of intervals. For variance σ and mean μ the general quantizer function reads

$$Q(x) = \int_{-\infty}^{\bar{q}_i} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} dx = \frac{1}{2}\text{erf}\left(\frac{x-\mu}{\sigma\sqrt{2}}\right) \tag{4.5}$$

A more elaborate quantization method, multibit adaptive quantization (MAQ) [95], takes real valued channel measurements and converts them to bits. This quantization scheme needs to be agreed between the users, necessitating communication before the measured values can be converted to bits.

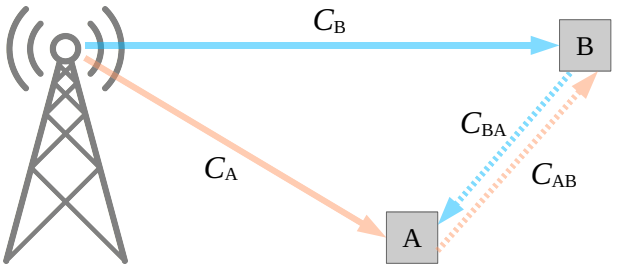


Figure 4.4. Channel construction between two backscatter devices. Ambient transmitter on the left and two backscatter devices on the right.

The bit strings Alice and Bob collected from RSSI values are not necessarily the same and it is also possible that an eavesdropper has some information about the bits. As discussed in sections 3.6 and 3.7, information reconciliation and privacy amplification procedures are needed before the bits can be used as a secret key.

4.5 Key Generation in AmBC Setting

The aforementioned key generation schemes rely on two communicating parties sending probing signals to each other, and measuring channel responses. In AmBC, and backscatter systems in general, the backscatter devices cannot directly estimate the channel between devices. The channel between two backscatter devices consists of two sections. The first section is from the ambient transmitter to the backscatter device and the second section is from one device to another. In Fig. 4.4, the channel from the ambient transmitter to backscatter device A is labelled C_{A}, and the channel from device A to device B is labelled C_{AB}. Correspondingly, the channels for device B are C_{B} and C_{BA}.

Therefore, it is a challenge to use existing physical layer security methods in AmBC systems, especially in case of D2D communications [104, 2]. The channels C_{A} and C_{B} from the ambient transmitter to backscatter devices are not identical, and therefore the channels between two backscatter devices are not reciprocal. This makes it difficult to use the channels C_{AB} and C_{BA} as a shared randomness source [2]. As a solution, authors in [2] proposed a method to estimate the channel between two backscatter devices that is based on the observation that the channel between devices is one side of a triangle formed by the ambient transmitter and two backscatter devices. The proposed method constructs the multiplication of three channels as a source of shared randomness.

5. Ambient Backscatter Device Design

5.1 Introduction

The motivation to develop and make the first backscatter modulator, the *reflective backscatter modulator*, was to have a versatile and reliable device that could be utilized in different use cases. Several backscatter modulators of this type were manufactured for use in **Publications I** and **IV**. This modulator is based on known principles: a switch element selects from two different impedances as discussed in Section 2.3 and [17]. The goal was to make the backscatter modulator easy to use and to cover a wide frequency range. A design decision was to match the impedance of the modulator to $50\ \Omega$ and use a common SMA connector to make changing antenna, and thus operating frequency as easy as possible. The use of this modulator also helped to better understand the backscatter setting, as AmBC was a relatively new research area.

The second backscatter modulator, the *polarization conversion based modulator*, and the corresponding analogue receiver front end circuitry is original research presented in **Publication III**. The modulator and the receiver circuitry was developed based on the insight that was gathered during the use of the first modulator in different use cases. The objective for developing this backscatter modulator was to mitigate the direct path interference from the ambient transmitter. The same modulator concept is used in **Publication VI** as a building block for securing ambient backscatter communication.

5.2 Reflective Backscatter Modulator

A reflective backscatter modulator that uses a diode as a current controlled switch was used in **Publications I** and **IV**. This modulator follows the principles discussed in Chapter 2.3. The schematic drawing of the modu-

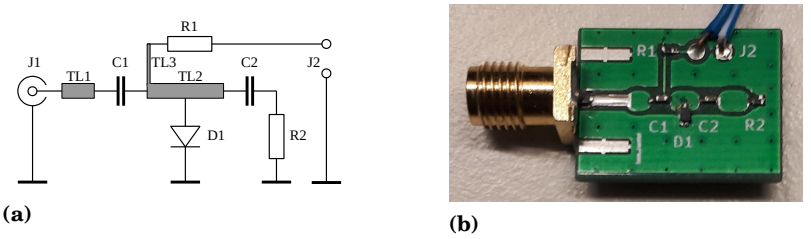


Figure 5.1. Reflective backscatter modulator: a) The schematic drawing, and b) circuit board [PI].

lator is shown in Fig. 5.1, part(a) and the corresponding circuit board is shown in Fig. 5.1, part (b). The antenna is connected to the SMA connector J1 and the modulating data signal is connected to connector J2. On the circuit board, the blue and blue-white wires are soldered in place of connector J2. The nominal impedance of the modulator is $50\ \Omega$, and the transmission lines TL1 and TL2 are matched to that impedance. The switching diode D1 is directly connected to TL2 and the current controlling the ON and OFF states of the diode is brought through a current limiting resistor R1 and a high impedance transmission line segment TL3. Capacitors C1 and C2 function as DC-blocking elements, preventing the control current flowing to the antenna or to the terminating resistor R2. The diode's ON state corresponds to the modulator's reflecting state and the diode's OFF state corresponds to the modulator's non-reflecting state. This type of backscatter modulator does not have a specific working frequency, it operates over a wide frequency range. It is desirable that the difference between the reflecting and non-reflecting states to be as large as possible to maximize the modulation factor M as in (2.5).

The imperfections of the components used to make the modulator and the quality of the circuit board limits the working frequency range of the modulator. As the operating principle of this modulator is based on the diode's ability to make a short circuit or to stay completely open, the forward resistance R_f during the reflecting (ON) state and the diode capacitance C_T during the non-reflecting (OFF) state are the major properties that affect the modulator's performance. The diode used in the modulator is BAR88-02V from Infineon Technologies AG [105]. The values read from the data sheet are $R_\mathrm{f} = 0.2\ \Omega$ with 0.5 mA control current and $C_\mathrm{T} = 0.28$ pF. The input reflection coefficient S_{11} and modulation factor M calculated from these values are presented in Table 5.1 for frequencies used in **Publications I** and **IV**. Two other popular frequencies, 100 MHz and 2.45 GHz, are also listed in the same table for reference.

The S_{11} values measured with a vector network analyzer (VNA) are shown in Fig. 5.2 for both reflecting and non-reflecting states of the modulator from 25 MHz to 3.0 GHz. The values are averages of twelve backscatter modulators used in several experiments and research over several years.

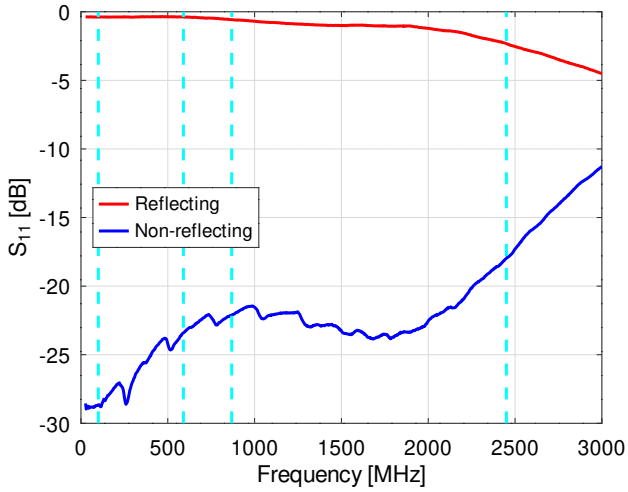


Figure 5.2. Average input reflection coefficient S_{11} for $n = 12$ modulators.

Table 5.1. Calculated values for input reflection coefficients and modulation factors with BAR88-02V switching diode at selected frequencies

Frequency	S_{11} Non-reflective	S_{11} Reflective	M
100 MHz	-46.9 dB	-0.70 dB	0.213
590 MHz	-31.7 dB	-0.70 dB	0.212
868 MHz	-28.4 dB	-0.70 dB	0.212
2.45 GHz	-19.4 dB	-0.70 dB	0.210

Numerical values for S_{11} and modulation factor M are presented in Table 5.2 for the same frequencies as in Table 5.1. All four frequencies are also marked with dashed lines in Fig. 5.2. At frequencies below 2 GHz, the proposed backscatter modulator works well, as the difference between reflecting and non-reflecting states is more than 20 dB.

The measured performance of the modulators reported in Table 5.2 corresponds well with the calculated results from Table 5.1. The non-reflecting state reflection coefficients are worse than the calculated ones, but the diode is not the only component contributing to the overall performance. There is a small impedance mismatch due to the connection of TL3 to TL2, and the capacitors C1 and C2 and the resistor R1 have their own parasitic inductances and capacitances that are causing small mismatches as well, and degrade the non-reflecting state performance. The measured S_{11} values for the reflecting state are better than the calculated ones, indicating that the forward resistance of the diode is actually smaller than the typical value given in the data sheet.

Table 5.2. Measured average input reflection coefficients and modulation factors at selected frequencies.

Frequency	S_{11} Non-reflective	S_{11} Reflective	M
100 MHz	-28.7 dB	-0.38 dB	0.212
590 MHz	-23.4 dB	-0.38 dB	0.198
868 MHz	-22.1 dB	-0.57 dB	0.184
2.45 GHz	-18.0 dB	-2.32 dB	0.102

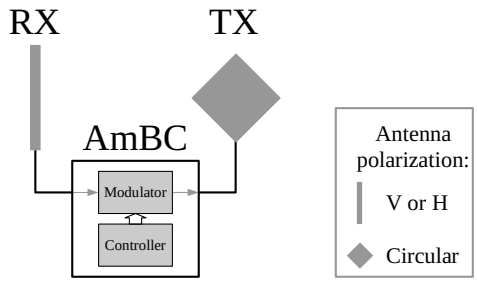


Figure 5.3. Polarization conversion based modulator [PIII].

5.3 Polarization Conversion Based Modulator

A backscatter modulator based on polarization conversion is developed in conjunction with a suitable antenna construction for the receiver in **Publication III**. A polarization conversion between the direct and scattered path signals is introduced at the backscatter modulator and exploited at the dual polarization receiver antenna to mitigate the direct path interference.

In the proposed design, the linearly polarized input antenna is connected to a circular polarized output antenna through a modulator. The operating principle of the backscatter device is shown in Fig. 5.3. The modulator is an RF switch and the controller can be e.g. a microcontroller. The RF switch is a non-reflective single pole double throw (SPDT) switch, also known as a change-over switch. As the modulation is realized by either connecting the two antennas together or isolating them from each other, the non-reflective construction of the RF switch helps to minimize unwanted backscattering when the antennas are not connected together. Without the non-reflecting construction, there is a possibility that the antennas are reflecting the incoming signal back uncontrollably. This would degrade the performance of the backscatter device by introducing a background backscattered signal.

It is possible that the modulated signal leaks back to the input antenna forming a loop back. However, there is a 3 dB attenuation due to the polarization mismatch between linear and circular polarizations and the insertion loss of the RF switch is added to the total attenuation of the loop causing the loop back signal to fade rapidly.

Table 5.3. Return and insertion loss values from data sheet and modulation factor for RF switch

Frequency	Return loss	Insertion loss	M
2.44 GHz	-18.0 dB	-1.0 dB	0.146

Table 5.4. Measured return and insertion loss values and modulation factor for RF switch

Frequency	Return loss	Insertion loss	M
2.44 GHz	-19.5 dB	-1.0 dB	0.154

The modulation factor for the polarization conversion modulator is calculated from (2.5). The non-reflecting and reflecting state reflection coefficients are calculated from the "Off State" return loss and the insertion loss values given in the data sheet [106]. The reported return loss and insertion loss values at 2.44 GHz and the resulting modulation factor M are presented in Table 5.3. The corresponding values measured with a VNA are presented in Table 5.4. The modulation factor is better than the one obtained using the reflective modulator at the same frequency.

The receiver has two circular polarized antennas, one receiving left-hand circular polarization (LHCP) and the other receiving right-hand circular polarization (RHCP). The signal from LHCP antenna is subtracted from the signal from RHCP antenna. As the modulator is only sending one circular polarization, say RHCP, the receiver then sees that signal because there is nothing to be subtracted. As the ambient signal is linear polarized and the power transfer ratio from linear to either circular polarization is 1/2, the ambient signal appears equally strong at both circular polarized antennas and gets cancelled. This is shown in the lower right corner of Fig. 5.4. The constant 1/2 in front of each power transfer ratio is due to the construction used in **Publication III** where the $180°$-hybrid doing the subtraction causes an additional 3 dB power loss. Under ideal circumstances, the proposed method completely removes the ambient signal, and in **Publication III** a 25 dB attenuation at 2.44 GHz was confirmed by measurements.

This modulator and receiver antenna construction is not frequency dependant in itself. It can be applied at different frequencies as long as there are suitable antennas and a $180°$-hybrid to do the subtraction of the signals coming from the LHCP and RHCP antennas. Figure 5.5 shows a prototype microstrip patch antenna and a $180°$-hybrid construction that was used in **Publication III**. The microstrip patch antenna is the square on the right side of the circuit board [107, pp.7-9]. The frequency sensitivity analysis in **Publication III** concerns this particular construction, but the underlying principle of DLI cancellation is applicable to other constructions as well. Figure 5.6 shows how the isolation decreases as the bandwidth

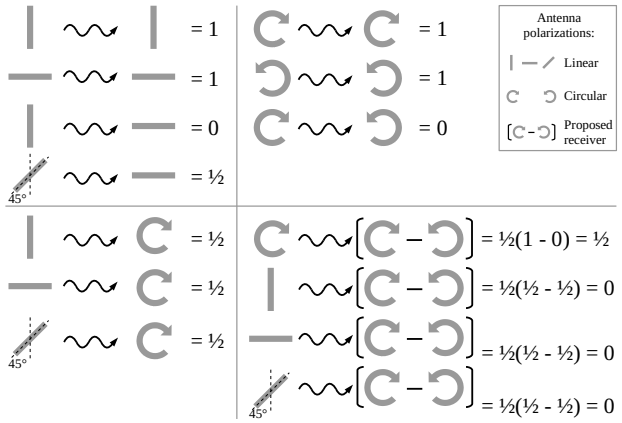


Figure 5.4. Power transfer between different antenna polarizations [PIII].

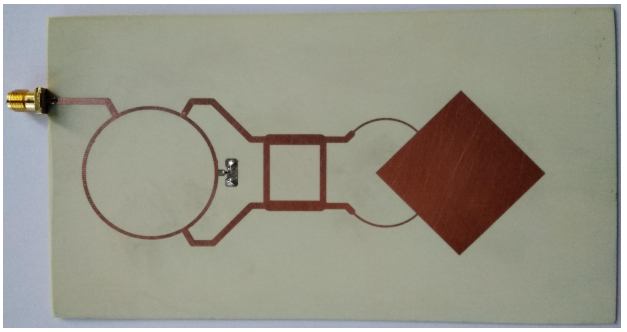


Figure 5.5. A prototype antenna construction for 2.44 GHz used at the receiver. [PIII].

of the signal is increased in comparison with the centre frequency. The bandwidth is expressed as a percentage value of the centre frequency. The proposed system offers more than 35 dB isolation between the ambient and backscattered signals if the signal bandwidth is less than one percent.

A drawback with microstrip patch antennas is the space required for them. The antenna dimensions are close to $\lambda/4$ and for lower frequencies the size of the resulting antenna might be a limiting factor. However, a number of other circular polarized antenna constructions are available, see e.g. Gao *et al.* [107].

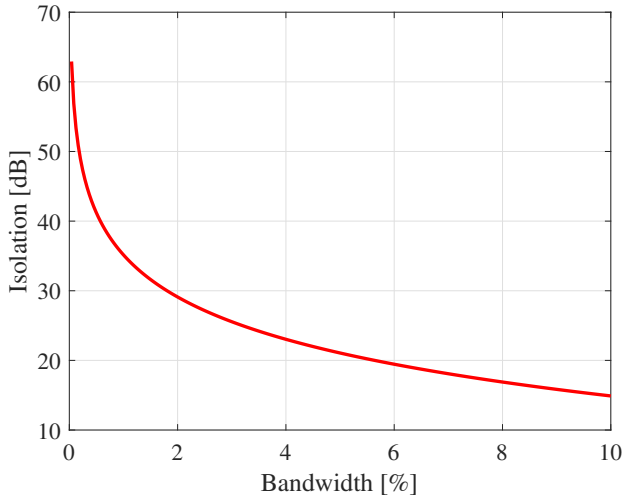


Figure 5.6. Isolation between ambient and backscattered signals vs. bandwidth percentage [PIII].

6. Two-way Protocol with Parity bit Reconciliation

6.1 Introduction

We proposed a novel secret key agreement protocol in **Publication II**. It belongs to the family of two-way protocols, as discussed in Section 3.8. The protocol uses an advantage distillation method from [74] and [90], as discussed in Section 3.5. We have named our protocol a Two-way Protocol with Parity bit Reconciliation (TPPR). A key agreement protocol is an essential building block towards secure AmBC, as shown in Fig. 6.1.

We have analysed the performance of our key agreement protocol in two different operating scenarios: in a QKD setting in **Publication II** and in a satellite setting in **Publication V**. The security of state-of-the-art key agreement protocols is usually analysed using either setting, therefore for the sake of generality, we have done the same. The QKD setting is discussed in Section 3.10 and the satellite setting is discussed in Section 3.9, correspondingly. The ambient backscatter scenario can be described in a generalized satellite setting, as is done in **Publication VI** and in Chapter 7. Although the protocol itself is the same, the underlying privacy

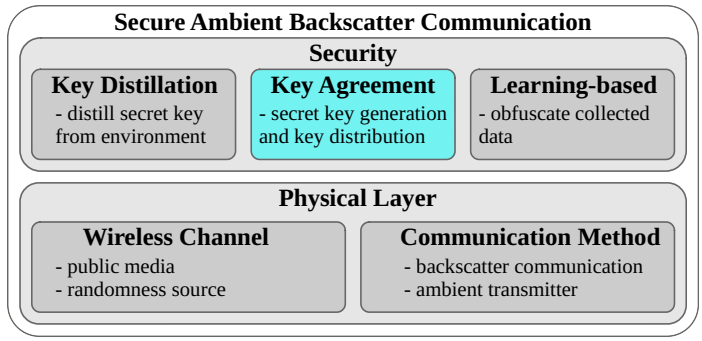


Figure 6.1. Secret key agreement protocol in the scope of secure AmBC.

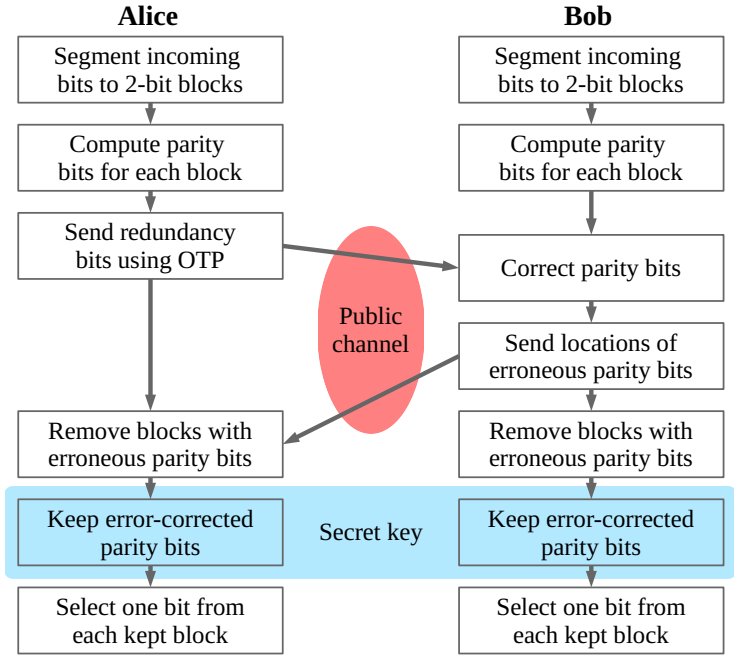


Figure 6.2. TPPR flow for one round.

amplification analysis differs drastically from each other, and accordingly the resulting key rates are also different. The protocol flow is discussed next, followed by the performance analyses of the different operating scenarios.

6.2 Secret Keys from Error Corrected Parity Bits

During each round of TPPR, Alice and Bob arbitrarily divide their bit strings into two-bit blocks, calculate parity bits for these blocks and where the parity bits differ, jointly discard those blocks. One bit from each remaining block will then be used as an input to the next round of the protocol. The flow of the protocol for one round and the actions taken by Alice and Bob are shown in Fig. 6.2.

Unlike in [74] and [90] the secret key is collected from error corrected parity bits and not from Alice's or Bob's original bit strings. The collection of the secret key is highlighted with a blue background in Fig. 6.2. Following [93] we use the knowledge that the parity bits between Alice and Bob are strongly correlated and Alice only needs to send sufficient information to Bob that he can correct his parity bits. This data is transmitted through the public channel encrypted with an OTP by using previously collected secret key. Bob then informs Alice of the locations of erroneous parity

bits. The two-way public channel is highlighted with a red background in Fig. 6.2. The secret key is then a concatenation of the error corrected parity bits collected during each round.

The secret key has to be shortened using privacy amplification protocol to remove Eve's knowledge before it can be used in any cryptographic application. Privacy amplification is discussed in Section 3.7.

6.3 TPPR in the QKD Setting

We assume the well-known BB84 QKD protocol [75], discussed in Section 3.10.1, where Alice and Bob share a quantum channel and an authenticated error free public channel. Alice creates a random string of bits, encodes them on the polarization of photons by randomly using two different coding bases and sends them to Bob. During the transmission, Eve will attack the transmitted bits using a quantum attack. We assume that Eve attacks each of the bits individually, and always by the same method, the method which is freely chosen by Eve [82, p.1322].

After the sifting phase, Eve performs her measurements on the wire-tapped photons. As mentioned Eve's attack here is always the same, but only in a probabilistic sense, where with certain probability p_1 Eve can perform attack 1, with probability p_2 attack 2, and so on. However, this selection of attacks and corresponding probabilities are assumed to be fixed during the quantum communication.

After Eve's measurement, the whole system can be modelled in terms of classical random variables and a probability density function (pdf) $p(X, Y, Z)$ [50, p.205]. Here X refers to Alice's bit string, Y to Bob's and Z represents Eve's measurement results and possible side information. It is expected that Eve completely knows this density function, while Alice and Bob only know the QBER p.

In the QKD setting TPPR consists of recursive iterations of the parity bit reconciliation block from Fig.6.2. The input of the jth iteration of the block consists of a fraction f_{in}^j of the N_{sif} sifted bits. The bit error rate between Alice and Bob is known to be p_{in}^j, and the collision probability of Eve to be x_{in}^j. Following [108, Eqn. (59)], Eve's bitwise collision probability of X satisfies

$$p_{\text{col}} := E_z[p_c^X(z)] \leq \frac{1}{2} + 2p - 2p^2 \ ,$$

where $p \leq 1/2$. This was derived under the assumption that Eve knows the locations of the errors in Bob's bit sequence. Now Alice and Bob jointly segment their bits to blocks of two bits and compute a parity bit for each block.

For the following description of TPPR in QKD setting, summarized as Algorithm 1, all actions for which the actor is not mentioned, are performed by both Alice and Bob. The arbitrary segmentations in Step 1, and selec-

Algorithm 1 TPPR in QKD setting [PII]

Initialization: Fraction of incoming bits $f_{\text{in}}^1 = 1$
Bob's error probability $p_{\text{in}}^1 = p$
Eve's collision probability $x_{\text{in}}^1 = p_{\text{col}} = 1/2 + 2p - 2p^2$

Input to Round j: Fraction of f_{in}^j of N_{sif} sifted bits with error probability p_{in}^j and collision probability $< x_{\text{in}}^j$

1. Arbitrarily segment bits to 2-bit blocks
2. Compute parity check bits for each block
3. Compute error probability p_{par}^j using [PII, Eqn. (7)]
4. Compute collision probability x_{par}^j using [PII, Eqn. (8)]
5. Compute secret key rate R_{par}^j using [PII, step 6]
6. **if** $R_{\text{par}}^j > 0$ **then**
7. Alice sends $N_{\text{sif}}(f_{\text{in}}^j/2)h(p_{\text{par}}^j)$ redundancy bits to Bob using one-time pad encryption
8. Save the corrected parity bits
9. **else**
10. Alice sends parity bits over the public channel
11. **endif**
12. Bob sends locations of erroneous parity bits over the public channel
13. Remove blocks with erroneous parity bits
14. Select one bit at arbitrarily from each kept block

Output: Fraction f_{out}^j of sifted bits with error probability p_{out}^j of [PII, Eqn. (6)], collision probability $< x_{\text{out}}^j$ of [PII, Eqn. (6)]

tions of bits in Step 14 are performed jointly by Alice and Bob over the public channel. The bits collected in Step 8 are, with high probability, all equal for Bob and Alice. Eve's information of them will be erased by using classical privacy amplification after each round, as discussed in Section 3.8. The resulting bit strings will be concatenated to produce the final key. The bits from Step 14 are fed to the protocol and the protocol terminates after a predetermined number of rounds. The outgoing bit error rate p_{out}^j and the outgoing collision probability x_{out}^j are used as input parameters in Step 1 as the protocol enters a new round.

The performance of the protocol is analysed in **Publication II** and the results are shown in Fig. 6.3. The theoretical upper bound for a one-way protocol at a given QBER value is the difference between mutual information between Alice and Bob and between Alice and Eve. The mutual information between Alice and Eve is calculated according to [89, Eqn. 64, p.39]. The theoretical upper bound is presented in Fig. 6.3 with a red curve. Watanabe *et al.* demonstrated in [93] that a two-way protocol can achieve a higher key rate than the best one-way protocol. The achieved key rate for Watanabe *et al.* from [93, Fig. 2] is shown in Fig. 6.3 for comparison. Their protocol is not able to break the theoretical one-way

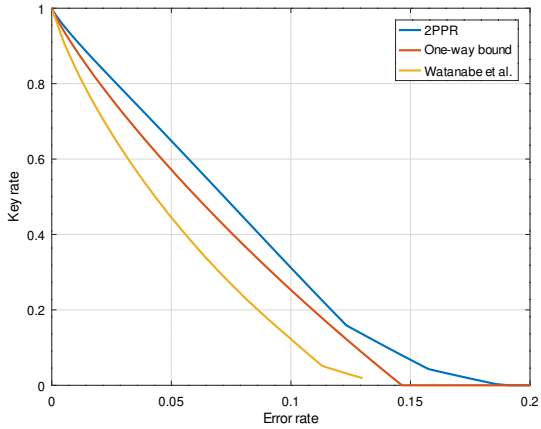


Figure 6.3. The key rate of TPPR in QKD setting [PII].

protocol bound, while TPPR with 12 rounds outperforms the one-way bound for almost the whole QBER range.

6.4 TPPR in the Source Model

Our key agreement protocol is used and analysed in a satellite setting in **Publication V**, where the source is sending random bits, and in a correlated source setting in **Publication VI**, where the input to TPPR comes from wireless channel measurements.

6.4.1 Satellite Setting

The TPPR protocol begins after the satellite communication as described in Section 3.9. The satellite is broadcasting a signal in the form of a sequence of uniformly distributed random bits U. Alice's received bits are $X \in \mathcal{X}$, Bob's bits are $Y \in \mathcal{Y}$, and Eve's are $Z \in \mathcal{Z}$. We run the protocol in a manner where Bob's parity bits are corrected with regard to Alice's parity bits. Bob's error probability with respect to Alice's original bits is β, given in (3.13). Individual bits in X are independent, while X_i, Y_i, Z_i are correlated. We define Bob's and Eve's error sequences as

$$B = Y \oplus X \ , \quad E = Z \oplus X \ . \tag{6.1}$$

These are correlated with the joint distribution given as $P_{E_i,B_i}(e,b) = \alpha_{be}$ with

$$\begin{aligned} \alpha_{00} &= \epsilon_A\epsilon_B\epsilon_E + (1-\epsilon_A)(1-\epsilon_B)(1-\epsilon_E) \\ \alpha_{01} &= \epsilon_A\epsilon_B(1-\epsilon_E) + (1-\epsilon_A)(1-\epsilon_B)\epsilon_E \end{aligned}$$

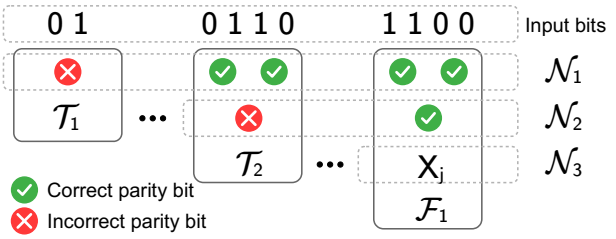


Figure 6.4. Parity bit sets for two rounds, $m = 2$ [PV].

$$\begin{aligned} \alpha_{10} &= \epsilon_A(1-\epsilon_B)\epsilon_E + (1-\epsilon_A)\epsilon_B(1-\epsilon_E) \\ \alpha_{11} &= \epsilon_A(1-\epsilon_B)(1-\epsilon_E) + (1-\epsilon_A)\epsilon_B\epsilon_E \ . \end{aligned}$$

The conditional probabilities of E given B are

$$P_{E|B}(e|b) = \frac{\alpha_{be}}{\alpha_{b0} + \alpha_{b1}} \ . \tag{6.2}$$

The error probability of Bob's bits when round m starts is the probability that both bits were wrong in the previous round, given that the parity was correct:

$$\beta_m = \frac{\beta_{m-1}^2}{\beta_{m-1}^2 + (1-\beta_{m-1})^2} \ , \tag{6.3}$$

while the error probability of the parity bits in round m is

$$p_m = 2\beta_m(1-\beta_m) \ . \tag{6.4}$$

For completeness, we define $p_0 = 0$ and $\beta_1 = \beta$. The protocol will induce correlations across blocks of bits, with the blocks of correlated bits growing in each round. The error correction of the distilled bits collected on round m consumes $h(p_m)$ bits per output bit, where h is the binary entropy function (3.7). The error correction cost has to be calculated for all the parity bits that are present at each round, as shown in Fig. 6.4 with sets $\mathcal{N}_m$.

The mutual information leaked to Eve has to be accounted for only once, when the side information leaked to Eve related to a set of distilled bits is not growing any more. This happens whenever one of Bob's parity bits is identified to be erroneous. After that, no further correlations are created related to this bit, and all the parity bits that have previously become correlated due to the information given by Bob's parity bit correctness in previous rounds. An erroneous parity bit in round m is correlated with 2^{m-i} parity bits in rounds $i = 1, \ldots m-1$. In total, an erroneous parity bit in round m represents a set $\mathcal{T}_m$ of

$$T_m = \sum_{i=1}^{m} 2^{m-i} = 2^m - 1 \tag{6.5}$$

Algorithm 2 TPPR in a satellite setting [PV]

Input to Round m**:** Fraction $2R_m$ of L initial bits with error probability β_m

1. Arbitrarily segment bits to 2-bit blocks
2. Compute parity check bits for each block
3. Compute error probability p_m using (6.4)
4. Alice sends $LR_m\, h(p_m)$ redundancy bits to Bob using one-time pad encryption
5. Bob corrects his parity bits
6. Bob sends locations of erroneous parity bits over the public channel
7. Remove blocks with erroneous parity bits
8. Compute Eve's mutual information of blocks with terminating parity bits and perform privacy amplification
9. Select one bit arbitrarily from each kept block

Output: Fraction $R_m(1-p_m)$ of original bits with error probability β_{m+1}

correlated parity bits in rounds $i = 1, \ldots, m$. The leakage of mutual information to Eve about this set of bits is *terminated* in round m. As an example, in Fig. 6.4 the sets $\mathcal{T}_1$ and $\mathcal{T}_2$ are terminated at rounds 1 and 2. Irrespective of which of the rounds $i \leq m$ a parity bit in this set is constructed in, we say that these bits are *terminated* on round m. The rate of bits terminating in round $m = 1, \ldots, M$ is

$$\tilde{R}_m = T_m\, p_m\, R_m\ . \tag{6.6}$$

In the final round, R_{M+1} represented the additional X_j bit, shown in Fig. 6.4 in set $\mathcal{F}_1$. Each of these is correlated with one correct parity bit from round M and $2^M - 2$ correct parity bits from previous rounds.

After each round of the distillation phase, privacy amplification is performed for the bits terminating in that round. The resulting round $m = 1, \ldots, M$ of TPPR is summarized in Algorithm 2. All actions for which the actor is not mentioned, are performed by both Alice and Bob. Arbitrary segmentation in Step 1 and bit selection in Step 9 are performed jointly by Alice and Bob over the public channel. The bits collected in Step 8 are, with high probability, all equal for Bob and Alice. The outgoing bit error rate β_{m+1} is used as an input parameter in Step 1 as the protocol enters a new round. The bits from Step 9 are fed to the protocol and the protocol terminates after a predetermined number of rounds, after which round $M+1$ is separately treated. With $M = 1$ the protocol is similar to the QKD protocol of [93].

From **Publication V**, the key rate for TPPR is

$$S \geq \sum_{m=1}^{M+1} p_m\, R_m\, H(Q_m|C_m)\ -\ h\,(p_m)\ , \tag{6.7}$$

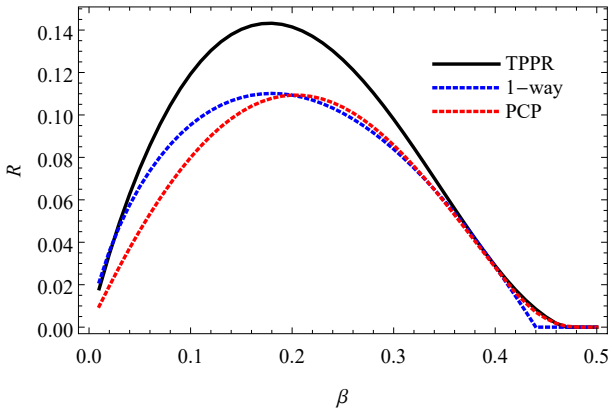


Figure 6.5. Key rates when Eve's error probability is $1.5\,\epsilon_B$ [PV].

where

$$R_m = \frac{1}{2^m} \prod_{i=0}^{m-1} (1 - p_i)\,,$$

and the entropy of Eve's error codeword arising from the corrected parity bits in round $m = 1, \ldots M$ is

$$H(Q_m|C_m) = -\sum_{(w_0,w_1)\in\mathcal{W}} \mu(w_0,w_1)\,\Psi(w_0,w_1)\;\mathrm{l}\;\mathrm{g}_2\,\Psi(w_0,w_1).$$

Here

$$\begin{aligned}
\mu(w_0,w_1) &= \frac{1+(1-\delta_{w_0,w_1})(1-\delta_{w_0,L/2-w_1})}{1+\delta_{w_0,L/4}\,\delta_{w_0,L/4}} \binom{\frac{1}{2}L}{w_0}\binom{\frac{1}{2}L}{w_1},\\
\Psi(w_0,w_1) &= \frac{1}{2}\left(\Phi(w_0,w_1)+\Phi\left(\frac{L}{2}-w_0,\frac{L}{2}-w_1\right)\right.\\
&\quad \left.+\Phi(w_1,w_0)+\Phi\left(\frac{L}{2}-w_1,\frac{L}{2}-w_0\right)\right),\\
\Phi(w_0,w_1) &= \frac{\alpha_{00}^{L/2-w_0}\,\alpha_{01}^{w_0}\,\alpha_{10}^{L/2-w_1}\,\alpha_{11}^{w_1}}{(\alpha_{00}+\alpha_{01})^{L/2}\,(\alpha_{10}+\alpha_{11})^{L/2}}.
\end{aligned}$$

The entropy of Eve's error codeword arising from the final bits in round $M+1$ is

$$H(Q_{M+1}|C_{M+1}) = -\sum_{w=0}^{L}\binom{L}{w}\Upsilon(w)\;\mathrm{l}\;\mathrm{g}_2\;\Upsilon(w),$$

where

$$\begin{aligned}
\Upsilon(w) &= P_B(0)\,\Xi(w|0) + P_B(1)\,\Xi(w|1),\\
\Xi(w|b) &= \frac{\alpha_{b,0}^{L-w}\alpha_{b,1}^{w}}{(\alpha_{b,0}+\alpha_{b,1})^{L}}\,.
\end{aligned}$$

The performance of the protocol is analysed in **Publication V** and the results are shown in Fig. 6.5. As an example, we have compared the secret

key rates of PCP and TPPR to the upper bound of any one-way protocol of the type [87, 83, 84] in a situation where $\epsilon_A = \epsilon_B/2$ and when Eve's error probability is $\epsilon_E = 1.5\,\epsilon_B$. All protocols are executed in a direction where Bob's bits are corrected to correspond to Alice's. Note that if the satellite source is not collaborating with Alice and Bob, they can estimate β but cannot estimate the individual error probabilities ϵ_A and ϵ_B. Then, Alice and Bob have to blindly choose the direction of the protocol, the simulated direction from **Publication V** being one option. The secret key rate for PCP is calculated using [72, Definition 5], and [72, Theorem 2], rephrased from [109]. The largest rate of PCP with $M = 1, \ldots, 6$ rounds is considered. TPPR rate is from (6.7), similarly the largest rate from $M = 1, \ldots, 6$ is taken.

6.4.2 Correlated Source Setting

The protocol flow in a correlated source setting is the same as in the satellite setting, but there are no error probabilities corresponding to ϵ_A, ϵ_B, and ϵ_E. Instead, Alice and Bob can directly measure the crossover probability β. The error rate γ between Alice and Eve, and the error rate η between Bob and Eve can be estimated. Bob's and Eve's error sequences are defined as in the satellite setting, given in (6.1), and the joint distribution $P_{E_i,B_i}(e,b) = \alpha_{be}$ is now with

$$\begin{aligned}
\alpha_{00} &= 1 - \frac{1}{2}(\beta + \eta + \gamma) \\
\alpha_{01} &= \frac{1}{2}(\eta + \gamma - \beta) \\
\alpha_{10} &= \frac{1}{2}(\beta + \eta - \gamma) \\
\alpha_{11} &= \frac{1}{2}(\beta - \eta + \gamma)\,.
\end{aligned}$$

These will replace the ones defined in Section 6.4.1 when the key rate is calculated for TPPR using (6.7).

7. Securing Ambient Backscatter Communications

7.1 Introduction

In the work detailed in **Publication VI** we introduce a method in order to secure IoT device or personal area network communications in an AmBC setting. We analyse secret key generation between ambient backscatter devices where the channel between an ambient transmitter and the backscatter devices is used as a source of randomness. We show that even in non-line-of-sight channels the distance from legitimate users to an eavesdropper being larger than a few wavelengths is not alone a sufficient security guarantee. This is in contrast with previous secret key generation methods where the distance is assumed to prevent the eavesdropper from having any information about the key prior to error correction. Our simulations show that a distance based approach is too optimistic, and there is a possibility that the eavesdropper still knows a substantial part of the final key.

We are combining an AmBC modulator and the corresponding receiver antenna system from **Publication III** and a secret key agreement protocol from **Publication V** with wireless channel security methods discussed in Section 4 to provide secret keys to IoT devices. These building blocks are shown in Fig. 7.1 in the scope of AmBC security. In addition to the method from **Publication VI**, we introduce a machine learning based data obfuscation method from **Publication IV** called *Camouflage Learning*.

In the literature [8, 15, 95, 9, 97, 98, 10, 13, 12, 2], the use of wireless channel as a source of randomness is based on two communicating parties sending probing signals to each other and measuring channel responses. In AmBC, the backscatter devices cannot directly estimate the channel between devices. The channel between two backscatter devices consists of two sections, as discussed in Section 4.5 and illustrated in Fig. 4.4. Therefore, it is a challenge to use existing physical layer security methods in AmBC systems, especially in case of D2D communications [104, 2].

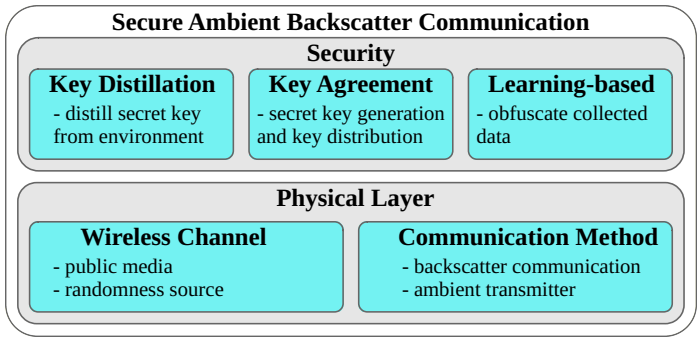


Figure 7.1. Building blocks used to secure ambient backscatter communication.

Instead of sending probing signals to each other, the backscatter devices measure the signal from an ambient transmitter. The key generation is based on correlations between received signals, rather than relying on channel reciprocity between the users. The measurements are used as raw key material to a secret key agreement protocol. We analyse the eavesdropper's mutual information based on fundamental principles, and we use state-of-the-art wireless channel models from 3GPP to model the radio channel between an ambient transmitter and the backscatter devices. The amount of key material that has to be discarded during the privacy amplification phase depends on the mutual information that the eavesdropper has of the secret key. We show how the legitimate users can estimate the eavesdropper's knowledge and balance between the reduction of achieved key rate and eavesdropper's knowledge.

7.2 System Model

The system considered here consists of a number of users and sensors associated with each user. The users are moving in an environment, where a signal from an ambient transmitter is present all the time. The sensors belonging to a user are communicating with each other, and possibly with a coordinator. The sensors use backscattering to embed their messages on top of the ambient signal, and therefore the sensors need to be able to receive the backscattered signals from other sensors.

The sensors associated with one user should be reasonably confident that they are only communicating with each other, and not with some other users' sensors. This is realized by using a shared secret key for authentication and message encryption between sensors. The raw key for secret key agreement comes from the wireless channel measurements as discussed in Section 4.3. This system is an example of a secret key distribution protocol applied in a satellite setting as discussed in Section 3.9.

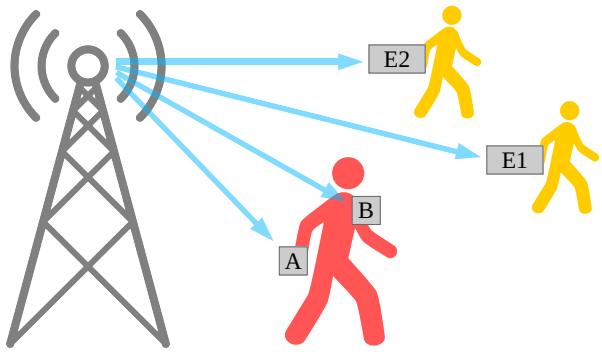


Figure 7.2. System model showing the ambient transmitter on the left, users and their sensors, and the signal paths to the users. The legitimate user has sensors A and B [PVI].

7.2.1 Users and Sensors

Figure 7.2 shows three users with their sensors. The first user is carrying sensors A and B and two other users are carrying sensors E1 and E2. Each sensor has its own signal path from the ambient transmitter, as shown in Fig. 7.2 with blue arrows. Although all users share a common environment, the signal paths are different to each user and their sensors. The signal paths to the sensors of one user are more similar to each other than the paths to different users.

In a bistatic system, as in AmBC, the backscattered signal is strongest if the backscatter device is either near the transmitter or receiver. This was shown in **Publication I**, where the link budget for an AmBC system was validated in sub-1 GHz band and confirmed with measurements at 590 MHz. In the use case considered here, it is therefore beneficial that the sensors are near each other, compared with the ambient transmitter.

7.2.2 Backscatter Device

The backscatter device needs to measure the signal level of the ambient transmitter to gather raw key material for secret key agreement, and therefore it needs a corresponding receiver. This is a distinctive feature of the proposed backscatter device, as those devices doing only backscatter modulation do not need a receiver for the ambient signal.

The operating principle of the proposed backscatter device is illustrated in Fig. 7.3. The modulator SW in the figure is an RF switch and the controller is e.g. a microcontroller that generates the modulating waveform. As the modulation is realized by either connecting the two antennas together or isolating them from each other, the antennas are connected to terminating resistors when they are in the isolated state. Without the terminations, there is a possibility that the antennas are reflecting the in-

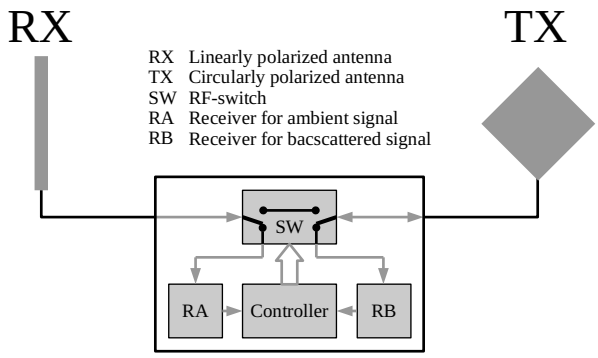


Figure 7.3. Block diagram of the backscatter device [PVI].

coming signal back uncontrollably. The terminations are actually receivers whose inputs are matched to the impedance of the system. The receiver connected to the linear polarized antenna receives the ambient signal and is responsible for making the channel measurements. The backscatter receiver connected to the circular polarized antenna listens to other sensors, and uses the polarization conversion method as in **Publication III** to better suppress the ambient signal at the receiver.

An actual realization of the backscatter device could use a commercially available power sensor IC to measure the incoming RF power. The output voltage of the power sensor IC is proportional to the input power. The ambient receiver could use either an RF demodulator in front of the power sensor to enable tuning the receiver to a certain ambient RF signal, or a simple band-pass filter could be used instead, if the frequency of the ambient signal is fixed. The output of the power sensor IC is sampled to obtain the raw power measurements. A general-purpose microcontroller is used to make measurements, process the information originating from another sensor, and control the backscatter modulator as needed.

7.3 Distilling a Shared Secret from Ambient Signal

We generate key material from the signal levels of the ambient transmitter at the sensors, as the users are moving with regard to the ambient transmitter. The sensors are receiving the ambient signal and measuring the received signal power. This is shown in Fig. 7.4 as step (a). The measurements are done in a coordinated way to increase correlation between the measurements, which leads to higher key rates. One of the sensors can act as a coordinator and send a command to the other sensor to start the power measurement procedure. Alternatively, a certain signal pattern from the ambient transmitter can trigger the measurements. Either way, the sensors are making the measurements simultaneously, thus avoiding

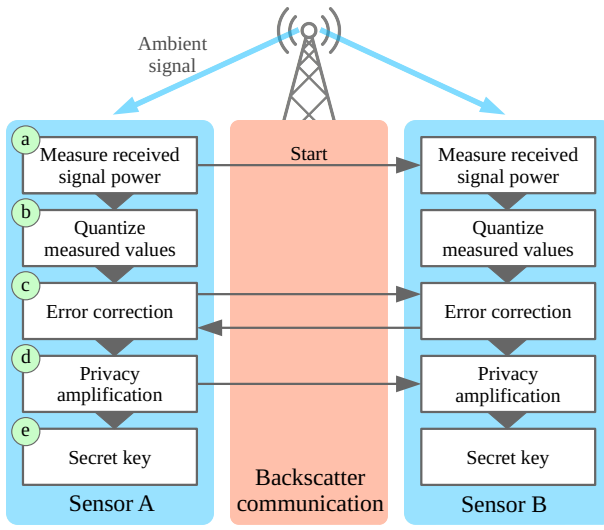


Figure 7.4. Device operation and communication for key generation from ambient signal. [PVI].

the time delay problem described in Section 4.3.

Let the measured values be $X = (x_1, x_2, ..., x_n)$ and $Y = (y_1, y_2, ..., y_n)$ where X corresponds to readings from sensor A and Y corresponds to readings from sensor B. The sensors use X and Y as raw key material, and independently extract random bits from them using a quantizer, as shown as step (b) in Fig. 7.4.

The bits extracted during step (b) are not the same for both sensors. Therefore, in step (c), an information reconciliation protocol is used to produce a key that both sensors A and B agree on. Here, two-way communication is considered in this step. Finally, in step (d) a privacy amplification protocol is applied to the key to make it secure. This is based on one-way communication. The sensors A and B use backscatter communication to exchange messages between them in steps (a), (c) and (d).

As discussed in Section 4.3, the most common bit extraction method is to measure amplitude or channel gain. This method is also used here, as the sensors measure the received signal power from the ambient transmitter at coherence time T_c intervals (4.1) and use the equiprobable quantizer method from Section 4.4 to convert the measured values to bits. A comparison of resulting error rate distributions between Alice and Bob using a level crossing, and 4- and 8-level equiprobable quantizers is shown in Fig. 7.5. The dataset used to produce the comparison is the same set of channel measurements that are used later as an input to the key agreement protocols.

As the sensors A and B can only measure the error rate β between themselves, therefore they can only guess the error rates γ and η between an eavesdropper and themselves. In [72] the eavesdropper's knowledge

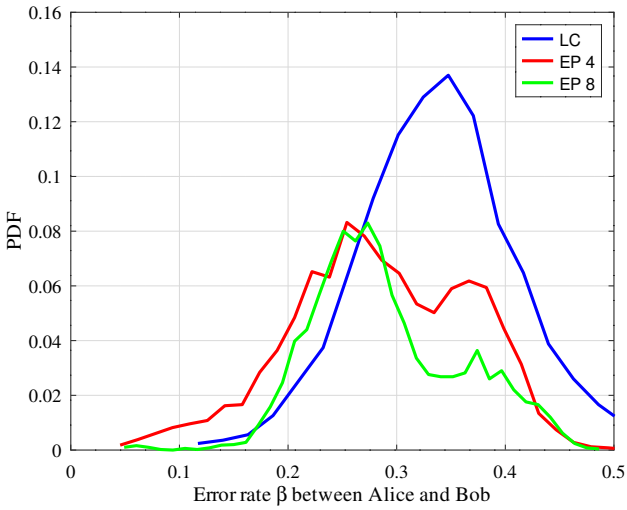


Figure 7.5. Error rate distributions with different quantizers [PVI].

about the channel compared with legitimate users was estimated in terms of a maximum size of the antenna array the eavesdropper has. Here, we take a similar approach. We model Alice's and Bob's estimates for γ and η in terms of a multiplicative factor k; Alice and Bob then run privacy amplification assuming that

$$\gamma = \eta = \min(k\beta, 0.5) \; . \tag{7.1}$$

In a given operational situation, these estimates may be more conservative than the realized error rates, or they may be too optimistic. In the latter case, the eavesdropper retains information on the secret key after privacy amplification. This approach allows us to calculate the achievable key rates in Section 7.5.2 and estimate Eve's average knowledge of the resulting secret key as a function of k in Section 7.5.3.

7.4 Computation and Communication Complexity

The sensors need to perform a series of computations in order to end up having a common shared secret. For example, if we start TPPR as described in Algorithm 2 from Section 6.4.1 with 1000 input bits, Alice and Bob at first calculate 500 parity bits and Alice sends Bob enough redundancy bits so that Bob can correct his parity bits. Bob then sends Alice the positions where the parities disagreed, and then they both discard the corresponding two-bit blocks. From each remaining block, they jointly select one bit and the protocol enters a new round. The bits remaining after the last round are error corrected and added to the shared secret.

The number of bit operations depends on the bit error rate. In Table 7.1 we report the estimated number of operations per input bit during three

Table 7.1. Number of bit operations per input bit for three rounds of the protocol [PVI].

β	0.05	0.10	0.20	0.30
Parity bit error correction	170	260	380	440
Error correction of last bits	0.01	0.15	1.9	7.3
Total	170	260	380	450

Table 7.2. Communication cost in terms of communicated bits per input bit [PVI].

β	0.05	0.10	0.20	0.30
Number of redundancy bits	0.24	0.37	0.55	0.64
Parity bit positions	0.84	0.81	0.75	0.70
Total	1.1	1.2	1.3	1.3

protocol rounds, for a selection of input bit error rates. Correcting parity bits is the heaviest task; when considering the errors remaining after the last round, significantly fewer computations are needed, as the advantage distillation process is very effective in decreasing the error rate. We assume that bit errors are corrected using 50 iterations of an LDPC code which has an average check node degree of 7.

The computational load in operations per seconds depends on the rate at which input bits are created. We may consider a situation corresponding to the scenario simulated in Section 7.5. If we assume a user walking at a 5 km/h pace, a carrier frequency of 590 MHz, taking samples at T_c intervals calculated from (4.1), and using an equiprobable quantizer from (4.5) with 4 levels, this results in 5.5 input bits per second. With the worst error rate considered in Table 7.1, this requires 2500 operations per second. If we have a low performance microcontroller running at e.g. 4 MHz clock rate and assume that one instruction takes four clock cycles to execute, the microcontroller may execute one million instructions per second. The computations related to key generation in this scenario take only a small fraction of the microcontroller capacity.

Another implementation aspect worth considering is the required amount of communication between Alice and Bob. Alice has to send the redundancy bits to Bob and in return Bob sends Alice the positions of erroneous parity bits. These bits represent the communication cost between the sensors. The communication cost per input bit during three protocol rounds is presented in Table 7.2. The achievable transmission rates in AmBC systems start from kbits/s, giving ample room for coding and protocol overhead as the sensors need to communicate less than 8 bits/s, in the considered scenario where 5.5 input bits are created per second.

Since the number of input bits per second is relatively low, neither the computational nor the communication capacity of the backscatter device

will be a bottleneck.

The number of instructions that are needed to run the key agreement protocol can be reduced by using precalculated lookup tables (LUT) to assist the protocol execution. For example, the parity check matrices for the LDPC code and the amount of needed privacy amplification can be precalculated for a selection of error rates, and the corresponding shortening algorithm could also be stored to a precalculated table. The parity bit calculation at the heart of the TPPR protocol is a simple exclusive-OR instruction, available at hardware level in virtually all microcontrollers.

The LUTs take up memory, and the more detailed the tables are, the more memory is needed. However, as the contents of the tables are static, they can be stored in non-volatile memory, thus helping to decrease the energy consumption of the backscatter device.

7.5 Performance Evaluation

We simulate the secret key generation using channel measurements as raw key material using state-of-the-art wireless channel models from 3GPP [110] and show that the distance between an eavesdropper and the legitimate users is not alone a sufficient security guarantee. We show how the legitimate users can estimate the eavesdropper's knowledge and balance between the reduction of achieved key rate and eavesdropper's knowledge.

7.5.1 Simulation Setup

The signal paths shown in Fig. 7.2 are showing only the line-of-sight (LOS) components from the ambient transmitter to the users. However, there are usually numerous multipath components and there may not even be an LOS signal path at all. The radio channels from the ambient transmitter to the sensors are modelled using QUAsi Deterministic RadIo channel GenerAtor (QuaDRiGa) [111]. QuaDRiGa has several built-in radio propagation models. We used the 3GPP TR38.901 urban and rural macro models to simulate the radio signal propagation between the transmitter and the receiver [110]. For each of these environments, a non-LOS signal propagation model was used in the simulations.

The receivers are placed in three different configurations shown in Fig. 7.6. The sensors A and B belong to the legitimate user, and sensors E1 and E2 belong to the eavesdropper. The sensors for each user are at the same height, 1.5 m from ground level. The configuration a) is the baseline situation, where the eavesdropper is near sensor B. In configuration b) the eavesdropper is further away from sensors A and B, and in configuration c) the eavesdropper is positioned between sensors A and B.

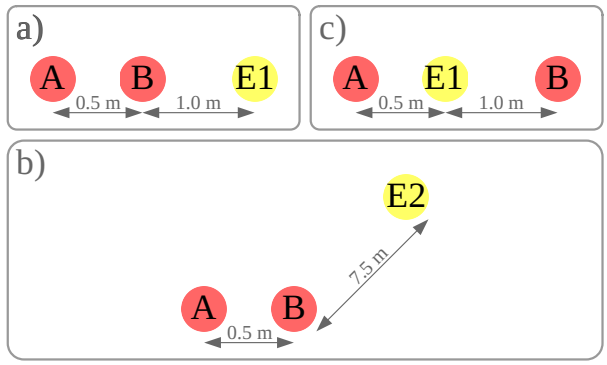


Figure 7.6. The initial receiver positions, a) baseline situation, b) Eve is further away, and c) Eve is between sensors A and B [PVI].

Table 7.3. Distances between sensors and half wavelengths at simulation frequencies [PVI].

Sensor pairs	Distance	100 MHz $\lambda/2 = 1.5$ m	590 MHz $\lambda/2 = 0.25$ m
A - B	0.5 m	$\lambda/6$	λ
B - E1	1.0 m	$\lambda/3$	2λ
B - E2	7.5 m	$5\lambda/4$	14.8λ

The distances between sensors are listed in Table 7.3 as are the half wavelengths corresponding the frequencies used in the simulations. At 100 MHz the sensors A and B are within the $\lambda/2$ limit, therefore the spatial channel responses should be alike. However, sensor E1 is also within the same limit to B, while sensor E2 is outside the $\lambda/2$ limit. At 590 MHz, all sensors are further away from each other than the corresponding $\lambda/2$ distance.

For each simulation case, the users are randomly dropped inside a 7.5 km square. The users are walking a 250 m long route at a 5 km/h pace maintaining their initial separations. The starting positions and random walking directions for a sample of 300 simulation cases are shown in Fig. 7.7. The ambient transmitter is located at coordinates $X = 0$ and $Y = 0$, marked with a red cross in Fig. 7.7 and is located 100 m above ground level. The transmitter antenna is a half-wave dipole and the receiver antennas are omnidirectional. Therefore, the orientation of the receiver antennas does not matter, making them suitable for modelling wearable sensors.

The ambient transmitter is either a terrestrial TV station or an FM radio station. The centre frequencies are 590 MHz and 100 MHz, correspondingly.

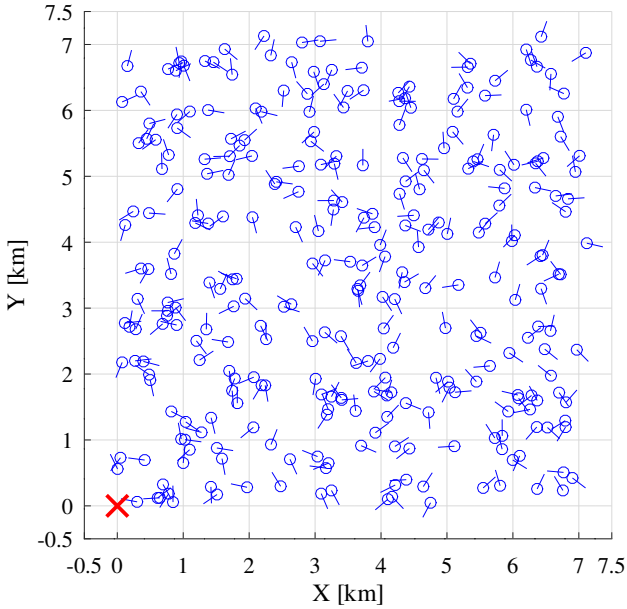


Figure 7.7. Random starting positions and walking directions for 300 simulation cases [PVI].

7.5.2 Achieved Key Rates

The simulations were at first run with known error rates. The error rate β between Alice and Bob, and error rates γ and η between Eve and the legitimate users were assumed to be known. The error rates for each simulated walking route were calculated for each receiver configuration shown in Fig. 7.6 from the quantized power levels. The error rates were used as input to PCP and TPPR protocols from sections 3.9 and 6.4.2 and the one-way protocol from Section 3.8. The key rate for PCP was calculated using [72, Theorem 2], rephrased from [109]. The key rate for TPPR was calculated using (6.7) and the key rate for a one-way protocol is defined as

$$R_{\mathrm{OW}} = \begin{cases} h(\gamma) - h(\beta), & \text{if Alice's bits are corrected} \\ h(\eta) - h(\beta), & \text{if Bob's bits are corrected} \end{cases} \tag{7.2}$$

where h is the binary entropy function (3.7). A total of 5000 simulation cases were used to produce the input to the aforementioned protocols. Both PCP and TPPR were run three rounds and the best key rate was taken for each of the 5000 cases. The radio channels were modelled using the urban macro scenario at 590 MHz centre frequency.

The averaged key rates over all simulation rounds are presented in Fig. 7.8 for the baseline configuration. On the average, both PCP and TPPR are able to produce secret key even in the presence of an eavesdropper over a wide range of error rates, and in most cases producing more secret key than one-way protocols.

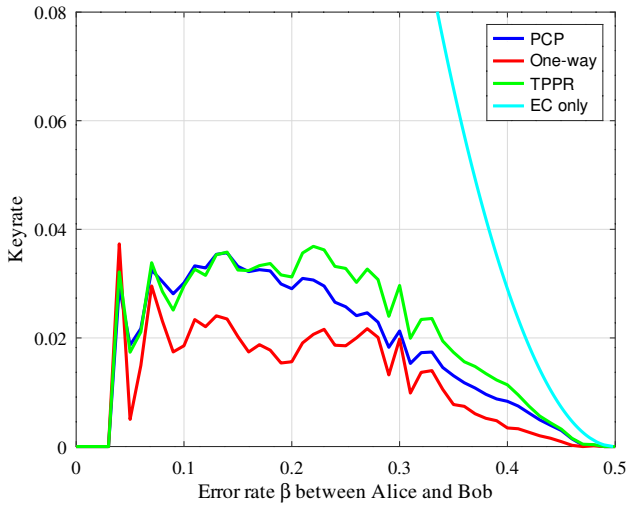


Figure 7.8. Average key rates for PCP and TPPR compared to one-way protocol key rate in baseline situation [PVI].

If the distance between Eve and the legitimate users were the only security guarantee, the key rate would have been substantially higher. In this case only the cost of error correction is taken into account when calculating the key rate, as Eve is supposed to have no prior knowledge of the key. For a comparison, the resulting key rate is shown in Fig. 7.8 with the *EC only* label. The proximity based device pairing system in [103] would reach this key rate for the baseline configuration.

Even if Eve is located between Alice and Bob as in receiver configuration c), it is possible to produce a secret key. The averaged key rates for configuration c) are shown in Fig. 7.9. In this configuration, the method of [103] would not produce any key, as Eve is too close to Alice.

Because the protocols of interest are capable of producing key with a wide range of error rates β, the choice of the quantizer does not play a significant role. However, there may be other reasons to favour a specific quantizer, e.g. the ease of implementation.

It is only possible to distil any secret key from a random source if there is some correlation between the raw key material, in this case in the measured power levels. The correlation of the power measurements as a function of distance was simulated for both urban and rural environments at 100 MHz and 590 MHz frequencies. The averaged correlations as a function of distance expressed in wavelengths are presented in Fig. 7.10. The positions of sensors B, E1 and E2 relative to sensor A are marked on the figure as the sensor A is located at $X = 0$.

It can be seen from the figures that although the correlation decreases rapidly as the distance is more than $\lambda/2$, on the average the level of correlation stays relatively high, even if the distance is several wavelengths. The reason for this is that even though the channels are non-LOS, they

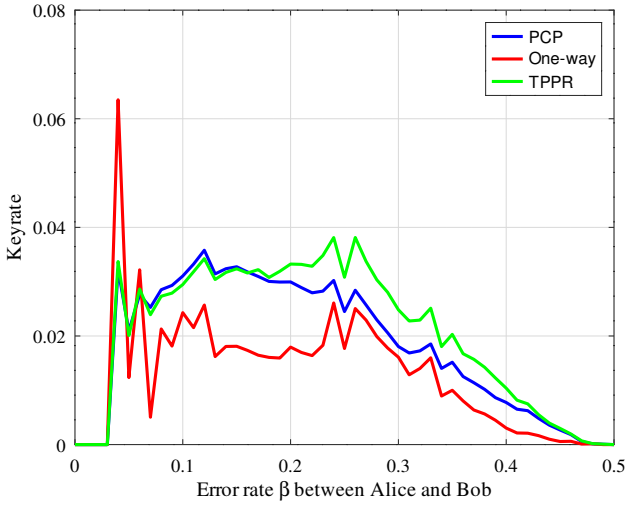


Figure 7.9. Average key rates for PCP and TPPR compared to one-way protocol key rate when Eve is between Alice and Bob [PVI].

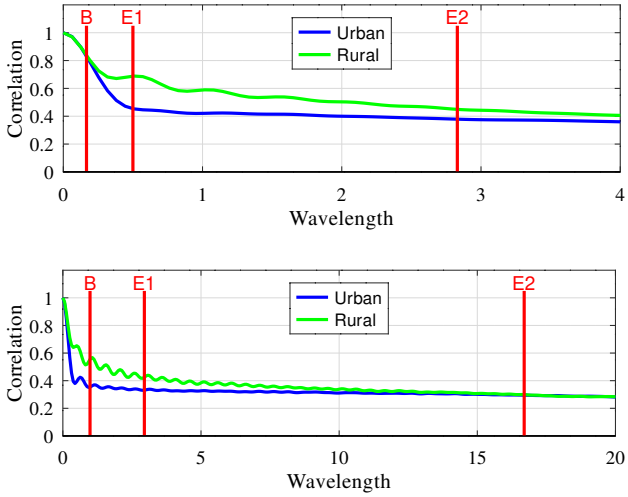


Figure 7.10. The mean correlation between power measurements as a function of distance in urban and rural environments for centre frequencies 100 MHz above and 590 MHz below [PVI].

are locally dominated by a few multipath components. As Fig. 7.10 shows, the level of correlation is similar at both frequencies and therefore the resulting key rates would be similar too. The correlation stays even higher in rural environments as there are fewer obstacles causing multipath propagation. It should be noted that in order to extract the same number of secret bits at 100 MHz would take more time, or longer walking route, as the coherence time is longer compared to that at 590 MHz.

7.5.3 Estimating Eve's Knowledge

Were these sensors operated in a real world situation, Alice and Bob could only measure the error rate β between themselves. They do not know the error probability between either one of them and a nearby eavesdropper. The amount of key material that has to be discarded during the privacy amplification phase depends on the mutual information that the eavesdropper has of the secret key, and that in turn is related to the error rate between e.g. Bob and Eve. Therefore, Alice and Bob need to estimate Eve's error rate γ between Alice and Eve, and error rate η between Bob and Eve. If the estimation were too optimistic, the key rate would be higher but Eve would possess residual information about the secret key even after privacy amplification.

We model Alice's and Bob's estimates for γ and η in terms of a factor k as in (7.1), with k in the range from 0.5 to 2. With S the key rate with estimated error rates and R the actual key rate with realized error rates, Eve's residual knowledge of the secret key is

$$K = \begin{cases} \frac{S-R}{S} & \text{, if } S - R > 0 \\ 0 & \text{, otherwise .} \end{cases} \tag{7.3}$$

Eve's average residual knowledge of the secret key over all simulation cases are presented in Fig. 7.11 for PCP and TPPR, as well as the one-way protocol. The figure shows results for receiver configurations a), b) and c) from Fig. 7.6. When $k < 1$ a one way protocol can not produce any key. When $k > 1$ Eve's knowledge of the secret key increases rapidly. A zoomed out region when $0.7 < k < 1$ is shown in the same figure for PCP and TPPR.

If again the distance between Eve and Alice or Eve and Bob were the only security guarantee, Eve's average knowledge compared to the one-way key rate realizations would be approximately 90% as shown in Fig. 7.11 with the *EC only a)* label in case a), and approximately 85% in case b), as shown with the *EC only b)* label. Note that in the simulated scenario, sensors A and B are at one wavelength distance from each other, while Eve is two wavelengths from B in case a) and almost 15 wavelengths in case b). In the studied realistic channel model, the distance based security guarantee is too optimistic, as Eve still knows a substantial part of the secret key.

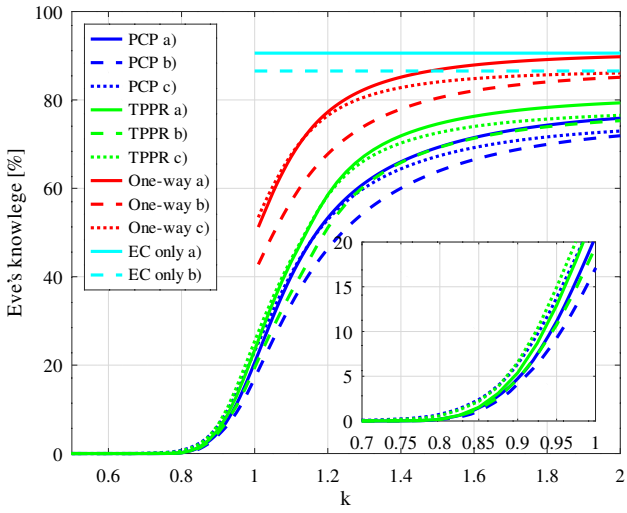


Figure 7.11. Eve's average residual knowledge of the final key when Eve's error probability is assumed k times Alice's and Bob's [PVI].

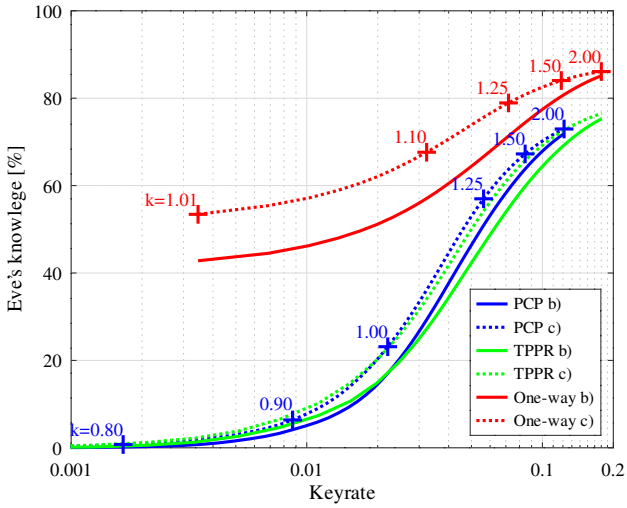


Figure 7.12. Eve's average residual knowledge of the final key vs. achieved key rate [PVI].

The factor k does not affect Eve's knowledge in this case as Eve's distance is not taken into account, and error rates γ and η are not used at all.

By choosing a suitable value for factor k, it is possible to balance between the reduction of achieved key rate and Eve's knowledge of the final key. Fig. 7.12 shows the trade off between Eve's knowledge of the final key vs. the achieved key rate. The results are shown for configurations b) and c). The curves start from $k = 0.78$, for which Eve's knowledge is practically zero. Six values of k are marked to the PCP c) curve and five values of k are marked to the one-way c) curve. For example, if $k = 1$ Eve knows on the average $\sim 23\%$ of the final key produced using either PCP or TPPR. With a smaller k, Eve's knowledge is reduced. This assumes that Eve has an advantage compared to Alice and Bob, as the assumption is that $\gamma = \eta < \beta$ meaning that no one-way protocol is able to produce a key anymore.

7.6 Learning Based Data Obfuscation

Another way to make use of the randomness of a fading wireless channel in securing AmBC setting is to exploit the interference of backscattered signals. Instead of extracting secret keys from wireless channel measurements to offer data privacy, machine learning based methods can be used to obscure the collected data. We proposed in **Publication IV** a distributed machine learning based data obfuscation method, *Camouflage Learning*, that uses backscattering for energy efficient communication. Our approach enables energy-less computation via physical-layer computation offloading, exploiting interference of backscattered signals for the aggregation of weighted feature values. These feature values can be e.g. temperature, humidity or some other measured values. In **Publication IV**, a single device extracts a single feature and sends the weighted value to the coordinator.

Camouflage learning advances data privacy compared to prior state-of-the-art methods such as Federated learning [112, 113, 114, 115] or homomorphic encryption [116, 117, 118], all of which demand high processing or communication resources. In contrast to existing distributed machine learning methods, in Camouflage learning the information on the model is scattered across devices. No single device has, at any time, knowledge on the complete model or on other device's feature values. In addition, the shared feature values are protected from potential eavesdroppers through obfuscation. Learning based data obfuscation is shown as an additional building block that can be used to secure AmBC in Fig. 7.1.

The proposed method was evaluated using backscatter devices in indoor environments, thus proving that Camouflage Learning is a suitable protocol for energy constrained devices. It thereby brings battery-free distributed learning and continuous operation in Ambient Intelligence environments into reach.

8. Conclusions and Future Work

This thesis addresses securing IoT device or personal area network communications in an AmBC setting. The security of IoT devices has become a concern, as IoT has made it possible for things and people to interact with each other anytime and any place. These devices are often limited in their computational, communication and power resources, due to their embedded nature. Therefore, using computationally heavy cryptographic methods to offer security to the connected devices is seldom possible. In this work, an information-theoretically secure two-way secret key agreement protocol is applied in a correlated source model, where the raw key material to the protocol is gathered from wireless channel measurements. The key agreement protocol makes it possible to use symmetric encryption methods to secure communication between devices and thus avoids the need for heavy computations. The wireless channels in question are from an ambient transmitter to the backscatter devices.

Backscatter communication is seen as a viable solution for resource limited devices, as the wireless nodes are communicating without any active RF components. The devices reflect the incoming RF signal back to the receiver, effectively becoming a modulator by changing the amount of reflection. However, the interference from the ambient transmitter remains a major challenge, as the ambient signal is present at the receiver together with the backscattered signal.

In the first part of this work, two backscatter devices are presented. The first one is based on known principles in the literature. The goal was to make the first backscatter device easy to use and to cover a wide frequency range. Based on the insight that was gathered during the use of the first backscatter device, a second device was developed. In an AmBC setting the signal from the ambient transmitter is usually several orders of magnitude stronger than the backscattered signal, and appears as interference at the backscatter receiver. The second backscatter device in combination with a corresponding antenna construction at the receiver end is able to significantly attenuate the ambient signal, thus decreasing the impact of interference.

The second part of this work presents a two-way secret key agreement protocol, TPPR. The protocol uses error corrected parity bits for advantage distillation. During each round of the protocol Alice and Bob calculate parity bits for two-bit blocks. As the parity bits are strongly correlated, Alice sends Bob only sufficient information that he can correct his parity bits. In contrast to similar protocols known in the literature, the secret key is gathered from error corrected parity bits, and not from either Alice's or Bob's original bit strings. In both QKD and satellite settings, TPPR is able to outperform the theoretical one-way protocol bound. In the QKD setting, this was analysed under the individual quantum attack model.

In the last part of this work, we analyse the secret key generation between ambient backscatter devices and show that the distance from legitimate users to an eavesdropper is not alone a sufficient security guarantee. This observation is in contrast with previous secret key generation methods from the literature where distance is the only safeguard against an eavesdropper, and privacy amplification merely removes any information that the eavesdropper overheard during the error correction phase. Existing secret key generation methods use the reciprocal radio channel between users as a source of randomness. Our setting uses the fading radio channels from the ambient transmitter to the backscatter devices as a source of randomness for secret key generation. Therefore, the backscatter devices do not need to estimate or measure the channel between themselves, which greatly simplifies the gathering of raw key material. We analyse the eavesdropper's mutual information based on fundamental principles, and we use state-of-the-art wireless channel models from 3GPP to model the radio channels between an ambient transmitter and the backscatter devices.

Our analysis shows that the distance-based approach is too optimistic and the eavesdropper may still know a substantial part of the final key. Furthermore, one-way protocols are insufficient for key generation, they lead either to no key, or the eavesdropper knowning most of the key. We show how Alice and Bob can estimate Eve's knowledge of the secret key by using a factor k to estimate Eve's error rates γ and η based on observed error rate β between Alice and Bob. By choosing a suitable value for factor k, it is possible to balance between the reduction of achieved key rate, and Eve's knowledge of the final key. This assumes that Eve has an advantage compared to Alice and Bob as the assumption is that $\gamma = \eta < \beta$ meaning that no one-way protocol is able to produce a key any more.

A working solution is based on a two-way key agreement protocol, such as TPPR, and assuming that Eve's error rates are k times that of Alice's and Bob's, with $k < 1$. On the average, this approach significantly decreases Eve's knowledge of the final key, at the expense of achievable key rate. This method gives Alice and Bob the freedom to trade off between achievable key rate and Eve's knowledge of the final key.

The observation that one-way protocols are not able to produce secret key at all, or that the eavesdropper knows most of the key in the studied AmBC scenario, raises the question, whether the same observation is valid in other similar key agreement scenarios. This opens possible avenues for future work, both evaluating existing key agreement scenarios, or developing new two-way methods for secret key agreement. Also, analysing TPPR under the coherent QKD attack model is a possible direction for future work.

The topics investigated in this thesis, backscatter communications and secret key agreement, are promising methods to be used with the upcoming sixth generation of mobile network (6G) devices. The density of autonomous IoT devices is expected to increase substantially when 6G networks are deployed. Such devices are not operated by humans, instead these devices are using machine-type communications (MTC) when exchanging information with each other or with some remote servers. Backscatter communication is an energy efficient communication method for these devices and secret key agreement protocols are an integral part of making the information exchange between devices secure.

References

[1] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Communications Surveys & Tutorials*, 2018.

[2] P. Wang, L. Jiao, K. Zeng, and Z. Yan, "Physical layer key generation between backscatter devices over ambient RF signals," in *IEEE Conference on Computer Communications*, 2021, pp. 1–10.

[3] C. Boyer and S. Roy, "Backscatter communication and RFID: Coding, energy, and MIMO analysis," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 770–785, Mar. 2014.

[4] A. Bletsas, S. Siachalou, and J. N. Sahalos, "Anti-collision backscatter sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, 2009.

[5] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Bistatic backscatter radio for power-limited sensor networks," in *IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 353–358.

[6] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in internet of things: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, 2018.

[7] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel." New York, NY, USA: Association for Computing Machinery, 2008.

[9] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[10] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.

[11] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice, 6th Ed.* Pearson London, 2014.

[12] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2763–2776, 2014.

[13] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[14] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Information*, vol. 7, p. 49, Aug. 2016.

[15] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 63–70, 2010.

[16] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, 1948.

[17] J. D.Griffin, G. D. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *IEEE Antennas and Propagation Magazine*, vol. 51, no. 2, 2009.

[18] J. Kimionis,A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 1091–1104, 2014.

[19] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," *ACM SIGCOMM Computer Communication Review*, 2013.

[20] D. M. Pozar, *Microwave Engineering*, 4th ed. Hoboken, NJ, USA: John Wiley & Sons, 2012.

[21] J. Wang, Chang Choi, and R. Moore, "Precision experimental characterization of the scattering and radiation properties of antennas," *IEEE Transactions on Antennas and Propagation*, vol. 30, no. 1, pp. 108–112, 1982.

[22] G. Vougioukas and A. Bletsas, "24μ Watt 26m range batteryless backscatter sensors with FM remodulation and selection diversity," in *IEEE International Conference on RFID Technology and Applications (RFID-TA)*, 2017, pp. 237–242.

[23] J. Qian, A. N. Parks, J. R. Smith, F. Gao, and S. Jin, "IoT communications with M-PSK modulated ambient backscatter: Algorithm, analysis, and implementation," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 844–855, 2019.

[24] G. Vougioukas and A. Bletsas, "Switching frequency techniques for universal ambient backscatter networking," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 464–477, 2019.

[25] Analog Devices, Inc., "ADG919 datasheet and product info," https://www.analog.com/en/products/adg919.html, accessed: Dec. 12, 2022.

[26] X. Wang, H. Yiğitler, R. Duan, E. Y. Menta, and R. Jäntti, "Coherent multiantenna receiver for BPSK-modulated ambient backscatter tags," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1197–1211, 2022.

[27] J. Kimionis and M. M. Tentzeris, "Pulse shaping: The missing piece of backscatter radio and RFID," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 12, pp. 4774–4788, 2016.

[28] J. Kimionis, A. Georgiadis, S. N. Daskalakis, and M. M. Tentzeris, "A printed millimetre-wave modulator and antenna array for backscatter communications at gigabit data rates," *Nature Electronics*, vol. 4, pp. 439–446, 2021.

[29] R. Fara, D.-T. Phan-Huy, A. Ourir, Y. Kokar, J.-C. Prévotet, M. Hélard, M. Di Renzo, and J. De Rosny, "Polarization-based reconfigurable tags for robust ambient backscatter communications," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1140–1152, 2020.

[30] F. Amato, C. W. Peterson, B. P. Degnan, and G. D. Durgin, "A 45 μW bias power, 34 dB gain reflection amplifier exploiting the tunneling effect for RFID applications," in *IEEE International Conference on RFID*, 2015, pp. 137–144.

[31] D. Darsena, "Noncoherent detection for ambient backscatter communications over OFDM signals," *IEEE Access*, vol. 7, pp. 159 415–159 425, 2019.

[32] Q. Zhang, H. Guo, Y.-C. Liang, and X. Yuan, "Constellation learning-based signal detection for ambient backscatter communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 452–463, 2019.

[33] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging ambient backscatter communication," *SIGCOMM Computer Communication Review*, vol. 44, no. 4, p. 619–630, Aug 2014.

[34] G. Yang, Y.-C. Liang, R. Zhang, and Y. Pei, "Modulation in the air: Backscatter communication over ambient OFDM carrier," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1219–1233, 2018.

[35] B. P. Lathi and Z. Ding, *Modern Digital and Analog Communication Systems*, 4th ed. New York, USA: Oxford University Press, 2010.

[36] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient backscatter communication systems: Detection and performance analysis," *IEEE Transactions on Communications*, vol. 64, no. 11, pp. 4836–4846, 2016.

[37] K. Lu, G. Wang, F. Qu, and Z. Zhong, "Signal detection and BER analysis for RF-powered devices utilizing ambient backscatter," in *International Conference on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1–5.

[38] J. Qian, F. Gao, G. Wang, S. Jin, and H. Zhu, "Semi-coherent detection and performance analysis for ambient backscatter system," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5266–5279, 2017.

[39] ——, "Noncoherent detections for ambient backscatter system," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1412–1422, 2017.

[40] M. A. ElMossallamy, M. Pan, R. Jäntti, K. G. Seddik, G. Y. Li, and Z. Han, "Noncoherent backscatter communications over ambient OFDM signals," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3597–3611, 2019.

[41] J. K. Devineni and H. S. Dhillon, "Non-coherent signal detection and bit error rate for an ambient backscatter link under fast fading," in *IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[42] S. Guruacharya, X. Lu, and E. Hossain, "Optimal non-coherent detector for ambient backscatter communication system," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 16 197–16 201, 2020.

[43] J. Qian, F. Gao, and G. Wang, "Signal detection of ambient backscatter system with differential modulation," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2016, pp. 3831–3835.

[44] H. Hwang and J.-H. Yun, "Adaptive transmission repetition and combining in bistatic WiFi backscatter communications," *IEEE Access*, vol. 8, pp. 55 023–55 031, 2020.

[45] Y. Hu, P. Wang, Z. Lin, M. Ding, and Y.-C. Liang, "Performance analysis of ambient backscatter systems with LDPC-coded source signals," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7870–7884, 2021.

[46] M. Cui, G. Zhang, and R. Zhang, "Secure Wireless Communication via Intelligent Reflecting Surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[47] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[48] S. Y. Park and D. In Kim, "Intelligent Reflecting Surface-aided Phase-Shift Backscatter Communication," in *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 2020, pp. 1–5.

[49] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward Smart Wireless Communications via Intelligent Reflecting Surfaces: A Contemporary Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2283–2314, 2020.

[50] G. Van Assche, *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.

[51] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[52] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[53] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[54] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[55] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in Cryptology*, T. Beth, N. Cot, and I. Ingemarsson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 33–50.

[56] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: John Wiley & Sons, 2006.

[57] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[58] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communications and Cryptography*. Springer, 1994, pp. 271–285.

[59] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology – CRYPTO*, R. Safavi-Naini and R. Canetti, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 294–311.

[60] R. Canetti, E. Kushilevitz, and Y. Lindell, "On the limitations of universally composable two-party computation without set-up assumptions," in *Advances in Cryptology — EUROCRYPT*, E. Biham, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 68–86.

[61] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in *Proc. IEEE Symposium on Foundations of Computer Science*, 2001, pp. 136–145.

[62] M. Pivk, "Quantum Key Distribution," in *Applied Quantum Cryptography*. Springer, 2010, pp. 23–47.

[63] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[64] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[65] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Transctions on Information Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[66] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[67] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988.

[68] R. König and U. Maurer, "Generalized strong extractors and deterministic privacy amplification," in *Cryptography and Coding*, N. P. Smart, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 322–339.

[69] Y. Dodis, X. Li, T. D. Wooley, and D. Zuckerman, "Privacy amplification and nonmalleable extractors via character sums," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 800–830, 2014.

[70] J. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143 – 154, 1979.

[71] N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, vol. 52, no. 1, pp. 43–52, 1996.

[72] D. Jost, U. Maurer, and J. L. Ribeiro, "Information-theoretic secret-key agreement: The asymptotically tight relation between the secret-key rate and the channel quality ratio," in *Theory of Cryptography*, A. Beimel and S. Dziembowski, Eds. Cham: Springer International Publishing, 2018, pp. 345–369.

[73] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT, LNCS*, vol. 1807, 2000, pp. 351–368.

[74] U. M. Maurer, "Protocols for secret key agreement by public discussion based on common information," in *Advances in Cryptology — CRYPTO*, E. F. Brickell, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 461–470.

[75] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179.

[76] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, pp. 661–663, Aug 1991.

[77] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Physical Review Letters*, vol. 68, pp. 3121–3124, May 1992.

[78] D. Bruß, “Optimal eavesdropping in quantum cryptography with six states,” *Physical Review Letters*, vol. 81, pp. 3018–3021, Oct 1998.

[79] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Physical Review Letters*, vol. 92, p. 057901, Feb 2004.

[80] ID Quantique SA, “Clavis XG QKD System,” https://marketing.idquantique.com/acton/attachment/11868/f-0b529250-51d1-49ea-8882-0f8ccba042e4/1/-/-/-/-/Clavis%20XG%20QKD%20System_Brochure.pdf, accessed: Apr. 11, 2023.

[81] Toshiba Digital Solutions Corporation, “Quantum Key Distribution > Products,” https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html, accessed: Apr. 11, 2023.

[82] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Review of Modern Physics*, vol. 81, no. 3, p. 1301, 2009.

[83] K. Nguyen, G. V. Assche, and N. J. Cerf, “Side-information coding with turbo codes and its application to quantum key distribution,” in *Proc. International Symposium on Information Theory and its Applications*, 2004.

[84] D. Elkouss, J. Martinez-mateo, and V. Martin, “Information reconciliation for quantum key distribution,” *Quantum Information & Computation*, vol. 11, no. 3, p. 226–238, Mar. 2011.

[85] P. Jouguet and S. Kunz-Jacques, “High performance error correction for quantum key distribution using polar codes,” *Quantum Information & Computation*, vol. 14, no. 3–4, p. 329–338, Mar. 2014.

[86] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” *Physical Review A*, vol. 72, p. 012332, Jul 2005.

[87] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” in *Advances in Cryptology — EUROCRYPT*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[88] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Physical Review Letters*, vol. 85, pp. 441–444, Jul 2000.

[89] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, pp. 145–195, Mar 2002.

[90] D. Gottesman and H.-K. Lo, “Proof of security of quantum key distribution with two-way classical communications,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 457–475, 2003.

[91] H. F. Chau, “Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate,” *Physical Review A*, vol. 66, p. 060302, Dec 2002.

[92] J. Bae and A. Acín, "Key distillation from quantum channels using two-way communication protocols," *Physical Review A*, vol. 75, p. 012334, Jan 2007.

[93] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication," *Physical Review A*, vol. 76, p. 032312, Sep 2007.

[94] S. T. Ben Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *International Conference on New Technologies, Mobility and Security*, 2009, pp. 1–5.

[95] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[96] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[97] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1578–1588, 2012.

[98] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. IEEE INFOCOM*, 2013, pp. 2283–2291.

[99] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *IEEE International Symposium on Information Theory*, 2006, pp. 2593–2597.

[100] S. P. Mohana, *Fading and Shadowing in Wireless Systems*. Cham, Switzerland: Springer International Publishing, 2017.

[101] T. S. Rappaport, *Wireless communications, Principles and Practices*. Upper Saddle River, NJ, USA: Prentice Hall, 2002.

[102] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Communications Letters*, vol. 21, no. 4, pp. 961–964, 2017.

[103] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: Proximity-based secure pairing using ambient wireless signals." New York, NY, USA: Association for Computing Machinery, 2011.

[104] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3442–3451, 2014.

[105] Infineon Technologies AG, "BAR88-02V silicon PIN diode, product info," https://www.infineon.com/cms/en/product/rf-wireless-control/rf-diode/rf-pin-diode/antenna-switch/bar88-02v/, accessed: Jul. 2, 2022.

[106] Analog Devices, Inc., "HMC270A datasheet and product info," https://www.analog.com/en/products/hmc270a.html#product-overview, accessed: Dec. 12, 2022.

[107] S. S. Gao, Q. Luo, and F. Zhu, *Circularly polarized antennas*. John Wiley & Sons, 2013.

[108] N. Lütkenhaus, “Estimates for practical quantum cryptography,” *Physical Review A*, vol. 59, pp. 3301–3319, May 1999.

[109] M. J. Gander and U. M. Maurer, “On the secret-key rate of binary random variables,” in *Proc. IEEE International Symposium on Information Theory*, 1994, p. 351.

[110] 3GPP TSG RAN, “TR38.901 V16.1.0 study on channel model for frequencies from 0.5 to 100 GHz,” Tech. Rep., 2019.

[111] S. Jaeckel, K. Raschkowski, K. Börner, and L. Thiele, “QuaDRiGa - Quasi Deterministic Radio Channel Generator, user manual and documentation,” Fraunhofer Heinrich Hertz Institute, Tech. Rep. v.2.6.1, 2021.

[112] V. Kulkarni, M. Kulkarni, and A. Pant, “Survey of personalization techniques for federated learning,” in *Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 794–797.

[113] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara, “High-throughput semi-honest secure three-party computation with an honest majority,” in *Proc. ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 805–817.

[114] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, “Inference attacks against collaborative learning,” *preprint arXiv:1805.04049*, vol. 13, 2018.

[115] L. Su and J. Xu, “Securing distributed machine learning in high dimensions,” *preprint arXiv:1804.10140*, 2018.

[116] I. Giacomelli, S. Jha, M. Joye, C. D. Page, and K. Yoon, “Privacy-preserving ridge regression with only linearly-homomorphic encryption,” in *International Conference on Applied Cryptography and Network Security*. Springer, 2018, pp. 243–261.

[117] Y. Aono, T. Hayashi, L. Trieu Phong, and L. Wang, “Scalable and secure logistic regression via homomorphic encryption,” in *Proc. ACM Conference on Data and Application Security and Privacy*, 2016, pp. 142–144.

[118] M. Kim, Y. Song, S. Wang, Y. Xia, and X. Jiang, “Secure logistic regression based on homomorphic encryption: Design and evaluation,” *JMIR medical informatics*, vol. 6, no. 2, p. e19, 2018.

Aalto-DT 83/2023

ISBN 978-952-64-1296-2 (printed)
ISBN 978-952-64-1297-9 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

Aalto University
School of Electrical Engineering
Department of Information and Communications Engineering
www.aalto.fi

BUSINESS + ECONOMY

ART + DESIGN + ARCHITECTURE

SCIENCE + TECHNOLOGY

CROSSOVER

DOCTORAL THESES