Thesis for the Degree of Doctor of Philosophy

Be More and Be Merry:

Enhancing Data and User Authentication in Collaborative Settings

Elena Pagnin

Department of Computer Science and Engineering
Chalmers University of Technology
Gothenburg, Sweden 2018

Be More and Be Merry: Enhancing Data and User Authentication in Collaborative Settings

Elena Pagnin

ISBN: 978-91-7597-774-4
Series number: 4455

Technical report 157D
ISSN0346-718X

Department of Computer Science and Engineering
Chalmers University of Technology
SE-412 96 Gothenburg, Sweden
Phone: +46 (0)31-772 10 53

Author e-mail: elenap@chalmers.se, pagnin.elena@gmail.com

Printed by Chalmers Reproservice
Gothenburg, Sweden 2018

Abstract

Cryptography is the science and art of keeping information secret to un-intended parties. But, how can we determine who is an *intended* party and who is not? Authentication is the branch of cryptography that aims at confirming the source of data or at proving the identity of a person. This Ph.D. thesis is a study of different ways to perform *cryptographic authentication of data and users*.

The main contributions are contained in the six papers included in this thesis and cover the following research areas: (i) *homomorphic authentication*; (ii) *server-aided verification of signatures*; (iii) *distance-bounding authentication*; and (iv) *biometric authentication*. The investigation flow is towards collaborative settings, that is, application scenarios where different and mutually distrustful entities work jointly for a common goal. The results presented in this thesis allow for secure and efficient authentication when more entities are involved, thus the title "*be more and be merry*".

Concretely, the first two papers in the collection are on homomorphic authenticators and provide an in-depth study on how to enhance existing primitives with *multi-key* functionalities. In particular, the papers extend homomorphic signatures and homomorphic message authentication codes to support computations on data authenticated using different secret keys. The third paper explores signer *anonymity* in the area of server-aided verification and provides new secure constructions. The fourth paper is in the area of distance-bounding authentication and describes a generic method to make existing protocols not only authenticate direct-neighbors, but also entities located *two-hop* away. The last two papers investigate the *leakage of information* that affects a special family of biometric authentication systems and how to combine verifiable computation techniques with biometric authentication in order to mitigate known attacks.

Keywords: Homomorphic Signatures, Server-Aided Verification, Verifiable Computation, Distance-Bounding Authentication Protocols, Biometric Authentication.

List of Publications

This Ph.D. thesis comprises a collection of six scientific articles devoted to exploring data and user authentication in different settings. References to these papers will be made using the associated Latin letters. The settings considered in this thesis are: authentication of computations on signed data (**Paper A** and **Paper B**); lightweight verification of data authenticity (**Paper C**); distance-bounding authentication (**Paper D**); and biometric authentication (**Paper E** and **Paper F**). The aforementioned articles are published at the following venues:

Paper A [39] *Multi-Key Homomorphic Authenticators.* D. Fiore, A. Mitrokotsa, L. Nizzardo, and E. Pagnin. In the 22nd International Conference on the Theory and Application of Cryptology and Information Security (asiacrypt), 2016.

Paper B [40] *Matrioska: A Compiler for Multi-Key Homomorphic Signatures.* D. Fiore and E. Pagnin. In the 11th Conference on Security and Cryptography for Networks (scn), 2018.

Paper C [72] *Anonymous Single-Round Server-Aided Verification of Signatures.* E. Pagnin, A. Mitrokotsa, and K. Tanaka. In the 5th International Conference on Cryptology and Information Security (latincrypt), 2017.

Paper D [86] *Two-hop Distance-Bounding Protocols: Keep your Friends Close.* A. Yang, E. Pagnin, A. Mitrokotsa, G. Hancke, and D. S. Wong. In IEEE Transactions on Mobile Computing (17:7), 2018.

Paper E [68] *On the Leakage of Information in Biometric Authentication.* E. Pagnin, C. Dimitrakakis, A. Abidin, and A. Mitrokotsa. In the 15th International Conference on Cryptology in India (indocrypt), 2014.

Paper F [70] *Revisiting Yasuda et al.'s Biometric Authentication Protocol: Are you Private Enough?* E. Pagnin, J. Liu, and A. Mitrokotsa. In the 16th International Conference on Cryptology and Network Security (cans), 2017.

Other articles published during my Ph.D., but not included in this thesis, are:

[67] *HIKE: Walking the Privacy Trail.* E. Pagnin, C. Brunetta, and P. Picazo-Sánchez. In the 17th International Conference on Cryptology and Network Security (cans), 2018.

[74] *HB+DB: Distance-Bounding Meets Human Based Authentication.* E. Pagnin, A. Yang, Q. Hu, G. Hancke, and A. Mitrokotsa. In Future Generation Computer Systems, 2018.

[**71**] *Privacy-Preserving Biometric Authentication: Challenges and Directions*. E. Pagnin and A. Mitrokotsa. In Security and Communication Networks, 2017.

[**69**] *Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-hop Neighbours*. E. Pagnin, G. Hancke, and A. Mitrokotsa. In IEEE Communications Letters, 2015.

[**73**] *HB+DB, Mitigating Man-in-the-Middle Attacks against HB+ with Distance-Bounding*. E. Pagnin, A. Yang, G. Hancke, and A. Mitrokotsa. In ACM Security & Privacy in Wireless and Mobile Networks (wisec), 2015.

[**4**] *Attacks on Privacy-Preserving Biometric Authentication*. A. Abidin, E. Pagnin, and A. Mitrokotsa. In the 19th Nordic Conference on Secure IT Systems (nordsec), 2014.

Acknowledgements

Der är lätt att vara efterklok.

Elena Pagnin

First and foremost, I want to thank my advisor Andrei Sabelfeld, who took over the supervision of my Ph.D. studies *in media res* and steadily supported me. Your joy and enthusiasm for research lit up my path in its darkest hour and made me regain passion for academic work. I also wish to express my deep gratitude and respect to my co-supervisor, mentor and guide Dario Fiore. It has been an honor to work with you, to learn from you and to have your valuable advice. I could not imagine having a better mentor than you. Besides my supervisors, I would like to thank David Sands, who kindly agreed to become my Ph.D. examiner. Your knowledge and experience were fundamental to set the quality bar of my research.

Next, a spacial thanks goes to Bart Preneel for accepting to be my Ph.D. opponent. You made me rediscover the pleasure of pen-and-paper feedback, including human-based handwriting decryption. I also gratefully acknowledge the grading committee members: Claudio Orlandi, Damien Vergnaud and Martin Hell for their positive and encouraging comments on this thesis.

My Ph.D. studies have been sprinkled with long research visits and several conferences. Adding-up, I have been working away from Sweden for over one year! Nonetheless, in the last period I found two good reasons for doing research within Chalmers: Carlo Brunetta, Pablo Picazo-Sánchez and his little son Óliver (they count as one entity). I will cherish the memories of our morning 'Kaffe?' messages, leading to long 'coffee breaks' that inevitably turned into lively research discussions. I am happy I met both of you. I am deeply grateful for our friendship and for the constructive camaraderie we have when working together. I would also like to mention another co-author and friend: Cristina Onete, who has my gratitude for opening my mind to new, exciting research horizons despite my initial reluctance. I admire your immense knowledge, passion, enthusiasm and helpfulness. It is always a pleasure to hard work with you, even when it leads to long-lasting discussions via Skype! My sincere thanks go also to Aysajan Abidin, Luca Nizzardo, Keisuke

Tanaka and Gerard Hancke for our fruitful collaborations.

Looking back at these last four years, there are still people within Chalmers whom I owe acknowledgement. Olaf Landsiedel, for our open exchange of opinions behind closed doors. Wolfgang Ahrendt, for shedding light on my ethical dilemmas. Agneta Nilsson and Mary Sheeran, for lending me their ears and guiding me to a better life. I can not thank you enough for what you did for me. Tomas Olovsson, for his help, support and especially the countless hours spent together trying to figure out positive solutions to negative situations. And last but not least at Chalmers, I want to say *tack* to all the secretaries of the Computer Science and Engineering Department who every day do an amazing work keeping all the paperwork running. I have never met such a devote, efficient and kind stuff. In particular, my thanks go to Eva Axelsson, Marianne Pleen-Schreiber, Elisabeth Kegel Andreasson, Rebecca Cyren, Anneli Andersson and Tiina Rankanen.

A heartfelt mention goes to my friends, including Cecilia, Guilhem, Inari, Irene, Iulia, Jeff, Marta, Micał, Thomas, Valentina, Wouter. You have been there when needed throughout all of these years, independently of where on Earth I was. Thank you for the many cooking sessions, board game evenings, hikes, saunas, *fika*s, proof-readings, sailings, fermentation parties and traditional Scandinavian activities such as *midsommar* fireplaces and berry picking. Above all, I am glad our paths have crossed and we have walked together along the way.

Loving thanks go to my *sambo* Hedvig Maria Jonsson, for her truthful support, encouragement and endless patient during the last half of my Ph.D. You managed to give me a constant motivation for going back to Sweden and made me start liking this Nordic country. Thank you for being part of my life, and for being stubborn ♡

I reserve the final thanks for the people without whom I most probably would not be where and who I am now: Frédérique Oggier, Mariuccia Paoletti, Marc Stöttinger, Arianna Pagnin, Annamaria Borgato, Lorenzo Pagnin and Aikaterini Mitrokotsa. I hope you can be proud and feel part of my achievement.

Contents

List of Abbreviations

BAP:	Biometric Authentication Protocol.
DBAP:	Distance-Bounding Authentication Protocol.
FHS:	Fully Homomorphic Signature (Scheme).
HA:	Homomorphic Authenticator.
HS:	Homomorphic Signature (Scheme).
MAC:	Message Authentication Code.
MK-HA:	Multi-Key Homomorphic Authenticator.
NP:	Non-deterministic Polynomial time.
Ph.D.:	Doctor of Philosophy (from the Latin *Philosophiae Doctor*).
RFID:	Radio Frequency IDentification.
SAV:	Server-Aided Verification.
SNARK:	Short Non-interactive ARgument of Knowledge.

Part I

Thesis Summary

Introduction

Man is by nature a social animal; an individual who is unsocial naturally and not accidentally is either beneath our notice or more than human.

Aristotle, Politics

The social nature of human beings renders communicating and storing information two essential needs for surviving. Knowing where to go, who people are, asking for clarifications and providing instructions is something we do everyday. In developed countries, the society has taken a *digital* approach: people 'talk' to each other in chats, e-mails or video-calls; and save information they want to 'remember' on smartphones or cloud back-ups. The migration to digital platforms has increased the demand for digital interaction and storage methods that achieve features similar to or better than face-to-face conversations and personal memory. Common concerns are: how can we be sure of the identity of our digital interlocutor, does someone else know what we are talking about; or what guarantees the stored data are always available to us only and not modified without us noticing? Cryptography addresses these and more concerns by keeping information secret to un-intended receivers and allowing secure communication in the presence of untrusted parties [47].

The Cryptographers' World

My parents' generation grew up having face-to-face as the most common way to communicate. For them it was clear who they were talking to and where and when the conversation was taking place. Thus, my parents could easily adjust the content and style of the conversation according to the circumstance. If they had to discuss something private or secret, they would ask to meet in a remote location, or in a place surrounded by people that had no interest in their secret. They would use letters or wired telephones to contact people who were far-away. In the first case, they would not know whether the letter reached its destination until they received a response (and recognized the sender's handwriting); in the second case, they were extremely suspicious on who was listening *inside* the telephone line, but still they were happy they could recognize the interlocutor by hearing their voice. Important information was either learned by heart or written on a piece of paper they would hide somewhere safe to make sure no-one would access it.

My generation is quite different. We were born with modern computers and digital technologies. We are used to asynchronous communications via e-mail and to instant messaging in social networks. Our most common way of communicating is in virtual environments. In particular, we almost never *see* or *hear* our interlocutors

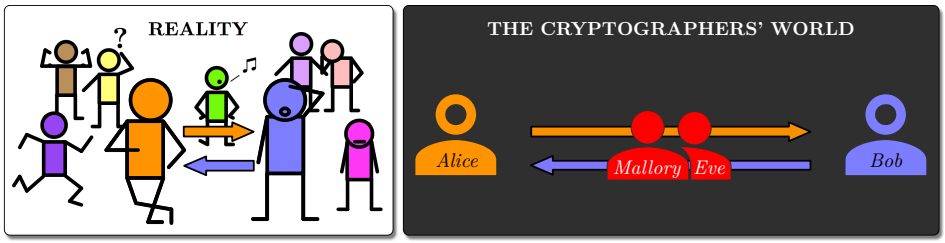

Figure 1: Quirky representation of some differences between the *real-* and the *cryptographers'* (perception of the) world.

in real time and have no way to determine when and where a piece of information is delivered or received. Regarding sensitive data, we may try to learn it by heart, but it is so much easier and handier to store it on our smartphones, computers or directly in the cloud! Therefore, in contrast to my parents, I find it very hard to know for sure who I am writing to, to adjust the content and style of my conversations or to make sure no-one can find my secret data. However, I would still like to have the same guarantees as my parents had. This is what cryptography tries to achieve.

In a nutshell, the cryptographer's world is looking at our digital world with some privacy-paranoid glasses, as figuratively depicted in Figure 1. In cryptography, the *talking* entity magically becomes Alice and has an urge to communicate highly sensitive information to another person, named Bob, who is located far, far away from her. Everyone around them turns into an evil being, Eve or Mallory according to the story, and is suspiciously interested in the content of Alice and Bob's conversation. This setting is formalized in the concept of *communication over an insecure channel*.

Investigating how paranoid the cryptographers' world can be is a Ph.D. on its own and falls outside the scope of this thesis. During my Ph.D., I regarded the cryptographers' view of the world as fascinating and immersed myself in it with the objective to develop some tools that would render it a brighter reality. To this aim, I collect in this thesis new proposals for data and user authentication. Concretely, the presented contributions can be used to ensure Alice that she is talking to Bob and not to Eve, and that her data have not been modified by Mallory.

The Main Security Goals of Cryptography

Cryptographic primitives and protocols are designed to maintain a desired set of security goals even under attempts at making them deviate from the expected functionality. We briefly describe the two most common security goals in the paragraphs below [81] assuming that an entity called Alice wants to communicate with another entity called Bob in the presence of an undesired party called, generically, the adversary.

Confidentiality. This is the main idea people associate to the term "Cryptography". In a nutshell, if a cryptographic scheme or protocol achieves confidentiality it means that Alice is able to send messages to Bob in such a way that only Bob can read the messages and no adversary is able to see the actual content of their communication. Encryption is the queen cryptographic primitive for confidentiality.

Authentication. This property can refer to both data and user authentication. In the case of user authentication, this functionality ensures that a certain person, *e.g.,* Alice, is who she claims to be. For message authentication, the goal is to provide some additional information that guarantees to Bob that the message he received was originated by Alice. In particular, no undesired third party should be able to impersonate Alice. Digital signatures and Message Authentication Codes (MAC) are the two knights cryptographic primitives that grant data authentication. Regarding user authentication, in this thesis we consider the case of distance-bounding and biometric protocols.

Confidentiality and authentication are the two main security goals of cryptography, however, there are other useful functionalities that cryptographic primitives and protocols can guarantee, such as: integrity [9], non-repudiation [27], controlled malleability [44], redactability [24], delegation [61], attribute-based confidentiality [50], proofs of knowledge [76], availability and proofs of work [55], and more. This Ph.D. thesis focuses on authentication and data integrity.

Why Authentication?

More than forty years ago, Diffie and Hellman flagged that authentication was perhaps the main barrier to the universal adoption of digital communications for sensitive data (*e.g.,* business transactions) and that it constituted the heart of any system involving 'contracts and billing' [37]. These statements acted as a spring for the development of (asymmetric) cryptographic tools for user authentication as well as data authentication, integrity and non-repudiation.

My Ph.D. has *authentication* as main topic. The real reason for which I chose to devote these years of my life to studying and (hopefully) contributing to the area of authentication is that I believe that (public-key) encryption looses large part of its usefulness if it is not combined with some sort of authentication. For instance, if I had a sensitive conversation about my health condition, I would *first* make sure that my interlocutor is my doctor –and not some impostor sending fake news to me– and only *secondly* that the conversation is encrypted (thus intelligible only to the doctor and me). Having reliable and secure authentication has become even more relevant thanks to the technological development we have witnessed in the last decades. Nowadays, authentication is a fundamental step in services such as online banking, e-health, e-commerce, automatized border controls and many more. My Ph.D. goal was therefore to get acquainted with known ways to achieve data and user authentication, to propose new solutions and to extend existing ones to collaborative scenarios, where multiple entities want to contribute to a joint cause. The main results of my work are collected into this Ph.D. thesis.

Thesis Overview

This thesis collects the major results I obtained during my Ph.D. at Chalmers University of Technology. The title *be more and be merry* captures the core idea of my works: guaranteeing that certain cryptographic primitives and protocols remain secure even in enhanced environments that involve a number of entities larger than the standard one. This is the case of collaborative scenarios such as team-work activity or sensor networks.

The thesis is organized in two parts. The first part begins with a high-level introduction, some background notions and a brief summary of the results. It concludes with an outlook on directions for future work. The second part of the thesis is a collection of six papers on data and user authentication in collaborative settings including sharing computation on data, taking over specific tasks, or enabling communication. Figure 2 displays connections among the published works I contributed to during my Ph.D. and groups them by topic.

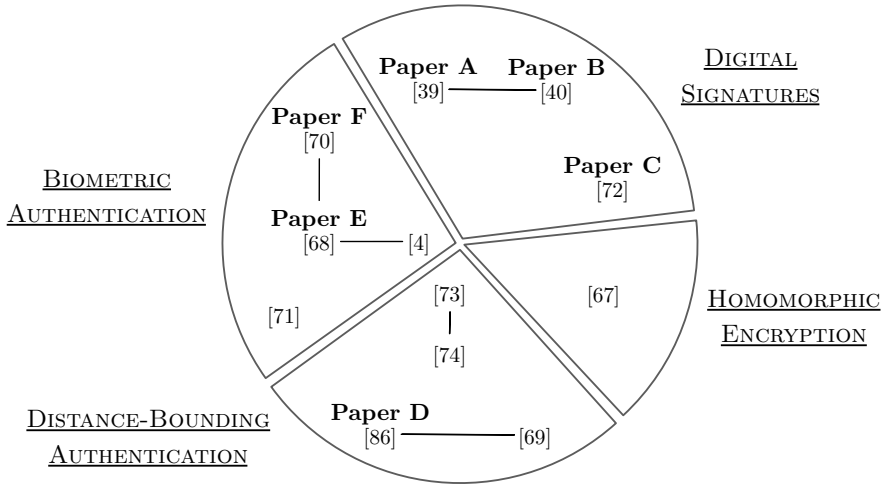

Figure 2: Pie diagram of my publications during the Ph.D. Lines between papers display logical connections among the results contained therein.

In detail, **Paper A** [39] and **Paper B** [40] provide ways for authenticating *computations* on data generated by *multiple users*; **Paper C** [72] investigates how to improve the efficiency and anonymity in settings where the verification of signatures is offloaded to an *untrusted server*. **Paper D** [86] and [69] extend the notion of distance-bounding to a collaborative setting by relying on an *untrusted linker* for authenticating an out-of-reach entity. In the same research area, [73, 74] propose a new authentication protocol that mitigates known attacks against the HB protocol [58]. **Paper E** [68], **Paper F** [70] and [4, 71] address issues in *biometric* authentication protocols. Finally, [67] is my most recent work and falls outside the wide area of authentication. It considers the problem of privacy-preserving processing of outsourced data in the context of user-customised services and develops a new lightweight protocol for private and secure storage, computation and disclosure of users' data.

Background

Cryptography is about communication
in the presence of an adversary.

Goldwasser and Bellare [47]

This section provides high-level and concise introductions to the four main areas of contributions of this thesis, namely: homomorphic signatures, server-aided verification, distance bounding authentication and biometric authentication. The reader is assumed to be familiar with basic concepts of public-key cryptography [47].

Homomorphic Signatures

Digital Signatures [18, 25, 48] enable the holder of a secret key to sign messages in such a way that anyone in possession of the corresponding public verification key can determine the validity of a given message-signature pair. For security, it is required that the signature is unforgeable, *i.e.,* no efficient adversary can forge a valid signature (unless the adversary knows the secret key).

Consider the use case of a school database for students' grades. To prevent students from tampering with their results, each teacher uploads a grade together with a signature (for the student and the grade). The unforgeability property ensures that students cannot arbitrarily change their grades, however, it also limits the utility of the database. For instance, if the school director wants to check the average of the students' grades on a certain subject, she would need to download all the grade-signature pairs related to the subject, check the authenticity of each grade and then compute the average on the (now certified) values. This procedure is quite inconvenient, since the grades need to be checked *before* computing the average, and has a high communication cost, due to the fact that *all* signed data need to be downloaded. A more desirable solution would allow the school director to download directly the average grade together with *one* signature attesting that the returned value is the correct one according to the grades available in the school database, and digitally signed by the legitimate teacher (see Figure 3). Such a scheme would have somehow *malleable* signatures, *i.e.,* signatures that support computation on authenticated data. This kind of schemes are called homomorphic signatures.

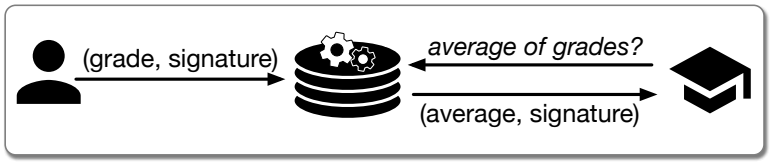

Figure 3: Application scenario for homomorphic signature schemes: a database of signed grades.

Homomorphic signature (HS) schemes [36] enable the holder of a secret key to sign messages $m_1, \ldots, m_n$ in such a way that anyone in possession of the corresponding signatures $\sigma_1, \ldots, \sigma_n$ and a function f can produce a valid signature σ for the message $y = f(m_1, \ldots, m_n)$. The key property of HS is succinctness: the size of the evaluated signature σ should be smaller than the concatenation $(\sigma_1, \ldots, \sigma_n)$ and it is usually logarithmic in n, the number of messages. In homomorphic settings the definition of unforgeability depends on the class of functions f supported by the scheme. For schemes that support only linear functions on a vector space, *e.g.,* [16], unforgeability states that the adversary should not be able to derive a correct signature for a message (vector) which cannot be obtained as a linear combination of previously honestly signed messages. If we applied the same reasoning to linearly homomorphic signatures with messages in a field or to Fully Homomorphic Signature schemes (FHS), *e.g.,* [15, 49], we would end up with a useless definition: given a pair (m, σ) it is possible to generate a valid signature σ' for any message $m' = f(m)$. Since f is any polynomial function, from a chosen m and its signature σ one can compute signatures for any message in the whole message space. A meaningful notion of unforgeability for FHS requires that the adversary should not be able to derive a valid signature σ^* for a value y^* that is not the correct output of $f(m_1, \ldots, m_n)$ [43, 49]. This notion is achieved thanks to labelled programs [43], as in FHS the signatures, the homomorphically evaluated signatures and the verification procedure all depend on the labels.

The unforgeability intuitions given in this section are approximations of the core meaning of the corresponding security notions. The formal definitions are quite elaborate and include several sub-cases (types of forgeries). We refer the readers to [16, 39, 49] for the details.

In the school database scenario, using FHS to sign the grades solves the problem of computing statistics on the performance of students in each subject. However, FHS does not directly allow to perform computations on grades signed by different teachers, leaving open the following problem:

> *How can we authenticate homomorphic computation of functions that involve data signed by different secret keys?*

To achieve this property we need to make the signature scheme not only homomorphic on the messages, but also 'flexible' enough to accommodate computations on data generated by different signers. The latter property is often referred to as *multi-key*. In **Paper A** [39], we address the above question and formalize the multi-key notion for FHS. Moreover, we provide concrete instantiations of schemes that are multi-key and homomorphic. In **Paper B** [40] we go one step further and investigate connections between single-key and multi-key homomorphic signatures.

Server-Aided Verification of Signatures

In the previous section, we mentioned how digital signature schemes have developed to support more and more advanced *homomorphic* properties. Computing on signed data, however, is not the only line of development for signature schemes. To cover the wide range of applications of this cryptographic primitive, other types of schemes have been proposed such as: ring signatures [10, 21, 62], group signatures [14, 29, 62, 63], blind signatures [2, 11, 28], attribute-based signatures [53, 65, 79], and structure preserving signatures [1, 63]. Despite the different aims, most signature schemes are designed around strong and well-established cryptographic assumptions that guarantee security at the cost of efficiency, especially in the verification process of signatures. There are three possible ways to enjoy both security

and efficiency: (i) using a different *hard problem* to design a secure signature scheme, (ii) trying to speed-up inefficient algorithms exploiting clever ways of computing the necessary data, and (iii) off-loading heavy computations to a third party and efficiently verifying the returned result. The latter approach falls into the *server-aided* category of cryptographic schemes. Since in signatures schemes the large bulk of computation is usually in the verification procedure, the main line of research is for Server-Aided signature Verification (SAV) schemes [31, 45, 83, 85]. The aim of such schemes is to reduce the gap between the computational cost of the signing algorithm and the one of the verification algorithm in pairing-based schemes. There exist also work on server-aided signature generation, however in this case the focus is not on efficiency [8, 56].

Relying on a server to carry out expensive computations is a natural solution in applications where resource-constrained devices are required to perform computations above the device capacity. From this point of view, server-aided verification renders computationally heavy signatures accessible to a wide range of resource-limited devices (*e.g.,* smartcards, small-battery smartphones) without affecting the device's performance or battery life. The idea behind this solution is to replace the verification algorithm of a signature scheme with an interactive protocol between the computationally weak verifier and the computationally powerful but untrusted server (see Figure 4).

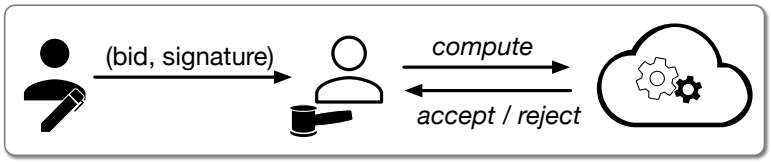

Figure 4: Application scenario for server-aided verification: signed auctions.

A bit more formally, SAV exploits the fact that the verification algorithm of any signature scheme can be split into two parts: a computationally expensive part (that includes most of the operations performed for the verification) and a lightweight equality-check part (see Figure 5). The aim is to replace the computationally expensive part with an interactive protocol that has the same functionality and is more efficient (at least in terms of computational cost for the delegator-verifier). Involving one more entity in the signature verification introduces new privacy and security concerns.

$$\mathsf{SetUp}(1^\lambda) \rightarrow \mathsf{gp} = \mathsf{BilinGroup}$$
$$\mathsf{KeyGen}(\mathsf{gp}) \rightarrow \mathsf{pk} = g^{\mathsf{sk}},\ \mathsf{sk} \leftarrow \mathbb{Z}_p$$
$$\mathsf{Sign}(\mathsf{sk}, m) \rightarrow \sigma = \mathsf{Hash}(m)^{\mathsf{sk}}$$
$$\mathsf{Verify}(\mathsf{pk}, m, \sigma) \rightarrow e(\sigma, g) \stackrel{?}{=} e(\mathsf{Hash}(m), \mathsf{pk})$$

Figure 5: The BLS [17] signature scheme. The expensive computations in the verification algorithm are highlighted with gray background. SAV schemes aim at reducing the gap between the computational cost of Sign and Verify.

There have been some attempts to provide a formal security framework for server-aided verification of signatures [31, 84, 85] and **Paper C** contributes to this line by proposing a more realistic security model and new SAV schemes that achieve stronger notions of security and privacy.

Distance-Bounding Authentication Protocols

Distance-Bounding Authentication Protocols (DBAP) [5, 20] are two-party interactive protocols that allow one entity (called the prover) to authenticate to a verifier under the following conditions: (1) the prover is legitimate and (2) the prover lies within a fixed radius from the verifier. The first condition is checked using a challenge-response approach: the verifier sends a (usually one-bit) challenge c, the prover computes the (usually one-bit) response r using a secret key and some light-weight cryptographic tools. The second condition is checked by equipping the verifier with a clock and measuring the time elapsed between sending c and receiving r. To prove its proximity to the verifier, the prover computes its r immediately after receiving c. To increase accuracy, DBAPs run a series of rapid challenge-response exchanges between the verifier and the prover. Figure 6 depicts the setting of DBAPs. In a nutshell, distance-bounding authentication protocols

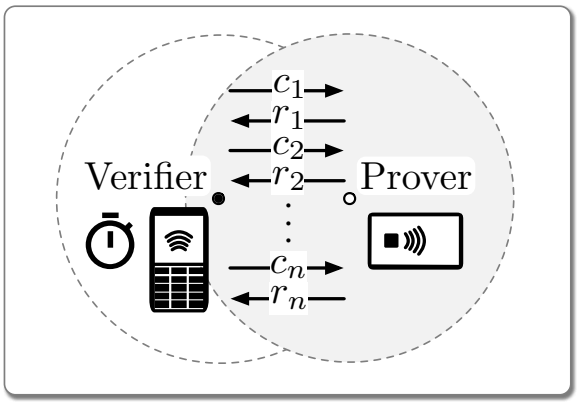

Figure 6: Schematic explanation of distance-bounding authentication. The verifier is a terminal for contact-less payments, the prover is a contact-less smartcard.

blend cryptographic primitives with timing tools to achieve accurate authentication. This dual nature is motivated by real world needs: DBAPs represent the best mitigation against severe attacks such as the ones described below.

Contact-less debit-cards, credit-cards and smartcards in general were designed to bring together security and usability. The chip present in contact-less cards is able to carry out quite sophisticated cryptographic computations once it is brought to life by a magnetic field. In order to authorize the card functionality (*e.g.,* small financial transactions) cardholders need to simply wave the card in front of a terminal machine (*e.g.,* point-of-sale). Within a few seconds the smartcard and the terminal *communicate* with each other and determine whether the functionality (*e.g.,* payment) was successful or not. Unfortunately, the most common contact-less EMV[1] payment protocols (Visa's payWave and MasterCard's PayPass) have flaws and have been shown vulnerable to relay attacks [13, 30, 38] that can be performed even with smartphones [66]. Such attacks may lead to undesirable consequences including changing the amount being charged or the party to be paid. For instance, a businessman seated in a café with his contact-less credit card 'safely' put in his pocket, may be the victim of an attack where an antenna bridges the communication between a contact-less terminal in the jewellery shop next to the café and the businessman's card. By relaying the communication through the antenna, the attacker in the shop may be able to pay the jewellery with the businessman's money! Similar

[1] EMV stands for Europay, MasterCard, and Visa.

attacks have been setup to amplify the communication range of RFID car-keys and unlock cars, while the keys were not in their physical proximity [41].

Relay attacks are a special family of man-in-the-middle attacks where the attacker bridges communications between two parties (the victims). Concretely, the relay-attacker is in communication with both parties and merely relays messages between the victims without manipulating them or even necessarily reading them. What makes relay attacks so dangerous is that in order to tamper with the protocol the adversary does not need to know the details of the protocol or to break the underlying cryptographic functions, it simply relays messages. A quaint example of relay attack is the little girl playing against two chess masters [33]. All the little girl needs to do is to challenge two Grandmasters at postal chess and relay moves between them. Without knowing the rules of the game, the little girl will win (or have a tie) in one of the two games.

The only way to distinguish a response that is being relayed from one that is directly sent by the card to the terminal is to measure how long it takes for the response to reach the terminal. As contact-less communication happens at most at the speed of light, accurate clocks would be able to detect a time difference that corresponds to half a meter space [20]. Therefore, a protocol that combines light-weight cryptographic functions with physical time measurements represents the natural solution against relay attacks. The keyed cryptographic functions are used in a challenge-response framework to authenticate the prover (*e.g.,* a contact-less smartcard) while the recorded round-trip-times of the communication provide an upper-bound on the maximal distance between the prover and the verifier (*e.g.,* contact-less card reader). These are exactly the characteristics of distance-bounding protocols.

Brands and Chaum's seminal work on distance-bounding [20] was followed by a long series of proposals [19, 51, 59, 74]. **Paper D** [86] provides the first formal framework to describe the main classes of existing distance-bounding protocols and also puts forward a general method to extend traditional prover-verifier protocols to the three-participant setting of prover-linker-verifier (two-hop distance estimation).

Biometric Authentication Protocols

While distance-bounding protocols authenticate a user (the prover) via a device she holds, biometric-based authentication relies solely on the user's human features. Biometric Authentication Protocols (BAP) allow quick, accurate and user-friendly authentication of people. In a nutshell, all you need to do is to provide the system with one biometric trait (*e.g.,* your fingerprint or iris scan) and from that point on the system is able to recognize you. In general, biometric traits are distinctive characteristics that are measurable and identify (almost) uniquely each individual. Therefore by measuring a fresh biometric template and comparing it with a reference, the system can recognize people and reject impostors claiming to be someone they are not. Common biometric credentials are: fingerprint [88], iris [35], and face shape [78].

Figure 7 provides a high-level intuition of the main aspects of biometric authentication. To give a concrete example, consider an access gate to a military facility. The gate is equipped with a sensor that scans the soldiers' iris. The iris scan transforms the biometric trait into a digital credential that is compared to a stored biometric template for the soldier. Access will be granted only after the person has been recognized as an authorized soldier in the military facility.

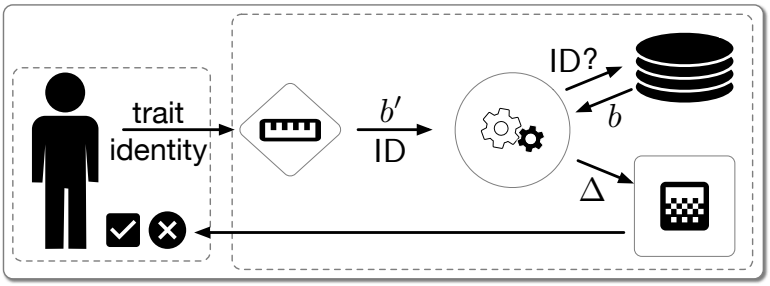

Figure 7: Schematic explanation of how biometric authentication works. The user provides a biometric trait and an identity. The sensor extracts from the trait a biometric template b' for identity ID. The system retrieves the reference template b corresponding to ID and performs a *matching process*. If b is *close enough* to b' (*i.e.,* Δ is small) the user is accepted, otherwise she is rejected.

Biometric authentication has become popular thanks to its usability and user-dependent nature, properties that cannot be achieved with classical authentication methods (*e.g.,* passwords, distance-bounding). In particular, biometric authentication removes the need for users to memorize complicated, long passwords or to carry along special secret tokens. Moreover, biometric credentials are characteristic features naturally bound to the user's body, are hard to steal, reproduce and to spoof [7, 80]. This very same advantageous property, however, raises serious security and privacy concerns in the case of a biometric trait being compromised (cloned, forged).

Unlike passwords or tokens, biometric credentials cannot be kept secret or hidden, and stolen biometrics cannot be revoked as easily [3]. Compromised biometric credentials have an even stronger impact than spoofed passwords or stolen tokens. With a stolen biometric credential attackers can perform crimes such as identity theft and individual profiling and tracking [71, 80]. Moreover, from stolen biometrics traits one can learn sensitive information about the owners, including ethnicity, genetic information [75], medical diseases [12] and can use these data to compromise health records [54].

Motivated by the high sensitivity of biometric data, in the past years several privacy-preserving biometric authentication protocols have been proposed [7, 82, 87]. Such protocols are designed to resist specific attack scenarios including the *biometric reference recovery* attack. In this attack, an unauthorized entity tries to recover the (plaintext) reference biometric template b for a target user ID. A successful reference recovery attack has particularly harmful consequences: the knowledge of the raw credential b gives unauthorized access to any system that uses b as the reference template for user ID and may additionally leak sensitive information about the user's physical characteristics and genetics.

Privacy-preserving biometric authentication protocols make use of advanced cryptographic techniques (such as Oblivious Transfer and Homomorphic Encryption) and are based on a distributed setting, where several entities take part in the protocol. The main reason for this approach is to minimize the amount of information known by each entity.

In **Paper E** [68] we generalize Abidin, Pagnin and Mitrokotsa's biometric reference recovery attack [3] to a wider family of BAPs and investigate the leakage of information that affects biometric authentication. In **Paper F** [70] we show how to mitigate Abidin's attack [3] using Verifiable Computation techniques.

Summary of Papers and Contributions

We hope this will inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly.

Diffie and Hellman, 1976 [37]

This section provides an overview of the main results of the papers included in Part II of this thesis. It also contains descriptions of my contributions to each work.

Multi-Key Homomorphic Authenticators

Problem statement and related work. Homomorphic authenticators enable a client to authenticate a large collection of data in such a way that any third party can generate a short authenticator vouching for the correctness of the output of some computation on the data and the authenticators. Previous works proposed Homomorphic signatures or homomorphic MAC schemes that could support computations of linear functions [16] or of more expressive polynomials [15, 49]. All the aforementioned schemes are however single-key, *i.e.,* computations can only be performed on data generated with a single secret key. This characteristic limits the application range of homomorphic authenticators to non-collaborative settings as it prevents the correct authentication of any computation that requires input from entities with different secret keys.

Consider the earlier example of a school database. Homomorphic signatures enable teachers to upload signed grades and anyone else (*e.g.,* the school director or the students' parents) to check for the authenticity of simple statistics on the grades. Unforgeability ensures that the students cannot upload fake grades. Homomorphic signatures schemes, however, do not directly support authenticated statistics on grades generated with different secret keys. In particular, in our example it would not be possible to authenticate the outcome of computations that involve grades by different teachers. To achieve this property, the signature scheme would need to be homomorphic even among messages signed with different secret keys, in other words, be multi-key and homomorphic.

Contributions and their implications. In this paper, we introduce the notion of Multi-Key Homomorphic Authenticators (MK-HAs), a reasonable security model for this new primitive and two independent constructions. MK-HAs extend the existing notions of Homomorphic Signatures and Homomorphic Message Authentication Codes to support computations on data generated by different secret

keys while relying on succinct authenticators, *i.e.,* the size of the authenticators depends at most logarithmically on the total number of inputs to the computation. Our Multi-Key HS scheme is based on standard lattices and supports the evaluation of circuits of bounded polynomial depth. Our construction of a Multi-Key Homomorphic MAC is particularly efficient, it is based on pseudorandom functions and supports the evaluation of low-degree arithmetic circuits.

Statement of contributions. This paper is the result of a collaboration between Dario Fiore, Luca Nizzardo, Aikaterini Mitrokotsa and myself. We developed and formalized the new primitive and its security model during my visit at IMDEA funded by CryptoAction. I mainly worked on the Multi-Key Homomorphic MAC construction and its security proofs. In addition, I proposed adding the **Z** component to the signatures of the Multi-Key HS scheme to mitigate a special family of forgeries.

Matrioska: A Compiler for Multi-Key Homomorphic Signatures

Problem statement and related work. This paper is a follow-up of our work on multi-key homomorphic authenticators [39]. Existing multi-key homomorphic signature schemes are ad-hoc adaptations of a single-key homomorphic signature [39] or derived by a generic construction that exploits strong, non-falsifiable cryptographic primitives such as SNARKs [60]. In particular, there is no formal study on the connections between multi-key and single-key HS schemes. This papers fills this gap and provides a generic compiler for constructing a secure multi-key variant of any (sufficiently expressive) single-key homomorphic signature scheme.

Contributions and their implications. In this paper, we establish formal connections between multi-key and single-key homomorphic signatures and *build a (theoretical) bridge* between these two primitives. In more details, we propose Matrioska: the first generic compiler that enhances any (sufficiently expressive) single-key HS with multi-key features under standard falsifiable assumptions only. The existence of this compiler implies that multi-key and single-key homomorphic signatures are equivalent (if they support evaluations of a special class of functions). Moreover, Matrioska can be used to define new multi-key HS schemes from any future proposal of a single-key homomorphic signature. The core of the Matrioska technique is to use the single-key homomorphic evaluation procedure in an original way that allows us to derive t signatures vouching for the authenticity of computations on an arbitrary number of signatures from t different signers. Our approach is completely different from the known ways to obtain multi-key HS schemes [39, 60].

Statement of contributions. This paper is the outcome of a joint work between Dario Fiore and myself. It is a natural follow-up to our paper on multi-key homomorphic authenticators [39] and dives in understanding the relation between single- and multi-key homomorphic signatures. My contribution in this work was to come up with the technical details that made the idea work correctly and securely. All authors contributed equally to the paper.

Anonymous Server-Aided Verification of Signatures

Problem statement and related work. Since the introduction of server-aided verification of signatures [8, 45, 64] there has been a constant development towards more efficient schemes and more realistic security models. The basic security notions for SAV are soundness and existential unforgeability [45]. Wu *et al.* [85] address for the first time attack scenarios where a malicious signer colludes with the server in order to tamper with the outcome of the server-aided verification. Chow *et al.* [31] refine previous definitions and show that the enabler of many attacks to previous SAV schemes is the absence of an integrity check on the results returned by the server. Integrity is not the only concern when outsourcing computations: *how about the signer's privacy?*

Contributions and their implications. In this paper, we provide formal definitions for known and new realistic attack scenarios against server-aided verification of signatures and propose three novel constructions of server-aided verification schemes. Concretely, we present the first compiler that defines a single-round (give-and-take) server-aided verification protocol for any signature given an appropriate verifiable computation scheme. We make use of our compiler to define new SAV schemes that are the first published proposals achieving existential unforgeability and soundness against collusion simultaneously.

In addition, we are the first to consider the notions of signer anonymity and extended existential unforgeability for SAV. To give an idea on the importance of these two attack scenarios consider the case of signed auctions, where bidders sign their bids (messages) to avoid other people impersonating them. In this setting, signer anonymity prevents a malicious server from distinguishing one signer from another. As a consequence, the server cannot 'keep out' target bidders from the auction by making their signatures appear invalid. We also provide an extension to the notion of unforgeability that additionally captures the following attack scenario. Imagine the adversary is a bidder taking part in the auction. In order to steer the price of certain items the adversary could get control over the server used for the aided verification and prevent signatures of higher bids from verifying correctly. Our compiler allows us to determine sufficient requirements on the signature scheme (and/or the verifiable computation scheme) in order to achieve security and anonymity.

Statement of contributions. This paper is the result of a study on server-aided verification of signatures started by Aiketerini Mitrokotsa and myself during a visit at Keisuke Tanaka Sensei's laboratory. Although Dario Fiore is not listed among the authors, he provided me with important technical feedback on the work. I am the main author of this work and developed all the results. This paper is of special importance within my Ph.D. because it represents my 'first step' as an independent researcher on the academic path.

Two-hop Distance-Bounding Protocols: Keep your Friends Close

Problem statement and related work. Traditional distance-bounding authentication protocols aim to authenticate a resource-constrained prover to a (more powerful) verifier [20, 51, 59, 73, 74], assuming that the prover lies within the communication range of the verifier. Albeit most DBAPs are designed for RFID tags,

there are works that consider slightly more powerful provers and define public-key privacy-preserving distance-bounding [42, 52] and group distance-bounding [26]. The common factor to all protocols, however, remains that authentication is subjected to the location of the parties: all devices must lie within each others' transmission range. While this requirement represents the main motivation for adopting distance-bounding authentication protocols as a countermeasure against relay attacks, it also limits their application scenarios. In particular, it is hard to directly employ traditional distance-bounding protocols in multiple access control scenarios, in ubiquitous computing environments and even to verify the proximity of a two-hop neighbor. Pagnin *et al.* [69] put forward the idea to extend DBAPs to two-hop neighbors, that is, when the prover and the verifier communicate through an in-between linker. However, a formal framework for constructing two-hop distance-bounding authentication from traditional DBAPs was missing.

Contributions and their implications. In this paper, we extend traditional distance-bounding authentication protocols to also authenticate two-hop neighbors, instead of adjacent devices only. This setting covers environments where the prover is out of the communication range of the verifier, but both parties lie in the proximity of the same untrusted entity, called the linker. We present an intuitive taxonomy of existing DBAPs and provide the first formal framework to extend any register-based protocol to additionally support the two-hop distance-bounding authentication. We also identify connections between attacks against the two-hop and the one-hop settings and implement five two-hop distance-bounding authentication protocols derived from the proposals in [19, 20, 59, 77] using our framework. Our experimental results demonstrate the correctness of our security analysis and the efficiency of our model.

Statement of contributions. This paper is the result of a collaboration started within the objective of a STINT grant awarded to Aikaterini Mitrokotsa and Gerhard Hancke. Anjia Yang is the first author, I am the corresponding author. My contributions in this work include the proposal of the taxonomy of existing distance-bounding authentication protocols, the development of the formalism and the description of the framework for generic extension of register-based DBAP to the two-hop setting. Additionally, I performed the formal security analysis.

On the Leakage of Information in Biometric Authentication

Problem statement and related work. User authentication via biometric credentials has become an increasingly popular way to authenticate people in highly sensitive services such as health care systems [34], but also in everyday tasks such as smartphone unlocking. If not implemented correctly, the wide adoption of these systems might raise severe concerns about the users' privacy and security. Privacy-preserving biometric authentication protocols are designed to mitigate dangerous threats including individual profiling, user tracking and leakage of sensitive information connected to biometric traits (*e.g.,* healthcare data [22, 23, 57]). The current framework for analyzing template security and privacy models distributed biometric authentication systems with internal adversaries [80]. Among the described attacks there is also the so-called center search attack.

Contributions and their implications. In this paper, we provide a formal mathematical framework to analyze the implications of center search attacks against privacy-preserving biometric authentication systems. The standard center search attack is defined on binary strings. In this work, we generalize this efficient hill-climbing technique to vectors with components in $\mathbb{Z}_q$ for $q \geq 2$. As a consequence, certain families of biometric authentication protocols become naturally vulnerable to our biometric template recovery attack. The main implication of our attack is that, if successful, it will let the adversary learn susceptible users' private data that can lead to disclosure of health condition and digital impersonation of the victim. However, not all is lost: one of the starting conditions for the attack to work is the knowledge of a biometric credential that is *close enough* to the target one. We investigated how to get such credentials in a theoretical way and showed that such a problem is equivalent to the set-covering problem which is known to be NP complete [32].

Statement of contributions. This work builds on a previous result by Abidin, Pagnin and Mitrokotsa [4] and has been developed by me, Christos Dimitrakakis, Aysajan Abidin and Aikaterini Mitrokotsa. I am the main author of this paper. I developed the way to generalize Abidin's attack to a larger setting, all the formal details and the proofs.

Revisiting Yasuda et al.'s Biometric Authentication Protocol: Are you Private Enough?

Problem statement and related work. Abidin, Pagnin and Mitrokotsa [4] showed that Yasuda *et al.*'s privacy-preserving biometric authentication protocol [87] is vulnerable to an ad-hoc biometric template recovery attack, and thus can no longer be considered fully privacy-preserving. Among the enablers of Abidin's attack is the fact that the attacker is a malicious computational server. In this paper, we redeem Yasuda's protocol and propose a mitigation to the aforementioned attack.

Contributions and their implications. In this paper, we put forward a generic strategy to transform privacy-preserving BAPs that are secure in the honest-but-curious model into schemes that can tolerate internal malicious attackers. The stronger security guarantee is derived by employing verifiable computation techniques during the matching process. Specifically, we define $\mathsf{BFR} + \mathsf{SHE}$, a biometric authentication protocol that essentially augments Yasuda *et al.*'s proposal [87] with Backes *et al.*'s verifiable computation scheme [6] and is no longer vulnerable to Abidin's attack [4].

We remark that, $\mathsf{BFR} + \mathsf{SHE}$ is still affected by the unavoidable leakage of information inherent to BAPs that employ the Hamming distance in the matching process [68]. However, for the leakage to actually happen, the adversary needs to already hold a matching template, and [68] shows that from a theoretical point of view finding a matching biometric template is an NP-hard problem.

Statement of contributions. This paper is the outcome of Jing Liu's successful master thesis project under the supervision of Aikaterini Mitrokotsa and myself. I contributed with constant support for technical matters during the development of the master thesis and shaped up the results into a publishable paper.

Conclusions and Outlook

Our research isn't finished and much is left to do
For instance, proving theorems completely in haiku

Trotta Gnam [46]

This Ph.D. thesis contributes to the body of knowledge in data and user authentication. It provides high-level explanations of four authentication methods and six state-of-the-art papers that investigate homomorphic signatures, server-aided signature verification, distance-bounding authentication and biometric authentication. This thesis brings in new constructions and aims to inspire further research.

Among the directions for future investigation that stem from the contributions of this thesis we highlight the following. **Paper A** and **Paper B** show how to construct multi-key homomorphic authenticators, but do not aim to give succinct instantiations. Constructing multi-key schemes with authenticators of size independent of the number of users involved in the computation is an open challenge, if one does not want to rely on strong cryptographic tools that are likely to be based on non-falsifiable assumptions (*e.g.,* SNARKs as proposed in [60]). Other directions of research in this area include: combining authentication and confidentiality so that the entity who runs the homomorphic evaluation (*e.g.,* the cloud) does not learn the data over which it computes; and developing *context-hiding* schemes that achieve privacy by revealing no non-trivial information about the computations' inputs. **Paper C** raises awareness about the need for more efficient verifiable computation schemes for bilinear-pairing evaluation that would render a wide range of signature schemes accessible to resource-limited devices via server-aided verification techniques. **Paper D** opens up a new scene for distance-bounding authentication and therefore calls for creative application scenarios in two-hop and multi-hop settings. Finally, **Paper E** and **Paper F** address privacy concerns in biometric authentication and identify the need for new tools to achieve non-leaky biometric template matching.

In addition to the six papers collected in Part II, during my Ph.D. I had several successful collaborations that resulted in the publications reported in the **List of Publications** at the beginning of this thesis. Figure 8 provides subway map inspired representation of my research work so far. Papers are represented as stations, and the four lines follow the paths of data/user privacy privacy, multi-key features, constrained settings and new attacks. The two, black, right-most stations in Figure 8 are outlooks of two on-going works that I describe in what follows.

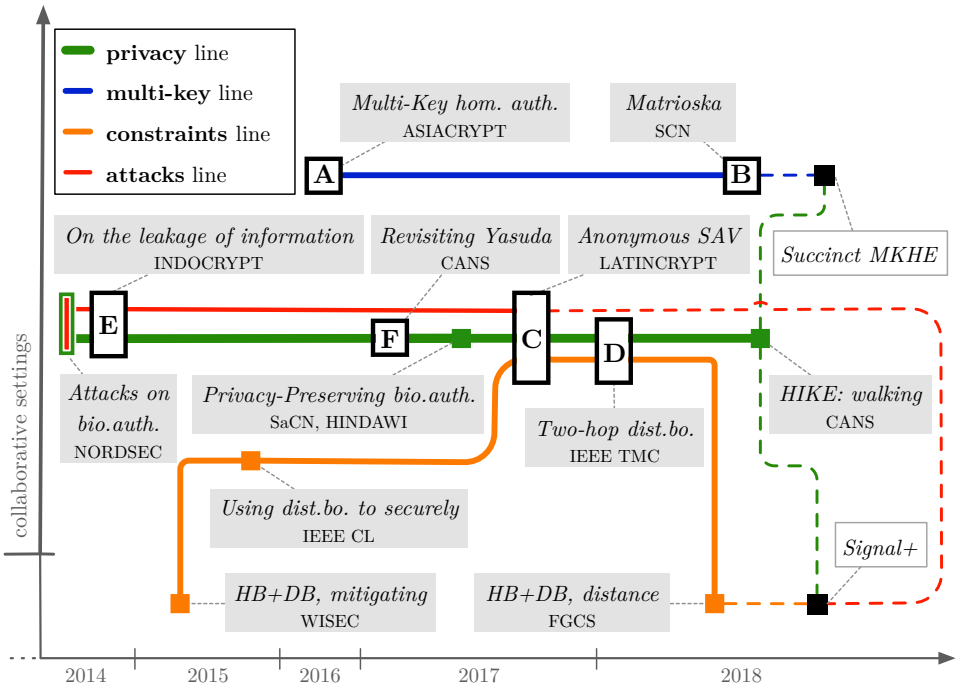

Figure 8: A subway-style map of the papers I contributed to during my Ph.D. The works are organized by the time of publication (or due date) on the x axis, and the size of the supported collaborative setting on the y axis (starting from two users and increasing progressively). Connections between papers are represented as 'subway lines' between 'stations'. The lines are named after the four main themes of my Ph.D. The Latin letters **A-F** refer to the corresponding papers appended to this thesis. Dashed lines lead to results currently under development and highlight directions for future work.

Paper *Succinct MKHE* in Figure 8 puts forward an original way to achieve fully succinct ciphertexts in multi-key additive homomorphic encryption. Exploiting the algebraic structure of some additive homomorphic encryption schemes, we define a new encryption scheme that is a hybrid of secret-key and public-key mechanisms. Our objective is to develop a scheme that supports linearly homomorphic computations on data encrypted by different users and has ciphertexts of constant-length. Paper *Signal+* investigates how to obtain secure asynchronous messaging under the presence of very powerful adversaries. The starting point is the widely deployed Signal protocol. We identify some weaknesses in the design of Signal and propose mitigations and improvements. Our two major goals are to change the trust assumptions of the Signal protocol and to develop a new approach to the ratchet mechanism that supports persistent entity authentication (partnering).

To conclude, I hope this thesis presents a pleasant tour in the land of data and user authentication. Authentication is only one side of the complex polyhedron of security goals in the cryptography world. I am confident that the authentication protocols and schemes we have now and will develop in the future will allow us to happily and safely collaborate in this digital Era even under the presence of malicious entities. Thus, I wish you all to *be more and be merry!*

Bibliography

[1] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. "Structure-Preserving Signatures and Commitments to Group Elements". In: *CRYPTO 2010*. Ed. by Tal Rabin. Vol. 6223. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2010, pp. 209–236.

[2] Masayuki Abe and Tatsuaki Okamoto. "Provably Secure Partially Blind Signatures". In: *CRYPTO 2000*. Ed. by Mihir Bellare. Vol. 1880. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2000, pp. 271–286.

[3] Aysajan Abidin and Aikaterini Mitrokotsa. "Security Aspects of Privacy-Preserving Biometric Authentication Based on Ideal Lattices and Ring-LWE". In: *Information Forensics and Security (WIFS), 2014 IEEE International Workshop on*. IEEE. 2014, pp. 60–65.

[4] Aysajan Abidin, Elena Pagnin, and Aikaterini Mitrokotsa. "Attacks on Privacy-Preserving Biometric Authentication". In: *Proceedings of the 19th Nordic Conference on Secure IT Systems (NordSec 2014)*. Springer. 2014, pp. 293–294.

[5] Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş, Cédric Lauradoux, and Benjamin Martin. "A Framework for Analyzing RFID Distance Bounding Protocols". In: vol. 19. 2. IOS Press, 2011, pp. 289–317.

[6] Michael Backes, Manuel Barbosa, Dario Fiore, and Raphael M. Reischuk. "ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data". In: *2015 IEEE Symposium on Security and Privacy*. San Jose, CA, USA: IEEE Computer Society Press, 2015, pp. 271–286.

[7] Manuel Barbosa, Thierry Brouard, Stéphane Cauchie, and Simão Melo de Sousa. "Secure Biometric Authentication with Improved Accuracy". In: *ACISP 08*. Ed. by Yi Mu, Willy Susilo, and Jennifer Seberry. Vol. 5107. LNCS. Wollongong, Australia: Springer, Heidelberg, Germany, 2008, pp. 21–36.

[8] Philippe Béguin and Jean-Jacques Quisquater. "Fast Server-Aided RSA Signatures Secure Against Active Attacks". In: *CRYPTO'95*. Ed. by Don Coppersmith. Vol. 963. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 1995, pp. 57–69.

[9] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. "A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols (Extended Abstract)". In: *30th ACM STOC*. Dallas, TX, USA: ACM Press, 1998, pp. 419–428.

[10] Adam Bender, Jonathan Katz, and Ruggero Morselli. "Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles". In: *TCC 2006*. Ed. by Shai Halevi and Tal Rabin. Vol. 3876. LNCS. New York, NY, USA: Springer, Heidelberg, Germany, 2006, pp. 60–79.

[11] Alexandra Boldyreva. "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme". In: *PKC 2003*. Ed. by Yvo Desmedt. Vol. 2567. LNCS. Miami, FL, USA: Springer, Heidelberg, Germany, 2003, pp. 31–46.

[12] James Bolling. "A Window to Your Health". In: *Special Issue: Retinal Diseases: Capacity and Examples Jacksonville Medicine* 51.9 (2000).

[13] Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, and Ross Anderson. "Chip and Skim: Cloning EMV Cards with the Pre-Play Attack". In: *Security and Privacy (SP)*. IEEE. 2014, pp. 49–64.

[14] Dan Boneh, Xavier Boyen, and Hovav Shacham. "Short Group Signatures". In: *CRYPTO 2004*. Ed. by Matthew Franklin. Vol. 3152. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2004, pp. 41–55.

[15] Dan Boneh and David Mandell Freeman. "Homomorphic Signatures for Polynomial Functions". In: *EUROCRYPT 2011*. Ed. by Kenneth G. Paterson. Vol. 6632. LNCS. Tallinn, Estonia: Springer, Heidelberg, Germany, 2011, pp. 149–168.

[16] Dan Boneh and David Mandell Freeman. "Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures". In: *PKC 2011*. Ed. by Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi. Vol. 6571. LNCS. Taormina, Italy: Springer, Heidelberg, Germany, 2011, pp. 1–16.

[17] Dan Boneh, Ben Lynn, and Hovav Shacham. "Short Signatures from the Weil Pairing". In: *ASIACRYPT 2001*. Ed. by Colin Boyd. Vol. 2248. LNCS. Gold Coast, Australia: Springer, Heidelberg, Germany, 2001, pp. 514–532.

[18] Dan Boneh, Emily Shen, and Brent Waters. "Strongly Unforgeable Signatures Based on Computational Diffie-Hellman". In: *PKC 2006*. Ed. by Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin. Vol. 3958. LNCS. New York, NY, USA: Springer, Heidelberg, Germany, 2006, pp. 229–240.

[19] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. "Practical and Provably Secure Distance-Bounding". In: *ISC 2013*. Ed. by Yvo Desmedt. Vol. 7807. LNCS. Dallas, TX, USA: Springer, Heidelberg, Germany, 2015, pp. 248–258.

[20] Stefan Brands and David Chaum. "Distance-Bounding Protocols (Extended Abstract)". In: *EUROCRYPT'93*. Ed. by Tor Helleseth. Vol. 765. LNCS. Lofthus, Norway: Springer, Heidelberg, Germany, 1994, pp. 344–359.

[21] Emmanuel Bresson, Jacques Stern, and Michael Szydlo. "Threshold Ring Signatures and Applications to Ad-hoc Groups". In: *CRYPTO 2002*. Ed. by Moti Yung. Vol. 2442. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2002, pp. 465–480.

[22] Julien Bringer, Herve Chabanne, Melanie Favre, Alain Patey, Thomas Schneider, and Michael Zohner. "GSHADE: Faster Privacy-Preserving Distance Computation and Biometric Identification". In: *Proceedings of the 2nd ACM workshop on Information hiding and multimedia security*. ACM. 2014, pp. 187–198.

[23] Julien Bringer, Hervé Chabanne, and Alain Patey. "Shade: Secure Hamming Distance Computation from Oblivious Transfer". In: *FC 13*. Springer. 2013, pp. 164–176.

[24] Christina Brzuska, Heike Busch, Özgür Dagdelen, Marc Fischlin, Martin Franz, Stefan Katzenbeisser, Mark Manulis, Cristina Onete, Andreas Peter, Bertram Poettering, and Dominique Schröder. "Redactable Signatures for Tree-Structured Data: Definitions and Constructions". In: *ACNS 10*. Ed. by Jianying Zhou and Moti Yung. Vol. 6123. LNCS. Beijing, China: Springer, Heidelberg, Germany, 2010, pp. 87–104.

[25] Jan Camenisch and Anna Lysyanskaya. "A Signature Scheme with Efficient Protocols". In: *SCN 02*. Ed. by Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano. Vol. 2576. LNCS. Amalfi, Italy: Springer, Heidelberg, Germany, 2003, pp. 268–289.

[26] Srdjan Capkun, Karim M. El Defrawy, and Gene Tsudik. "Group Distance Bounding Protocols - (Short Paper)". In: *TRUST 11*. Pittsburgh, PA, USA, 2011, pp. 302–312.

[27] Jae Choon Cha and Jung Hee Cheon. "An Identity-Based Signature from Gap Diffie-Hellman Groups". In: *PKC 2003*. Ed. by Yvo Desmedt. Vol. 2567. LNCS. Miami, FL, USA: Springer, Heidelberg, Germany, 2003, pp. 18–30.

[28] David Chaum. "Blind Signatures for Untraceable Payments". In: *CRYPTO 82*. Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Santa Barbara, CA, USA: Plenum Press, New York, USA, 1982, pp. 199–203.

[29] David Chaum and Eugène van Heyst. "Group Signatures". In: *EUROCRYPT 91*. Ed. by Donald W. Davies. Vol. 547. LNCS. Brighton, UK: Springer, Heidelberg, Germany, 1991, pp. 257–265.

[30] Tom Chothia, Flavio D. Garcia, Joeri de Ruiter, Jordi van den Breekel, and Matthew Thompson. "Relay Cost Bounding for Contactless EMV Payments". In: *FC 2015*. Ed. by Rainer Böhme and Tatsuaki Okamoto. Vol. 8975. LNCS. San Juan, Puerto Rico: Springer, Heidelberg, Germany, 2015, pp. 189–206.

[31] Sherman S. M. Chow, Man Ho Au, and Willy Susilo. "Server-Aided Signatures Verification Secure against Collusion Attack (Short Paper)". In: *ASIACCS 11*. Ed. by Bruce S. N. Cheung, Lucas Chi Kwong Hui, Ravi S. Sandhu, and Duncan S. Wong. Hong Kong, China: ACM Press, 2011, pp. 401–405.

[32] Vasek Chvatal. "A Greedy Heuristic for the Set-Covering Problem". In: *Mathematics of operations research* 4.3 (1979), pp. 233–235.

[33] John Horton Conway. "On Numbers and Games". In: *London Mathematical Society Monographs*. 6. Academic Press London-New-San Francisco, 1976.

[34] Ashok Kumar Das and Adrijit Goswami. "A Secure and Efficient Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care". In: *Journal of Medical Systems* 37.3 (2013), p. 9948.

[35] John Daugman. "How Iris Recognition Works". In: *The essential guide to image processing*. Elsevier, 2009, pp. 715–739.

[36] Yvo Desmedt. "Computer security by redefining what a computer is". In: *Proceedings on the 1992-1993 workshop on New security paradigms*. ACM. 1993, pp. 160–166.

[37] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[38] Saar Drimer and Steven J. Murdoch. "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks". In: *USENIX 97*. Boston, MA, USA, 2007.

[39] Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, and Elena Pagnin. "Multi-key Homomorphic Authenticators". In: *ASIACRYPT 2016, Part II*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10032. LNCS. Hanoi, Vietnam: Springer, Heidelberg, Germany, 2016, pp. 499–530.

[40] Dario Fiore and Elena Pagnin. "Matrioska: A Compiler for Multi-Key Homomorphic Signatures". In: *SCN 18*. LNCS. Amalfi, Italy: Springer, Heidelberg, Germany, 2018.

[41] Aurélien Francillon, Boris Danev, and Srdjan Capkun. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars". In: *NDSS 2011*. San Diego, CA, USA: The Internet Society, 2011.

[42] Sébastien Gambs, Cristina Onete, and Jean-Marc Robert. "Prover Anonymous and deniable Distance-Bounding Authentication". In: *ASIACCS 14*. Ed. by Shiho Moriai, Trent Jaeger, and Kouichi Sakurai. Kyoto, Japan: ACM Press, 2014, pp. 501–506.

[43] Rosario Gennaro and Daniel Wichs. "Fully Homomorphic Message Authenticators". In: *ASIACRYPT 2013, Part II*. Ed. by Kazue Sako and Palash Sarkar. Vol. 8270. LNCS. Bengalore, India: Springer, Heidelberg, Germany, 2013, pp. 301–320.

[44] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *41st ACM STOC*. Ed. by Michael Mitzenmacher. Bethesda, MD, USA: ACM Press, 2009, pp. 169–178.

[45] Marc Girault and David Lefranc. "Server-Aided Verification: Theory and Practice". In: *ASIACRYPT 2005*. Ed. by Bimal K. Roy. Vol. 3788. LNCS. Chennai, India: Springer, Heidelberg, Germany, 2005, pp. 605–623.

[46] Trotta Gnam. "Zero-Knowledge Made Easy so It Won't Make You Dizzy - (A Tale of Transaction Put in Verse About an Illicit Kind of Commerce)". In: *SCN 16*. Ed. by Vassilis Zikas and Roberto De Prisco. Vol. 9841. LNCS. Amalfi, Italy: Springer, Heidelberg, Germany, 2016, pp. 191–197.

[47] Shafi Goldwasser and Mihir Bellare. "Lecture Notes on Cryptography". In: *http://www. cs. ucsd. edu/users/mihir/papers/gb.html* (2015).

[48] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. "A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks". In: *SIAM Journal on Computing* 17.2 (Apr. 1988), pp. 281–308.

[49] Sergey Gorbunov, Vinod Vaikuntanathan, and Daniel Wichs. "Leveled Fully Homomorphic Signatures from Standard Lattices". In: *47th ACM STOC*. Ed. by Rocco A. Servedio and Ronitt Rubinfeld. Portland, OR, USA: ACM Press, 2015, pp. 469–477.

[50] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data". In: *ACM CCS 06*. Ed. by Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati. Alexandria, Virginia, USA: ACM Press, 2006, pp. 89–98.

[51] Gerhard P. Hancke and Markus G. Kuhn. "An RFID Distance Bounding Protocol". In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, (SecureComm)*. 2005, pp. 67–73.

[52] Jens Hermans, Roel Peeters, and Cristina Onete. "Efficient, Secure, Private Distance Bounding Without Key Updates". In: *Security and privacy in wireless and mobile networks (WiSec)*. ACM. 2013, pp. 207–218.

[53] Javier Herranz, Fabien Laguillaumie, Benoît Libert, and Carla Ràfols. "Short Attribute-Based Signatures for Threshold Predicates". In: *CT-RSA 2012*. Ed. by Orr Dunkelman. Vol. 7178. LNCS. San Francisco, CA, USA: Springer, Heidelberg, Germany, 2012, pp. 51–67.

[54] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. "Biometric Template Security". In: Hindawi Publishing Corp., 2008, p. 113.

[55] Markus Jakobsson and Ari Juels. "Proofs of Work and Bread Pudding Protocols". In: *Secure Information Networks: Communications and Multimedia Security (CMS '99)*. Springer, 1999, pp. 258–272.

[56] Markus Jakobsson and Susanne Wetzel. "Secure Server-Aided Signature Generation". In: *PKC 2001*. Ed. by Kwangjo Kim. Vol. 1992. LNCS. Cheju Island, South Korea: Springer, Heidelberg, Germany, 2001, pp. 383–401.

[57] Ayman Jarrous and Benny Pinkas. "Secure Hamming Distance Based Computation and Its Applications". In: *ACNS 09*. Ed. by Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud. Vol. 5536. LNCS. Paris-Rocquencourt, France: Springer, Heidelberg, Germany, 2009, pp. 107–124.

[58] Ari Juels and Stephen A. Weis. "Authenticating Pervasive Devices with Human Protocols". In: *CRYPTO 2005*. Ed. by Victor Shoup. Vol. 3621. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2005, pp. 293–308.

[59] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. "The Swiss-Knife RFID Distance Bounding Protocol". In: *ICISC 08*. Ed. by Pil Joong Lee and Jung Hee Cheon. Vol. 5461. LNCS. Seoul, Korea: Springer, Heidelberg, Germany, 2009, pp. 98–115.

[60] Russell W. F. Lai, Raymond K. H. Tai, Harry W. H. Wong, and Sherman S. M. Chow. "A Zoo of Homomorphic Signatures: Multi-Key and Key-Homomorphism". Cryptology ePrint Archive, Report 2016/834, `http://eprint.iacr.org/2016/834`. 2016.

[61] Byoungcheon Lee, Heesun Kim, and Kwangjo Kim. "Strong Proxy Signature and its Applications". In: *Proceedings of SCIS*. Vol. 2001. 2001, pp. 603–608.

[62] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. "Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors". In: *EUROCRYPT 2016, Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. LNCS. Vienna, Austria: Springer, Heidelberg, Germany, 2016, pp. 1–31.

[63] Benoît Libert, Thomas Peters, and Moti Yung. "Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions". In: *CRYPTO 2015, Part II*. Ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9216. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 2015, pp. 296–316.

[64] Chae Hoon Lim and Pil Joong Lee. "Server (Prover/Signer)-Aided Verification of Identity Proofs and Signatures". In: *EUROCRYPT'95*. Ed. by Louis C. Guillou and Jean-Jacques Quisquater. Vol. 921. LNCS. Saint-Malo, France: Springer, Heidelberg, Germany, 1995, pp. 64–78.

[65] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. "Attribute-Based Signatures". In: *CT-RSA 2011*. Ed. by Aggelos Kiayias. Vol. 6558. LNCS. San Francisco, CA, USA: Springer, Heidelberg, Germany, 2011, pp. 376–392.

[66] Konstantinos Markantonakis, Lishoy Francis, Gerhard Hancke, and Keith Mayes. "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones". In: *Radio Frequency Identification System Security: RFIDsec* 12 (2012), p. 21.

[67] Elena Pagnin, Carlo Brunetta, and Pablo Picazo-Sanchez. "HIKE: Walking the Privacy Trail". In: *Cryptology and Network Security (CANS)*. LNCS. Naples, Italy, 2018.

[68] Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin, and Aikaterini Mitrokotsa. "On the Leakage of Information in Biometric Authentication". In: *INDOCRYPT '14*. Ed. by Willi Meier and Debdeep Mukhopadhyay. Vol. 8885. LNCS. New Delhi, India: Springer, Heidelberg, Germany, 2014, pp. 265–280.

[69] Elena Pagnin, Gerhard P. Hancke, and Aikaterini Mitrokotsa. "Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-hop Neighbours". In: *IEEE Communications Letters* 19.7 (2015), pp. 1173–1176.

[70] Elena Pagnin, Jing Liu, and Aikaterini Mitrokotsa. "Revisiting Yasuda et al.'s Biometric Authentication Protocol: Are you Private Enough?" In: *Cryptology and Network Security (CANS)*. LNCS. Hong Kong, 2017.

[71] Elena Pagnin and Aikaterini Mitrokotsa. "Privacy-preserving biometric authentication: challenges and directions". In: *Security and Communication Networks* (2017). Article ID 7129505.

[72] Elena Pagnin, Aikaterini Mitrokotsa, and Keisuke Tanaka. "Anonymous Single-Round Server-Aided Verification". In: *5th International Conference on Cryptology and Information Security in Latin America* (2017).

[73] Elena Pagnin, Anjia Yang, Gerhard P. Hancke, and Aikaterini Mitrokotsa. "HB+DB, Mitigating Man-in-the-Middle Attacks against HB+ with Distance Bounding". In: *Security & Privacy in Wireless and Mobile Networks (WiSec)*. ACM. 2015, 3:1–3:6.

[74] Elena Pagnin, Anjia Yang, Qiao Hu, Gerhard Hancke, and Aikaterini Mitrokotsa. "HB+ DB: Distance Bounding Meets Human Based Authentication". In: *Future Generation Computer Systems* 80 (2018), pp. 627–639.

[75] LS Penrose. "Dermatoglyphic topology". In: *Nature* 205.4971 (1965), pp. 544–546.

[76] Charles Rackoff and Daniel R. Simon. "Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack". In: *CRYPTO'91*. Ed. by Joan Feigenbaum. Vol. 576. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, 1992, pp. 433–444.

[77] Jason Reid, Juan Manuel González Nieto, Tee Tang, and Bouchra Senadji. "Detecting Relay Attacks with Timing-Based Protocols". In: *ASIACCS 07*. Ed. by Feng Bao and Steven Miller. Singapore: ACM Press, 2007, pp. 204–213.

[78] M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla. "Cancelable biometric filters for face recognition". In: *International Conference on Pattern Recognition, ICPR*. Vol. 3. 3. 2004, pp. 922–925.

[79] Siamak Fayyaz Shahandashti and Reihaneh Safavi-Naini. "Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems". In: *AFRICACRYPT 09*. Ed. by Bart Preneel. Vol. 5580. LNCS. Gammarth, Tunisia: Springer, Heidelberg, Germany, 2009, pp. 198–216.

[80] Koen Simoens, Julien Bringer, Hervé Chabanne, and Stefaan Seys. "A framework for analyzing template security and privacy in biometric authentication systems". In: *IEEE Transactions on Information Forensics and Security* 7.2 (2012), pp. 833–841.

[81] William Stallings. *Cryptography and network security: principles and practice*. Pearson Education, 2003.

[82] Alex Stoianov. "Cryptographically secure biometrics". In: *Biometric Technology for Human Identification VII*. Vol. 7667. International Society for Optics and Photonics. 2010, p. 76670.

[83] Zhiwei Wang. "A new construction of the server-aided verification signature scheme". In: *Mathematical and Computer Modelling* 55.1 (2012), pp. 97–101.

[84] Zhiwei Wang, Licheng Wang, Yixian Yang, and Zhengming Hu. "Comment on Wu et al.'s Server-aided Verification Signature Schemes." In: *International Journal of Network Security* 10.2 (2010), pp. 158–160.

[85] Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang. "Provably secure server-aided verification signatures". In: *Computers & Mathematics with Applications* 61.7 (2011), pp. 1705 –1723.

[86] A. Yang, E. Pagnin, A. Mitrokotsa, G. P. Hancke, and D. S. Wong. "Two-hop Distance-Bounding Protocols: Keep your Friends Close". In: *IEEE Transactions on Mobile Computing* 17.7 (2018), pp. 1723–1736.

[87] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokomaya, and T. Kashiba. "Practical packing method in somewhat homomorphic encryption". In: *DPM/SETOP*. Vol. 8147. LNCS. Springer Berlin Heidelberg, 2013, pp. 34–50.

[88] Naser Zaeri. "Minutiae-Based fingerprint extraction and recognition". In: *Biometrics*. InTech, 2011.