Thesis for the Degree of Licentiate of Engineering

Authentication under Constraints

Elena Pagnin

Networks and Systems Division
Department of Computer Science and Engineering
Chalmers University of Technology
Göteborg, Sweden 2016

Authentication under Constraints
Elena Pagnin

Technical report 155L
ISSN 1652-876X
Department of Computer Science and Engineering

Networks and Systems Division
Chalmers University of Technology
412 96 Göteborg, Sweden
Phone: +46 (0)31-772 10 53

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

Printed by Chalmers Reproservice
Göteborg, Sweden 2016

Authentication under Constraints

Elena Pagnin
Department of Computer Science and Engineering, Networks and Systems Division
Chalmers University of Technology

Thesis for the degree of Licentiate of Engineering, an intermediate degree between the M.Sc. and the Ph.D.

Abstract

Authentication has become a critical step to gain access to services such as on-line banking, e-commerce, transport systems and cars (contact-less keys). In several cases, however, the authentication process has to be performed under challenging conditions. This thesis is essentially a compendium of five papers which are the result of a two-year study on authentication in constrained settings. The two major constraints considered in this work are: (1) the noise and (2) the computational power. For what concerns authentication under noisy conditions, **Paper A** and **Paper B** address the case in which the noise is in the authentication credentials. More precisely, the aforementioned papers present attacks against biometric authentication systems, that exploit the inherent variant nature of biometric traits to gain information that should not be leaked by the system. **Paper C** and **Paper D** study proximity-based authentication, *i.e.*, distance-bounding protocols. In this case, both of the constraints are present: the possible presence of noise in the channel (which affects communication and thus the authentication process), as well as resource constraints on the computational power and the storage space of the authenticating party (called the prover, *e.g.*, an RFID tag). Finally, **Paper E** investigates how to achieve reliable verification of the authenticity of a digital signature, when the verifying party has limited computational power, and thus offloads part of the computations to an untrusted server. Throughout the presented research work, a special emphasis is given to privacy concerns risen by the constrained conditions.

Keywords: Authentication, Digital Signatures, Privacy, Anonymity, Biometrics, Distance-Bounding, Security.

List of Appended Papers

Paper A *"Attacks on Privacy-Preserving Biometric Authentication"*, Aysajan Abidin, Elena Pagnin, Aikaterini Mitrokotsa. In Proceedings of the 19th Nordic Conference on Secure IT Systems, NordSec 2014, Tromsø, Norway, October 2014.

Paper B *"On the Leakage of Information in Biometric Authentication"*, Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin and Aikaterini Mitrokotsa. In Proceedings of Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, pp. 265–280.

Paper C *"HB+DB: Distance Bounding Meets Human Based Authentication"*, Elena Pagnin, Anjia Yang, Gerhard P. Hancke and Aikaterini Mitrokotsa. Future Generation Computer Systems, Journal. Elsevier. Year 2016.

Paper D *"Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-Hop Neighbours"*, Elena Pagnin, Gerhard P. Hancke and Aikaterini Mitrokotsa. In IEEE Communications Letters, vol. 19, num. 7, pp. 1173–1176, year 2015.

Paper E *"Server-Aided Anonymous Signature Verification"*, Elena Pagnin, Aikaterini Mitrokotsa and Keisuke Tanaka. Paper under submission.

Acknowledgements

Allt blir bra.

Hedvig Jonsson

I begin this sequence of 'thanks' by recalling the people who helped, supported and contributed to my research and work in the last two years. In particular, I am grateful to the researchers I have collaborated with, for their knowledge share and brainstorming sessions, and to my supervisor, for her guidelines and all the opportunities she has offered me. I also owe a capital Thanks to some of the current and former members of Chalmers' Department of Computer Science and Engineering, for the collaborative mood and the research exchanges we had, as well as for the fun times out of our offices. In particular, I am grateful to all my colleagues who also became friends and a source of light in the dark periods. A special thanks goes to my dearest, one and only *roomie* for enduring all my italian-temper mutters ... among other situations! ☺ Last but not least, I would like to say *tack* to all the secretaries of the 6^{th} floor, you have been amazing 'fairies' always able to 'magically' solve any kind of problems.

I reserved the final thanks for the people without whom, I most probably would not have come to Chalmers: Frédérique Oggier, Marc Stöttinger, Mariuccia Paoletti, Arianna Pagnin, Annamaria Borgato and Lorenzo Pagnin. I hope you can be proud and feel part of my achievements.

Sorry if I forgot someone, I'm not a fan of these things: I prefer to keep people close to my heart, to show my support and availability, rather than to write a 'thank you – *name* –' under the 'acknowledgements' session of a thesis.

Contents

Part I

Thesis Summary

1 Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it claims to be. In the physical world, with face-to-face communication, authentication is achieved by showing IDs, passports or different kinds of certificates. In several circumstances, however, authentication needs to happen in a digital fashion and under some constraints such as noise, limited storage and computational power. Example of applications in which digital authentication is crucial are: on-line baking, e-health systems, credit-card payments, cloud-storage services, access to military facilities, as well as car-unlocking and email accounts. A common way to achieve authentication is to require an *identity*, *e.g.*, user-name, and a *credential* (*e.g.*, password) for the claimed identity. In more detail, the authentication process succeeds if one provides *correct* answers to the following questions: *who are you?* and *how can you prove it?*

This thesis studies authentication systems in two challenging contexts: (1) when authentication is affected by noise (either in the environment or in the credentials) and (2) when the authentication process happens under storage and computational constraints. The authentication systems considered in this work are based on: biometrics, distance-bounding and digital signatures.

1.1 Authentication in Constrained Settings

The technological development of the last decades has widen the horizon of applications that require accurate and reliable authentication. Nowadays, authentication is a fundamental step in services such as on-line banking, e-commerce websites, e-Health, as well as transport systems and border controls. In many cases, it is desirable that the employed authentication system is, to some extent, user-friendly, practical and always accessible. These three requirements often imply that the authentication process needs to happen under some challenging conditions such as (1) *noise* in the environment (*e.g.*, communication channel) or in the authentication credentials (*e.g.*, biometric traits) or (2) through *computational-constrained devices* (*e.g.*, smart-cards and Radio Frequency IDentification (RFID) tags).

This work investigates three different authentication systems that are employed

in noisy conditions, or under resource constrains: *biometric authentication*, *distance-bounding authentication* and *server-aided signature verification*.

Biometric Authentication. As the name suggests, a biometric authentication system authenticates users, *e.g.*, employees in a company, according to some data derived from the users' body, *e.g.*, an iris or a fingerprint scan. Intuitively, these systems treat the biometric trait as a unique and complicated password that authenticates the user's identity. The inherent variant nature of biometric traits, however, makes the data collecting process affected by a high degree of variability. For example, if the same user attempts to authenticate twice using her fingerprint, the two scans may result to two different captured data due to, *e.g.*, difference in finger pressure or orientation during the scan, and dirt on the surface. Thus, biometric authentication systems have to rely on comparison mechanisms that keep into account the innate *noise* of the biometric credentials.

Distance-Bounding Authentication. From a high-level perspective, distance-bounding authentication protocols combine light-weight cryptographic functions with physical measurements obtained by *resource-constrained devices*. A user is authenticated if her device (prover) replies correctly to a set of challenges within a pre-determined time-frame. The correctness of the responses demonstrates that the prover (*e.g.*, a smartcard for contactless payments) knows the correct secret key, while the time limit gives an upper-bound on the maximal distance between the prover (smartcard) and the verifier (*e.g.*, payment point, contactless card reader), assuming that the messages travel at the speed of light. In this case, what authenticates the user are 1) the physical distance of her device (prover) to the verifier and 2) the possess of the secret key.

Server-Aided Verification of Signatures. Digital signatures are the cryptographic primitive that provides data authentication, *i.e.*, that verifies the source of messages. Loosely speaking, the digital signature of a message has the same properties as the physical signature on a paper document. To guarantee security, however, most signature schemes rely on strong security assumptions which require the employment of expensive computations in order to verify the authenticity of a signature. Server-aided verification has been introduced to enable *resource-constrained devices* to perform verification of such signatures. The main idea behind server-aided signature verification is to outsource part of the computation load of the verifier (*e.g.*, a smartphone or a tablet) to a third party (*e.g.*, a computationally powerful server). Involving one more entity to perform signature verification, however, makes it challenging to achieve basic properties such as accuracy, reliability and privacy (signer anonymity).

1.2 Thesis Objective & Organisation

This thesis is organised in two main parts: Part I is more introductory and provides high-level descriptions to help the reader to understand the contributions of this work. Part II is a collection of papers in which the author of this thesis has contributed. The papers in Part II cover three separate and complementary goals:

1. Finding attacks against existing authentication systems.
2. Designing new authentication protocols.
3. Extending existing security notions and authentication systems to new settings.

The first part of this thesis gives an overview of biometric authentication systems, distance-bounding authentication protocols and signature schemes with server aided-verification. Part I concludes with a summary of the contributions of the author of this thesis in the papers reported in Part II. In more detail, **Paper A** and **Paper B** describe attacks against biometric authentication systems and possible ways to prevent the attacks. **Paper C** combines an existing light-weight protocol with distance-bounding authentication. The resulting scheme is a new distance-bounding protocol for user authentication, which is no longer vulnerable to the known attacks against the employed light-weight protocol. **Paper D** is also in the area of distance-bounding. The paper introduces the notion of two-hop distance-bounding, and studies how distance-bounding authentication can be efficiently and securely extended to a three party case (the prover, the verifier and a linker). The last paper of this collection is about digital signature schemes in which the verifier is a resource-constrained device, *e.g.*, a smartcard or a smartphone, that carries out the verification of signatures with the help of an untrusted server. This setting is called server-aided signature verification. **Paper E** introduces the notions of anonymity and of soundness after collusion (between the signer and the server) in signature schemes with server-aided signature verification. Additionally, the paper presents a new efficient idea for verifying the delegation of the computation of the optimal Ate pairing (which is a function often employed in signature schemes).

Enjoy the reading! ☺

2 Background & Related Work

The aim of this chapter is to introduce the reader to the authentication systems used in the papers collected in Part II. More precisely, this chapter presents the essential background knowledge for authentication systems based on: biometrics, distance-bounding and digital signatures with server-aided verification.

2.1 Biometric Authentication

Biometric authentication is a quick, accurate and user-friendly way to perform efficient and reliable user recognition. It constitutes an indispensable tool to grant access to, *e.g.*, restricted areas, confidential documents or high-level security systems. The base for biometric authentication is the extraction of biometric traits from the human body or behaviour. Some biometric traits used nowadays for user authentication are: voice, signature, DNA, fingerprint [40], iris [12], face geometry [30], gait [34], palm print [25], ear shape [22]. In all cases, the biometric trait is a distinctive characteristic that is measurable and identifies (almost) uniquely each individual. There are two main reasons that made biometric authentication systems become popular. First, biometric credentials have an undeniable strong link to the user, *e.g.*, one can easily 'not recognise' or 'repudiate' a signature, but not an iris scan or a DNA test. Secondly, biometric credentials are considered hard to imitate, therefore a good prevention against impersonation attacks. Although biometric authentication systems are attractive and reliable, it is of utmost importance to assure that they preserve the users' privacy. The issues that rise when a biometric credential gets compromised, *i.e.*, captured, cloned, or forged, are particularly severe due to the inherit connection between the biometric trait and some physical characteristics of the biometrics' owner. For instance, a compromised biometric credential may lead to identity theft, individual profiling and tracking, and even to disclosure of genetic information [28], medical diseases [5] and health records [23].

Biometric authentication is based on a matching process: a user is authenticated if the biometric trait she provides is *close enough* to the biometric template stored in the system when the user registered. To give an example, consider an access gate equipped with a sensor for iris scan. In this case, to perform biometric authentication the sensor can scan the iris of the user, and transform the information

into digital data (*e.g.*, a binary vector $b' \in \{0,1\}^n$). The user is authenticated if the iris scan (called *fresh* biometrics) *matches* the stored template (*e.g.*, the binary vector $b \in \{0,1\}^n$). For biometric credentials, to match means that the vectors b' and b are *similar*. Note that it is not possible to require that $b' = b$ since biometric traits are, by nature, subjected to small variations. For instance, in the case of an iris scan, the two major causes of a mismatch between b' and b are the light conditions and the relative position of the the user and the sensor. These two factors, indeed, influence the diameter and the shape of the pupil, and the detected colour of the iris.

Figure 2.1 depicts the authentication step of a biometric authentication system. The parties involved in the authentication process are the user, $\mathcal{C}$, the sensor, $\mathcal{S}$, the computational server, $\mathcal{CS}$, the database, $\mathcal{DB}$, and the authentication server, $\mathcal{AS}$. This distributed architecture is employed in [38, 39], while previous works, *e.g.*, [8], usually consider the simpler case in which the authentication server and the computational server merge in a single party. The main motivation for the splitting of the tasks among different entities is privacy: in a distributed architecture the sensitive information is indeed distributed in multiple entities. In this way, the corruption of one entity does not lead to the full disclosure of the biometric credentials.

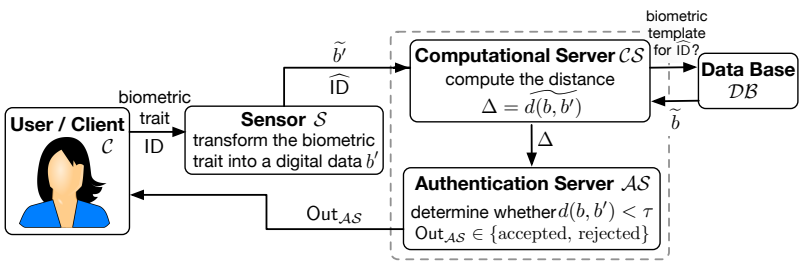

Figure 2.1: Authentication phase in a distributed biometric authentication system.

In detail, biometric authentication systems work as follows. The user, $\mathcal{C}$, first registers to the system, *i.e.*, provides her biometric trait b (called reference template) and her identity ID. These pieces of information are stored in the database $\mathcal{DB}$, either in plain-text (*i.e.*, $\widetilde{b} = b$ and $\widehat{\mathsf{ID}} = \mathsf{ID}$) or in an encrypted form (*i.e.*, $\widetilde{b} \neq b$ and $\widehat{\mathsf{ID}} \neq \mathsf{ID}$). In the latter case, the system is called *privacy-preserving*. Privacy-preserving biometric authentication systems aim at preventing eavesdropping and disclosure of the biometric templates. The biometric templates are protected using cryptographic primitives, such as partially-homomorphic encryption [8, 16, 38], (extended) private information retrieval [9], or zero-knowledge proof of knowledge [4]. After enrolling in the system, the user can authenticate herself (*e.g.*, to get access to a military station, or to some data-bank with confidential information), by providing her identity together with a fresh biometric trait (*e.g.*, finger print). The sensor trans-

forms the biometrics into a digital information b' (*e.g.*, a binary vector) and possibly performs some transformations on it such us encrypting, obtaining $\widetilde{b'}$. Similarly the sensor can process on the provided identity ID and compute $\widehat{\mathsf{ID}}$. The sensor sends $\widetilde{b'}$ and $\widehat{\mathsf{ID}}$ to the computational server, who queries the database (where the biometric data is stored) for the reference template corresponding to the identity $\widehat{\mathsf{ID}}$. If the identity is present in the database, $\mathcal{CS}$ gets the reference template of the claimed identity, *i.e.*, the $\widetilde{b}$ provided by the user in the enrolment phase. The computational server computes the distance between b, and b' (or the encoding thereof[1]). The result of the computation is sent to the authentication server, which authenticates the user only if the fresh and the reference templates are matching, *i.e.,* if and only if $\mathtt{dist}(b, b') < \tau$, where `dist` is an appropriate distance and τ is a threshold value.

The distance function `dist`, and the value of the threshold τ may depend on the system, the biometric trait and even the user. For instance, [8, 27] employ the Hamming distance, [12] performs iris recognition using the normalised Hamming distance, while [2, 16, 17, 32] employ the Euclidean distance. Finding the optimal value for the threshold τ is a research field orthogonal to the scope of this thesis. To give an intuition of the matter, if the value τ is 'too little', the biometric authentication system may reject a legitimate user who provides a fresh template which, due to the fickle nature of biometric traits, happens to be *too far* from the stored reference template (false rejection). On the other hand, if the threshold is 'too large', the system may authenticate an illegitimate person whose biometric credential is *not too far* from a client's reference template (false acceptance). Doddington *et al.* [14] study the false acceptance/false rejection problem in detail and propose an fun classification of user called the *biometric zoo*. In [31], Ross and Jain discuss a different approach: *multi-modal biometrics* fusion schemes. The idea behind this method is to require multiple traits in the authentication phase (*e.g.*, fingerprint, face and voice; index and middle fingers). In this case, the accuracy of the authentication does not depend on the threshold value solely, but rather on the fact that the user can provide several credentials, each one close to some reference template. A theoretical study on the accuracy of biometric authentication can be found in [33]. The objective of this thesis, however, is not to improve the accuracy of biometric authentication. The topics of interest are the privacy and security implications due to the leakage of information in the authentication step.

[1] In a privacy-preserving biometric authentication system, the computational server does not have access to any plain-text information. For instance, consider the case in which the sensor $\mathcal{S}$ encrypts both the fresh biometric template b' (*i.e.*, $\widetilde{b'} = \mathsf{Enc}(b')$) and the identity ID of the user (*i.e.*, $\widehat{\mathsf{ID}} = \mathsf{Enc}(\mathsf{ID})$) using a homomorphic encryption scheme. The computational server can homomorphically compute the encryption of the Hamming distance (HD) between b' and b as $\mathsf{HD}(\widetilde{b}, \widetilde{b'}) = \mathsf{Enc}(\mathsf{HD}(b, b'))$, and send it to the authentication server, who decrypts and authenticates the user if the returned value is smaller than the threshold.

2.1.1 Problem Statement

Biometric credentials are often considered as a unique, complicated and secure password that cannot be forgotten, or as an authentication token that is always available and can never be lost. Nevertheless, the use of biometric credentials in contrast to passwords exposes the owner of the biometric trait to severe privacy and security issues, in case the biometric credential gets compromised (captured or forged).

This thesis investigates how to capture and forge digital biometric credentials, exploiting the information leaked during the matching process. In detail, **Paper A** and **Paper B** show how to adopt a hill-climbing technique to attack any biometric authentication system, privacy-preserving or not, as long as it employs a *leaking distance* (*e.g.*, the Hamming distance and the Euclidean distance) in the matching process. An implication of these results is that assuring security and privacy in biometric authentication using known techniques (such as secure multi-party computation and encryption) is a very challenging task. A direction for future work is to mitigate these attacks using cryptographic primitives such as verifiable delegation of computations, to prevent the leakage of information to a malicious computational server.

2.2 Distance-Bounding Authentication Protocols

The development of wireless technology enlarged the horizon of application scenarios for Radio Frequency IDentification (RFID). Nowadays people are using RFID tags in everyday life thanks to contact-less smart-card payments, proximity identification systems, passive key-less cars and much more. Besides the multiple benefits, RFID communication systems are vulnerable to a serious weakness: relay attacks. An example of a relay attack is the following. A businessman, is seated in a café with his contact-less credit card 'safely' put in his pocket. The attacker is equipped with an antenna that amplifies RFID communications, and has an accomplice in the jewellery shop next by. When buying an item from the jewellerly shop, the attacker relays the communication between the businessman's credit card and the RFID-reader of the shop, essentially paying the good with the businessman's money! Similar attacks have been mounted to amplify the communication range of RFID car-keys and unlock cars, while the keys are not physically close to them [18].

In order to combat relay attacks, Brands and Chaum [7] introduced distance-bounding protocols. Classical distance-bounding protocols [6, 21, 24, 29] involve two parties: the user (called the *prover* $\mathcal{P}$), and the RFID reader (called the *verifier* $\mathcal{V}$). Generally speaking, distance-bounding protocols have two simultaneous aims: (1) to authenticate the prover, and (2) to bound the prover's distance from the verifier. The two goals are achieved by employing real-time challenge-response authentication protocols, in which the round-trip-time of multiple challenge-response pairs is

used to determine an upper bound on the physical distance[2] between $\mathcal{V}$ and $\mathcal{P}$.

Figure 2.2 depicts the model of a generic distance-bounding protocol.

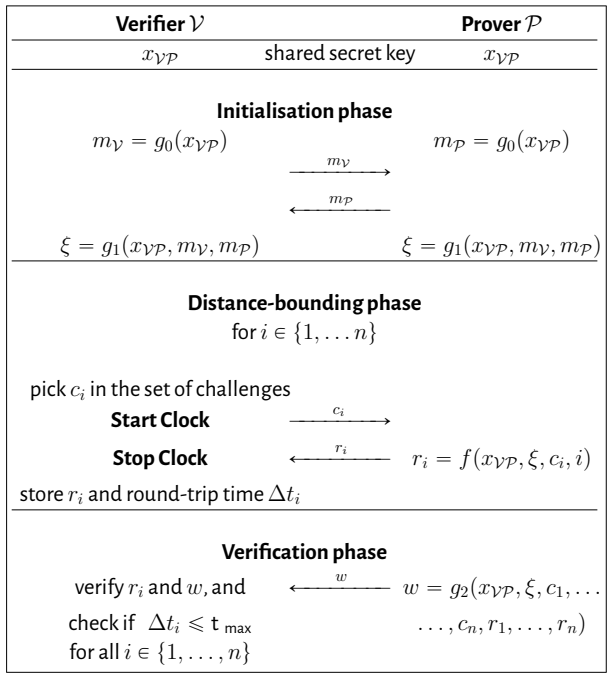

Figure 2.2: General structure of a distance-bounding protocol.

In the initialisation phase, the prover and the verifier use their shared secret key $x_{\mathcal{VP}}$ to produce the session-keys $m_{\mathcal{P}}$ and $m_{\mathcal{V}}$ respectively. Usually the function g_0 is a random selection of an element in $\{0,1\}^N$, for some large positive integer N. The session-keys and the secret key are input to the function g_1, that outputs a string ξ, employed by the prover in the next phase. The distance-bounding phase, is made of n repetitions of a simple protocol: $\mathcal{V}$ sends a challenge c_i, and $\mathcal{P}$ replies to it

[2]The upper bound on the physical distance between the prover and the verifier is derived in the following way. Set a maximum-allowed distance d. Given that the challenges and the responses of a distance-bounding protocol are sent via radio waves, they travel at the speed of light ($c \approx 3.00 \times 10^8 m/s$). As a result, the verifier can state that the prover is within distance d if it receives correct responses in less than $t_{\text{max}} = d/c$ seconds. Note that the accuracy in the measurement of the round-trip time (Δt_i) is of utmost importance: if the distance bound is set to $d = 30$ centimetres – desirable bound for contact-less payments –, then $t_{\text{max}} \approx 1$ nanosecond.

with r_i, computed using c_i and an opportune function f. To give an example, in the Hancke-Kuhn distance-bounding protocol [21], the function g_1 is a Pseudorandom Function that outputs two n-bit strings $a^{(0)}, a^{(1)} \in \{0,1\}^n$, and f is simply $a_i^{(c_i)}$, *i.e.*, it outputs the i-th bit of the c_i-th register (where $c_i \in \{0,1\}$). In the last phase of the distance-bounding protocol, the verifier verifies that (1) the prover answered the challenges correctly, *i.e.*, it is authenticated, as it knows the shared secret $x_{\mathcal{VP}}$, and (2) the prover's responses reached the verifier within the time limit, thus the prover is *close enough*. The constraint on the round-trip time of challenge-response messages (*i.e.*, the proximity test) makes distance-bounding protocols resilient against relay attacks.

2.2.1 Problem Statement

The most challenging part when designing a distance-bounding protocol is to make sure that the new proposal is secure against the three following threats:

1. **Distance Fraud** [7]: a dishonest prover $\mathcal{P}^*$ attempts to prove that it is close to the verifier $\mathcal{V}$ while in reality it is far away.

2. **Mafia Fraud** [13]: this is a *man-in-the-middle* attack, the adversary $\mathcal{A}$ is located between an honest prover $\mathcal{P}$ –which lies outside the communication rage of $\mathcal{V}$– and $\mathcal{V}$. The aim of $\mathcal{A}$ is to make $\mathcal{P}$ appear closer to $\mathcal{V}$, by convincing $\mathcal{V}$ that it communicates with $\mathcal{P}$ directly, while in reality both $\mathcal{P}$ and $\mathcal{V}$ are communicating with $\mathcal{A}$.

3. **Terrorist Fraud** [13]: this attack is an extension of the mafia fraud. A dishonest prover $\mathcal{P}^*$ colludes with the adversary against the verifier. The aim of the colluding pair $(\mathcal{A}, \mathcal{P}^*)$ is to convince $\mathcal{V}$ that the prover is actually close by, when in reality $\mathcal{P}^*$ is far away. Note that, in this threat the prover is dishonest and helps $\mathcal{A}$ to get authenticated in its behalf.

The reader not familiar with the field of distance-bounding may wonder what is the intuition behind the names of the last two attacks in the list above. Essentially, these quirky names are due to the creative mind of Desmedt [13] and have been adopted as a standard way to refer to the two attack scenarios, although there is no direct relation between the distance-bounding attacks and actual mafia frauds or terrorist attacks. Figure 2.3 gives an intuition of the setting of the three frauds.

Since distance-bounding protocols keep into account the round-trip time of the challenge-response pairs, in order to succeed in a mafia fraud, $\mathcal{A}$ cannot simply relay the communication between $\mathcal{P}$ and $\mathcal{V}$. The hardest threat to protect against is terrorist fraud. For this reason, different approaches on how to define terrorist fraud

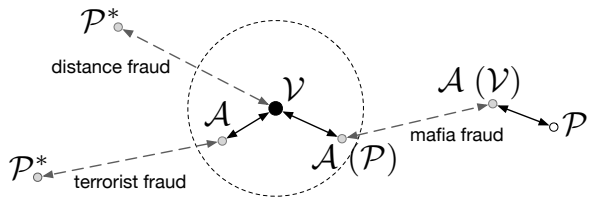

Figure 2.3: The three main threats in distance-bounding authentication. Dishonest communications are depicted in a lighter colour and dashed lines, malicious parties (*e.g.*, $\mathcal{P}^*$, $\mathcal{A}$) are highlighted with a grey dot. In mafia fraud, we consider a powerful attacker that impersonates the prover when communicating to $\mathcal{V}$, while, at the same time, it pretends to be the verifier when communicating to $\mathcal{P}$ (possibly using another device in a different location).

have been proposed [1, 6, 15]. The most intuitive one is to consider an attack successful if $\mathcal{P}^*$ does not reveal its secret key to the attacker (or equivalently, any information that will let, later on, $\mathcal{A}$ succeed in another fraud on its own).

This thesis contains two papers on distance-bounding: **Paper C** and **Paper D**. **Paper C** designs a new distance-bounding protocol, which is proven to be resilient against the three threats mentioned above, while **Paper D** generalises the idea of distance-bounding to the case in which the prover and the verifier does not lie in the communication range of each other, and investigates how the notions of distance fraud, mafia fraud and terrorist fraud modify in this new setting.

2.3 Server-Aided Signature Verification

Communication technologies and portable devices have revolutionized the way we manage our personal lives and communicate with other people. Mobile and resource-constrained devices enjoy an always increasing range of application and capabilities, thanks to the research of new technologies and materials, as well as efficiency improvements of computational algorithms. Lately, researchers have identified a new approach to make computational expensive tasks accessible to user-friendly devices: cloud computing. Users can now *access* the cloud (a computationally powerful server with large storage space), *outsource* computations to the server from their personal devices, and *obtain* results which used to be prohibitive for the device to compute. This is the setting of server-aided signature verification (also depicted in Figure 2.4).

The concept of *server-aided signature verification* was introduced in 1995 in two independent works [3, 26] and refined ten years later in [20]. The intuition behind it was to enable a verifier (*e.g.*, a resource-constrained device) to outsource part of the signature verification process to an untrusted third party (*e.g.*, a computationally

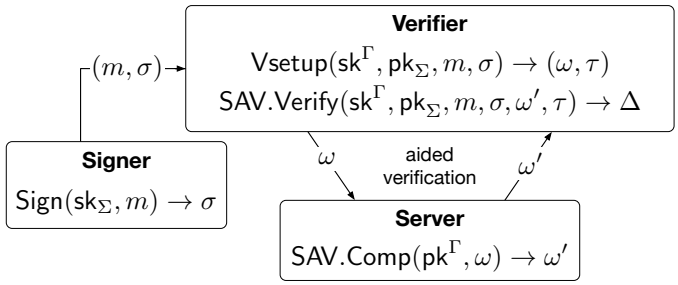

Figure 2.4: Setting for server-aided signature verification. The Greek letter Σ denotes the keys of the digital signature scheme, while Γ denotes the keys of the verifiable delegation scheme. The signer signs a message m using its secret key sk_{Σ} and sends the pair (m, σ) to the verifier. The verifier first runs the verification setup to obtain (ω, τ), and then it sends the public output ω to the server. The server computes the outsourced task and returns ω' to the verifier. Finally, the verifier checks the correctness of ω' and determines a decision $\Delta \in \{\perp, 1, 0\}$, where $\Delta = \perp$ if the verifier has detected a cheating server, $\Delta = 1$ if σ is a *valid* signature for the message m, and $\Delta = 0$ if σ is a *invalid*.

powerful server). The fact of relying on untrusted entities naturally rises concerns about the *privacy* of the outsourced data and the *integrity* of the outsourced computation. In addition, the server-aided-verification protocol should guarantee the same security and correctness as the initial signature scheme, and yet be *lighter*, *i.e.*, less computational demanding, for the verifier. More precisely, a signature scheme should enable a signer (in possess of a secret key) to sign a message, *i.e.*, to produce a signature for the message, such that the verifier, in possess of the signer's public key and interacting with the server, can verify the *authenticity* of the signature for the message. Authenticity essentially means that 1) the message was created by the signer (authentication), 2) the message was not altered in transit (integrity) and that 3) it is not possible for the signer to deny having created the signed message (non-repudiation).

Since server-aided verification protocols involve an additional entity with respect to standard signature schemes, they are inherently vulnerable to more threats. The thorniest attack scenario considered in the literature is a *collusion* between a malicious signer and the server [11, 35–37]. The key of success for a collusion attack is the face that most of the existing schemes do not check the correctness of the computation outsourced to the server, *e.g.*, [35–37]. For this reason, [11] proposed to mitigate the impact of the attack by combining the server aided-verification with a protocol for verifiable delegation of computation [19]. This last setting is the one reported in Figure 2.4 for *reliable* server-aided verification of signatures.

2.3.1 Problem Statement

Since the introduction of server-aided signature verification, the research community put a constant effort at identifying new attack scenarios. The first papers on the topic considered only soundness and existential unfogeability against the server-aided verification scheme. More recent works introduced the concept of a malicious signer colluding with the server in order to tamper with the outcome of the server-aided verification. **Paper E** continues along the line of identifying new threats in server-aided signature verification and formalises two new security notions: *anonymity* and *soundness after collusion*. In the former case, the aim is to protect the privacy of the signer, thus avoiding to leak data about the identity of the signer during server-aided verification. Soundness after collusion states that after a successful collusion attack, the server should not be able to forge the signature scheme on its own (using the information leaked by the malicious signer during the collusion attack).

The large majority of the papers on server-aided verification of signatures considers pairing-based signature schemes. In this case, in order to be resilient against collusion, a server-aided signature verification needs to adopt a protocol for verifiable computation for bilinear pairings. Generally speaking, in such a verifiable computation scheme the verifier (or delegator), in order to check the correctness of the outsourced operations, needs to perform some operations on the value returned by the server. In particular, existing schemes [10], require the verifier to perform both membership testing and exponentiations in the target group. These two are expensive operations, whose computational cost is often comparable or even higher than the one of the bilinear pairing itself. In this context, **Paper E** proposes a new scheme that can be employed for server aided-verification of pairing based signature schemes.

3 Summary of the Thesis Contributions

This section provides an overview of the main results of the papers presented in Part II and explains the contributions of the author in each work.

3.1 Paper A and Paper B

The first two papers of this collection deal with biometric authentication.

In **Paper A**, we review two privacy-preserving biometric authentication protocols proposed by Yasuda *et al.* [38, 39]. The protocols are based on two packed homomorphic encryption schemes, that are claimed to protect the privacy of the users' biometric credentials. We present two attacks in the form of algorithms. The first attack (Algorithm 1) enables the malicious user (or the computational server) to recover a reference biometric template b using a matching template, *i.e.*, a vector $b' \in \{0,1\}^n$ such that $\texttt{dist}(b, b') < \tau$. More interestingly, our second attack (Algorithm 2) shows how the computational server $\mathcal{CS}$ can recover a reference template of an arbitrary user, without a matching template to start with. The main enabler of this second attack is the lack of verification of the correctness of the computations performed by the computational server. Namely, $\mathcal{CS}$ can tamper with the result provided to the authentication server and deduce information about the target biometric template without being detected.

Paper B builds on the results of the previous paper and investigates in detail the leakage of information that happens in the matching process. I am the main author of this work, and the creator of the attack algorithms and the proofs of the paper. The idea of the attack comes from a simple observation: the matching process makes use of a suitable distance which measures the similarities between the two biometric templates. If the distance is sensible to variations in a single component of the biometrics (seen as a vector in $\mathbb{Z}_q^n$), it is possible to recover information by submitting a fresh template to the biometric authentication system and observe

the output of the authentication server. My contributions on the paper are:

- Formal definition of *leaking distances* (which include the Hamming and the Euclidean distance).
- Design of a hill-climbing attack that enables an attacker, external to the authentication system, to recover reference biometric template from a matching one.
- Statement and proof of the theorems.
- Identification of different brute-force attacks to find a matching template without any previous information (in particular, I proposed the tree algorithm).

We note that recovering stored biometric templates has a severe impact since the same reference template might be used in multiple biometric authentication systems or leak a match in criminal biometric template databases. Moreover, our results and proofs hold true also for privacy-preserving biometric authentication protocols and are not affected by the use of a protection mechanism such as homomorphic encryption.

3.2 Paper C and Paper D

This thesis contains two papers in the area of distance-bounding authentication protocols.

Paper C was born from the idea of fixing a well-known flaw in the HB^+ protocol with distance-bounding techniques. In this paper, we demonstrate that it is possible to mitigate a serious man-in-the-middle attack against the HB^+ protocol by simply measuring the response-time of the prover, instead of modifying the cryptographic response function (as done in previous works). My contributions in the paper are mostly on:

- The formalisation of the proposed $\mathsf{HB}^+\mathsf{DB}$ protocol.
- The analysis of the accuracy (correctness) of $\mathsf{HB}^+\mathsf{DB}$ despite the errors and noise.
- The security analysis of the proposed $\mathsf{HB}^+\mathsf{DB}$ protocol.

Until **Paper D**, distance-bounding authentication protocols were considered to be executed between the prover and the verifier, lying in each other's communication range. In this paper, we introduce the concept of *two-hop* distance-bounding

authentication. This new setting allows proximity-based authentication in case the prover and the verifier are not *close* to each other. The communication relies on an intermediate untrusted party (the linker), as shown in Figure 3.1.

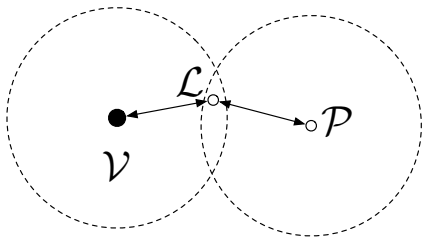

Figure 3.1: Setting for two-hop distance-bounding authentication. Entities involved: verifier $\mathcal{V}$, linker $\mathcal{L}$, prover $\mathcal{P}$.

In this paper I took care of:

- Formalising the general structure of two-hop distance-bounding protocols,
- Generalising the known threats against single-hop distance-bounding protocols, to the two-hop case,
- Discussing the security of the proposed protocol, under the presence of a malicious linker.

3.3 Paper E

The last paper of this collection is a work – currently under submission – on server-aided signature verification. The topic was suggested during last summer's research visit at Tokyo Institute of Technology. I am the main author of the paper, my supervisor and Professor Tanaka's contributions are mostly in suggesting guidelines and directions of research. **Paper E** investigates new attack scenarios in server-aided signature verification (SAV in short). More precisely, we introduce the concept of SAV-anonymity, and I suggested and defined the notion of *soundness after collusion*. In addition, we introduce a rigorous formalism to describe SAV-signature schemes, and a black-box construction to combine any signature scheme with a verifiable computation scheme (for the main computation involved in the signature verification).

All the results and the proofs presented in the paper are done by me. Also, I proposed new signature schemes extended to the server-aided verification setting and investigated their efficiency. Last but not least, I wanted to have a contribution that would be beneficial in the SAV context, but which is also of independent interest:

a verifiable delegation scheme for pairing computations which has a different approach than all existing schemes. Inspired by this idea, I tried to think 'outside the box' and defined a new efficient and private protocol for *securely outsourcing the computation of the Optimal Ate pairing*. The originality of my approach is to look into the algorithm to compute the bilinear pairing, and outsource the heavy step, which is the final exponentiation (in the target group). The computational cost of the suggested protocol for verifiable computation of the Optimal Ate pairing is almost *half* of the cost of computing the whole pairing.

Bibliography

[1] Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardas, Cédric Lauradoux, and Benjamin Martin. "A framework for analyzing RFID distance bounding protocols". In: *Journal of Computer Security* 19.2 (2011), pp. 289–317.

[2] Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, Dario Fiore, Riccardo Lazzeretti, Vincenzo Piuri, Fabio Scotti, and Alessandro Piva. "Privacy-preserving fingercode authentication". In: *Multimedia and Security Workshop, MM&Sec 2010, Roma, Italy, September 9-10, 2010*. 2010, pp. 231–240.

[3] Philippe Béguin and Jean-Jacques Quisquater. "Fast Server-Aided RSA Signatures Secure Against Active Attacks". In: *Advances in Cryptology - CRYPTO '95*. 1995, pp. 57–69.

[4] Abhilasha Bhargav-Spantzel, Anna C Squicciarini, Shimon Modi, Matthew Young, Elisa Bertino, and Stephen J Elliott. "Privacy preserving multi-factor authentication with biometrics". In: *Journal of Computer Security* 15.5 (2007), pp. 529–560.

[5] James Bolling. "A window to your health". In: *Jacksonville Medicine, Special Issue: Retinal Diseases* 51.9 (2000).

[6] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. "Practical and provably secure distance-bounding". In: *Journal of Computer Security* 23.2 (2015), pp. 229–257.

[7] Stefan Brands and David Chaum. "Distance-bounding protocols". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1993, pp. 344–359.

[8] Julien Bringer, Hervé Chabanne, Malika Izabachène, David Pointcheval, Qiang Tang, and Sébastien Zimmer. "An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication". In: *Australasian Conference on Information Security and Privacy*. LNCS. Springer-Verlag, 2007, pp. 96–106.

[9] Julien Bringer, Hervé Chabanne, David Pointcheval, and Qiang Tang. "Extended private information retrieval and its application in biometrics authentications". In: *International Conference on Cryptology and Network Security*. Springer. 2007, pp. 175–193.

[10] Sébastien Canard, Julien Devigne, and Olivier Sanders. "Delegating a pairing can be both secure and efficient". In: *International Conference on Applied Cryptography and Network Security*. Springer. 2014, pp. 549–565.

[11] Sherman S.M. Chow, Man Ho Au, and Willy Susilo. "Server-Aided Signatures Verification secure against collusion attack". In: *Information Security Technical Report* 17.3 (2013), pp. 46 –57.

[12] John Daugman. "How iris recognition works". In: *IEEE Transactions on circuits and systems for video technology* 14.1 (2004), pp. 21–30.

[13] Yvo Desmedt. "Major security problems with the "unforgeable" (Feige)-Fiat-Shamir proofs of identity and how to overcome them". In: *Proceedings of SECURICOM*. Vol. 88. 1988, pp. 15–17.

[14] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. "Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation". In: *In Proceedings of the 5th ICSLP*. 1998, pp. 1351–1354.

[15] Ulrich Dürholz, Marc Fischlin, Michael Kasper, and Cristina Onete. "A formal approach to distance-bounding RFID protocols". In: *International Conference on Information Security*. Springer. 2011, pp. 47–62.

[16] Zekeriya Erkin, Martin Franz, Jorge Guajardo, Stefan Katzenbeisser, Inald Lagendijk, and Tomas Toft. "Privacy-preserving face recognition". In: *International Symposium on Privacy Enhancing Technologies Symposium*. Springer. 2009, pp. 235–253.

[17] David Evans, Yan Huang, Jonathan Katz, and Lior Malka. "Efficient privacy-preserving biometric identification". In: *Proceedings of the 17th conference Network and Distributed System Security Symposium*. 2011.

[18] Aurélien Francillon, Boris Danev, and Srdjan Capkun. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." In: *NDSS*. 2011.

[19] Rosario Gennaro, Craig Gentry, and Bryan Parno. "Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers". In: *Advances in Cryptology – CRYPTO*. 2010, pp. 465–482.

[20] Marc Girault and David Lefranc. "Server-Aided Verification: Theory and Practice". In: *Advances in Cryptology - ASIACRYPT 2005*. Vol. 3788. 2005, pp. 605–623.

[21] Gerhard P. Hancke and Markus G. Kuhn. "An RFID Distance Bounding Protocol". In: *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. SECURECOMM '05. IEEE Computer Society, 2005, pp. 67–73.

[22] David J. Hurley, Mark S. Nixon, and John N. Carter. "Force field feature extraction for ear biometrics". In: *Computer Vision and Image Understanding* 98.3 (2005), pp. 491 –512.

[23] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. "Biometric template security". In: *EURASIP Journal on Advances in Signal Processing* 2008 (2008), p. 113.

[24] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. "The swiss-knife RFID distance bounding protocol". In: *International Conference on Information Security and Cryptology*. Springer. 2008, pp. 98–115.

[25] Wai Kin Kong, David Zhang, and Wenxin Li. "Palmprint feature extraction using 2-D Gabor filters". In: *Pattern Recognition* 36.10 (2003), pp. 2339 –2347.

[26] Chae Hoon Lim and Pil Joong Lee. "Server (Prover/Signer)-Aided Verification of Identity Proofs and Signatures". In: *EUROCRYPT '95*. 1995, pp. 64–78.

[27] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. "SCiFI - A System for Secure Face Identification". In: *Security and Privacy, 2010 IEEE Symposium on*. 2010, pp. 239–254.

[28] L.S. Penrose. "Dermatoglyphic Topology". In: *Nature* 205 (1965), pp. 544–546.

[29] J. Reid, J. M. Gonzalez Nieto, T. Tang, and B. Senadji. "Detecting Relay Attacks with Timing-based Protocols". In: *ASIACCS '07: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*. Singapore: ACM, 2007, pp. 204–213.

[30] Arun Ross and Anil Jain. "Information fusion in biometrics". In: *Pattern recognition letters* 24.13 (2003), pp. 2115–2125.

[31] Arun Ross and Anil K Jain. "Multimodal biometrics: An overview". In: *Signal Processing Conference, 2004 12th European*. IEEE. 2004, pp. 1221–1224.

[32] Ahmad-Reza Sadeghi, Thomas Schneider, and Immo Wehrenberg. "Efficient privacy-preserving face recognition". In: *International Conference on Information Security and Cryptology*. Springer. 2009, pp. 229–244.

[33] Kenta Takahashi Takao Murakami and Kanta Matsuura. "Toward Optimal Fusion Algorithms With Security Against Wolves and Lambs in Biometrics". In: *IEEE Transaction on Information Forensics and Security* 9 (2 2014).

[34] Liang Wang, Tieniu Tan, Huazhong Ning, and Weiming Hu. "Silhouette analysis-based gait recognition for human identification". In: *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 25.12 (2003), pp. 1505–1518.

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

[36] 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.

[37] Wei Wu, Yi Mu, Willy Susilo, and Xinyi Huang. "Server-Aided Verification Signatures: Definitions and New Constructions". In: *Provable Security*. Vol. 5324. 2008, pp. 141–155.

[38] Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshiba. "Packed homomorphic encryption based on ideal lattices and its application to biometrics". In: *International Conference on Availability, Reliability, and Security*. Springer. 2013, pp. 55–74.

[39] Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshiba. "Practical packing method in somewhat homomorphic encryption". In: *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2014, pp. 34–50.

[40] Naser Zaeri. "Minutiae-based Fingerprint Extraction and Recognition". In: *Computer and Information Science - Artificial Intelligence - "Biometrics"*. 2011.