# Authentication in Constrained Settings

Aikaterini Mitrokotsa

Chalmers University of Technology, Gothenburg, Sweden
aikmitr@chalmers.se

**Abstract.** Communication technologies have revolutionized modern society. They have changed the way we do business, travel, manage our personal lives and communicate with our friends. In many cases, this crucially depends on accurate and reliable authentication. We need to get authenticated in order to get access to restricted services and/or places (i.e. transport systems, e-banking, border control). This authentication is performed in constrained settings due to: i) privacy issues, ii) noisy conditions, iii) resource constraints. Privacy-preservation is essential for the protection of sensitive information (i.e. diseases, location, nationality). Noisy conditions refer to physical noise in the communication channel that may lead to modification of the transmitted information, or natural variability due to the authentication medium (e.g. fingerprint scans). Resource constraints refer to limited device power/abilities (i.e. sensors, RFID tags). It is a very challenging problem to develop privacy-preserving authentication for noisy and constrained environments that optimally balance authentication accuracy, privacy-preservation and resource consumption. In this paper, we describe the main challenges of the problem of authentication in constrained settings, the current state-of-the-art of the field and possible directions of research.

## 1 Introduction

Authentication used to rely on visual evidence and physical tokens (mechanical keys, signatures, official seals). As time progressed the use of communication technologies has had a tremendous expansion and a transformative impact in our life. Wireless and resource constrained technologies have already become widespread and are bound to become even more in the near future. Tiny and weak microprocessors, smart cards, RFID tags and sensors are now pervasive in machinery, supply chain management, environmental monitoring, smart home appliances, healthcare applications, keyless entry in automobiles, highway toll-collection and NFC (Near Field Communication)/WiFi payments. Often, these devices are required to perform critical authentication processes under noisy conditions, while respecting the privacy of the involved parties. Smart grids, energy efficiency, transport systems, vehicular networks, healthcare, inventory control and

mobile communication are just a few of the domains that benefit from reliable authentication.

Naturally, these new technologies suffer from serious limitations and security and privacy risks. Attackers might attempt to impersonate a legitimate user and get access to restricted services/locations while dishonest legitimate users may try to abuse their access rights. Numerous recent studies have shown that existing authentication systems can be easily broken.

Authentication is especially challenging when it appears under *constrained settings* due to: i) *privacy* issues, ii) *noisy* conditions, and iii) *resource* limits. This is a significant research challenge that needs to be addressed in order to guarantee reliable and secure communication and prepare us for the future Internet of Things (IoT) rather than the partial solutions of the "Intranet of Things".

By *privacy issues*, we refer to the risks raised by leaving our digital fingerprint whenever we get authenticated for a service/place. Especially for wireless communications the danger that private information shall be collected silently and cheaply is great.

By *noisy* conditions, we refer to the physical noise in the communication channel that may lead to transmission errors and subsequently to modification of the transmitted information. Additionally, noise might be due to the natural variability of the authentication information. For instance, two different scans of the same fingerprint would result to different captured data (i.e. due to the difference in finger pressure during the fingerprint scanning).

By *resource* limits, we refer to communication technologies with limited resources or high cost. These include wireless technologies such as wireless ad hoc networks, WSN (wireless sensor networks) and RFID (Radio Frequency Identification Systems) that are increasingly being deployed in a broad range of applications. There is a pertinent need for reliable but lightweight authentication mechanisms that can be deployed in such inherently resource-deprived technologies. Things become more challenging if we consider that authentication often involves the communication between heterogeneous devices with diverse computational and communication capabilities as well as storage power.

Due to these limitations, service providers and users become more reluctant on using resource-deprived devices that may jeopardise the reliability of a service and the user's privacy.

## 2 Current state of research in the field

We divide the research field into two main areas: i) authentication in *noisy conditions*, and ii) *privacy-preserving* authentication. Both of these areas include *resource constrained* devices.

### 2.1 Authentication in noisy conditions

*Noisy authentication & decision making:* Authentication is a *decision making* problem where we need to decide whether or not to accept the credentials of an identity-carrying entity; a decision that becomes very challenging under noisy conditions. The different regions of the authentication process depending on the certainty of the verifier (due to noise about the identity of the prover – legitimate user or adversary) could be discriminated into the following categories [1]: i) the *honest region* represents the cases for which the verifier has high confidence that the prover is a legitimate user. This could be when the prover is close enough to the verifier and thus erroneous responses are very few, ii) the *uncertainty region* represents the area where noise makes the verifier's decision difficult leading to errors, iii) the *adversarial region* represents the area where the verifier has high confidence that the entity that attempts to get authenticated is an adversary. This *decision making* process can be modeled using *game theory* [2]. The authentication problem is formulated as a two-player game between the authentication system (verifier) and the prover. Nevertheless, existing approaches [2] are based on unrealistic assumptions such as knowing the adversary's utility (payoff). It is an open question how to apply decision making techniques when the utility of the adversary and the model parameters are unknown.

Below we describe some representative cases of authentication in noisy conditions that are directly connected to the research problem of authentication in constrained settings.

*Distance-bounding authentication:* In many cases, we can only have access to a service by proving we are sufficiently close to a particular location. For instance, in applications such as automobile and building access control the key (prover) has to be close enough to the lock (verifier). In these cases, proximity can be guaranteed through signal attenuation. However, using additional transmitters an attacker can *relay* signals from a key that is located arbitrarily far [3]. This type of attack can also be mounted against bankcards [4], mobile phones, proximity cards [5] and wireless

ad hoc networks. Thus, the problem is: *How can the verifier check the distance of a prover?*

Distance-bounding (DB) protocols [6], are challenge-response authentication protocols, that allow the verifier, by measuring the time-of-flight of the messages exchanged, to calculate an upper bound on the prover's distance. The time-critical part of this authentication process is performed under noisy conditions, which implies that we should allow the responses to be partially incorrect. It is not easy to balance correctness with accuracy, while the resource constraints make this problem even more challenging. For this reason, many attacks [7,8,9,10,11,7,12,13] onto DB protocols [14,15,16,17] continue to be published. Recently, the first family of provably secure DB protocols – called SKI [18,19,20] – has been proposed, that is secure even under the real-life setting of noisy communications, against the main types of relay attacks. Another provably secure protocol that attains quite strong relay attack resistance requirements has been proposed recently by Fischlin and Onete [21]. A detailed comparison between the SKI family of protocols and the Fischlin and Onete protocol [21] is given by Vaudenay [22].

Additionally, for this class of protocols an analysis of the expected loss when authenticating an attacker and when legitimate users are not authenticated [23,24] has been performed. However, the security of DB protocols is dependent on the underlying communication channel. It is an open question whether the proposed DB protocols can be applied in practice in conventional channels similar to those in NFC.

*Biometric authentication:* Biometric techniques [25] are a potential simple and efficient method for authentication. However, this is not straightforward. The data collecting process has a high degree of variability. For instance, two different scans of the same fingerprint would result to different captured data (i.e. difference in finger pressure during the fingerprint scan, orientation and dirty finger). The biometric comparison and the approximate equality between a fresh biometric trait and a stored biometric template is a challenge for any biometric scheme. Different approaches have been proposed to efficiently perform this comparison based on error-correcting codes [26], fuzzy commitments, fuzzy vaults [27], fuzzy extractors [28]. Many of these approaches have been shown to be vulnerable to multiple attacks. More robust approaches are those based on secure multi-party computation [29] algorithms. Among the most challenging problems in biometric authentication are: (i) the resistance to impersonation attacks [30], (ii) the irrevocability of biometric templates,

and (iii) guarantee that personal information will remain private. Furthermore, biometrics can be used for authentication in mobile devices [31,32] but in this case the authentication problem becomes more challenging considering the limited available resources.

*Other cases:* Captchas and Physically Unclonable Functions (PUFs) are also strongly connected to the authentication problem under noisy conditions. Captchas are employed in online transactions to make sure that the entity that attempts to get authenticated is a human being and not a machine [33]. The challenge consists of a set of puzzles, which the prover must solve. Erroneous response may be given by humans due to simple mistakes or comprehension difficulties. While the security of captcha-like puzzles has been analyzed for the case where the error rates are known [34], it is an open question whether captchas with a certain performance profile can be automatically designed. PUFs are used mainly for device identification and authentication [35,36] as well as for binding software to hardware platforms [37,38] and anti-counterfeiting [39]. PUFs authentication involves generating a response that depends both on the received challenge as well as on physical properties (i.e. ambient temperature, supply voltage) of the object in which the PUF is embedded. Thus, a PUF will always return a slightly different response for the same challenge.

### 2.2 Privacy-preserving authentication

Often, we need to get authenticated without revealing sensitive information. We consider two types of privacy preservation: privacy-preservation of *context information* such as the location of a sensor or an RFID tag as well as privacy-preservation of *content information* such as biometric templates or information related to our medical history, our nationality etc.

*Location & identity privacy:* Location and identity can be easily leaked when using wireless communications by eavesdropping transmitted messages, checking signal strengths and messages' arrival times. A survey of privacy preservation in wireless sensor networks is presented in [40], while [41] investigates the identity privacy problem in the context of RFID communication. More general privacy problems have been studied in the fields of data mining [42] and databases [43] both of which are intrinsically linked to the authentication problem. Rasmussen and Čapkun have proposed a location privacy-preserving distance bounding protocol (RČ) [44]. Nevertheless, this protocol has several problems [11,7]. A new DB protocol [7] that improves the basic construction of the RČ

protocol has been proposed. However, location privacy considering the information leakage at the physical layer is quite challenging. It has been shown recently [45], that for protocols with a beginning or a termination, it is theoretically impossible to achieve location privacy for very powerful adversaries (omniscient). However for limited adversaries, carefully chosen parameters enable computational, provable location privacy.

*Privacy & biometrics:* Biometric authentication involves the comparison between a fresh and a stored biometric template. This comparison is usually performed using some distance or divergence between the fresh and stored template. Later on the distance is compared to a pre-defined threshold and an authentication decision is taken (acceptance/rejection). Numerous approaches have been proposed in order to guarantee privacy-preserving biometric authentication: quantization schemes [46], fuzzy extractors [28], fuzzy commitment [47], cancelable biometrics [48], and fuzzy vault [27], while the most secure are based on secure-multi party computation techniques including oblivious transfer [49], homomorphic encryption [50] as well as private information retrieval [51]. Multiple privacy-preserving biometrics authentication protocols have been proposed based on secure multi-party computation [52,53,54]. Nevertheless, it has been proven that many of these schemes are vulnerable to threats [55], such as cross-matching [56] and hill-climbing [55,57,58,59]. More precisely, it has been recently proven that all biometric authentication protocols (including privacy-preserving ones) that rely on leaking distances (e.g. Hamming distance, Euclidean distance) are susceptible to leakage of information that may lead to the disclosure of stored biometric templates (even if the latter are encrypted). Pagnin et al. [60] provide a formal mathematical framework to analyse this leakage.

*Privacy & machine learning:* The authentication problem especially using biometrics relies extensively on machine learning techniques. Privacy-learning has been studied by research communities in security, databases, theory, machine learning and statistics. Recently, the strands of this work have begun to merge, with the formalism of *differential privacy* [61]. Differential privacy offers a formal framework that can be used to bound the amount of info that an adversary can discover. Much work has been done to understand how algorithms and methods can guarantee differential privacy and performance [62,63]. Recently Dimitrakakis et al. [64] have generalized the concept of differential privacy to arbitrary dataset distances and proved that Bayesian learning is inherently private. Recently a number

of differentially-private versions of machine learning algorithms have been proposed (e.g. [65]).

## 3 Open Questions and Challenges

In order to solve the problem of authentication in constrained settings we need to address the following questions:

- How robust is an authentication system performing under noisy conditions and resource constraints?
- How can we minimise the resource cost?
- How can we maximize (/*minimise*) the probability to authenticate a legitimate user (/*an attacker*)?
- How can we preserve the privacy rights of the parties involved in the authentication process in a collective way?

Many of existing authentication protocols use informal models and are poorly grounded theory. Additionally, in many cases the information leakage is addressed locally without considering that an adversary may have access to multiple services or devices. The following dimensions of the problem need to be taken into account when we design reliable and privacy-preserving authentication protocols for constrained settings.

*i)* The privacy implications of wireless communication may lead to oppressive electronic data surveillance. The wireless medium renders the privacy preservation a big challenge. To combat eavesdropping and the involvement of untrusted parties (e.g. databases) secure multi-party computation and differential privacy are valuable tools that could be employed. However, there is a need for development of lightweight techniques for resource-constrained devices where the trade-off between privacy and computation is tuned according to the target application.

*ii)* Designing provably secure protocols resistant to relay attacks is a very challenging task. Accurate authentication could be strengthened by relying on cross-layer authentication protocols that employ properties of the physical layer (e.g. noise of the communication channel, response time) in order to provide high security guarantees and efficiency in realistic conditions.

## References

1. Ahmadi, H., Safavi-Naini, R.: Secure distance bounding verification using physical-channel properties. arXiv:1303.0346 (2013)

2. Barni, M.: A game theoretic approach to source identification with known statistics. In: Proc. of ICASSP'12, Kyoto, Japan (Mar. 2012) 1745–1748
3. Francillon, A., Danev, B., Čapkun, S.: Relay attacks on passive keyless entry and start systems in modern cars. In: Proc. NDSS'11, San Diego, CL, USA (2011)
4. Drimer, S., Murdoch, S.J.: Keep your enemies close: distance bounding against smartcard relay attacks. In: Proc. of USENIX'07, Berkeley, CA, USA (2007) 7:1–7:16
5. Hancke, G.P., Mayes, K.E., Markantonakis, K.: Confidence in Smart Token Proximity: Relay Attacks Revisited. Computers & Security **28**(7) (October 2009) 404–408
6. Brands, S., Chaum, D.: Distance-Bounding Protocols (Extended Abstract). In: Proc. of EUROCRYPT'93. (1993) 344–359
7. Mitrokotsa, A., Onete, C., Vaudenay, S.: Mafia Fraud Attack against the RČ Distance-Bounding Protocol. In: Proc. IEEE RFID-TA'12, Nice, France (Nov. 2012) 74–79
8. Munilla, J., Peinado, A.: Attacks on a Distance Bounding Protocol. Computer Communications **33** (2010) 884–889
9. Boureanu, I., Mitrokotsa, A., Vaudenay, S.: On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols – PRF-ness alone Does Not Stop the Frauds! In: Proc. of LATINCRYPT 2012. Volume 7533 of LNCS., Springer (Oct. 2012) 100–120
10. Bay, A., Boureanu, I., Mitrokotsa, A., Spulber, I., Vaudenay, S.: The Bussard-Bagga and Other Distance Bounding Protocols under Man-in-the-Middle Attacks. In: Proceedings of Inscrypt'2012, 8th China International Conference on Information Security and Cryptology. Lecture Notes in Computer Science, Beijing, China, Springer (2012)
11. Aumasson, J.P., Mitrokotsa, A., Peris-Lopez, P.: A Note on a Privacy-Preserving Distance-Bounding Protocol. In: Proc. of ICICS'11. LNCS, Beijing, China (Nov. 2011) 78–92
12. Mitrokotsa, A., Peris-Lopez, P., Dimitrakakis, C., Vaudenay, S.: On selecting the nonce length in distance-bounding protocols. The Computer Journal **56**(10) (April 2013) 1216–1227
13. Mitrokotsa, A., Dimitrakakis, C., Peris-Lopez, P., Castro, J.C.H.: Reid et al.'s distance bounding protocol and mafia fraud attacks over noisy channels. IEEE Communications Letters **14**(2) (February 2010) 121–123
14. Singelée, D., Preneel, B.: Distance Bounding in Noisy Environments. In: Proc. ESAS'07. Volume 4572 of LNCS., Springer-Verlag (2007) 101 –115
15. Tu, Y.J., Piramuthu, S.: RFID Distance Bounding Protocols. In: Proc. EURASIP Workshop on RFID Technology, Vienna, Austria (Sept. 2007) 67–68
16. Bussard, L.: Trust Establishment Protocols for Communicating Devices. PhD thesis, Ecole Nationale Supérieure des Télécommunications, Institut Eurécom, Télécom Paris (2004)
17. Kim, C.H., Avoine, G., Koeune, F., Standaert, F., Pereira, O.: The Swiss-Knife RFID Distance Bounding Protocol. In: Proc. of ICISC'08. LNCS, Springer-Verlag (Dec. 2008)
18. Boureanu, I., Mitrokotsa, A., Vaudenay, S.: Secure & lightweight distance-bounding. In: Proc. of LightSec'13, Gebze, Turkey (May 6-7 2013)
19. Boureanu, I., Mitrokotsa, A., Vaudenay, S.: Practical and provably secure distance-bounding. In: Proceedings of the 16th Information Security Conference (ISC), Dallas, Texas, USA (November 2013)

20. Boureanu, I., Mitrokotsa, A., Vaudenay, S.: Practical & provably secure distance-bounding. Journal of Computer Security (2014)
21. Fischlin, M., Onete, C.: Terrorism in distance bounding: Modeling terrorist fraud resistance. In: Proceedings of the International Conference on Applied Cryptography and Network Security ACNS'13. Volume 7954 of lncs., Springer (2013) 414 – 431
22. Vaudenay, S.: On modeling terrorist frauds - addressing collusion in distance bounding protocols. In: Proceedings of the 7th International Conference on Provable Security (ProvSec 2013). Volume 8209 of Lecture Notes in Computer Science., Melaka, Malaysia, Springer (October 2013) 1–20
23. Dimitrakakis, C., Mitrokotsa, A., Vaudenay, S.: Expected Loss Bounds for Authentication in Constrained Channels. In: Proc. of INFOCOM'12, Orlando, FL, USA (Mar. 2012) 478–85
24. Dimitrakakis, C., Mitrokotsa, A., Vaudenay, S.: Expected loss analysis for authentication in constrained channels. Journal of Computer Security (2014)
25. Li, S.Z., Jain, A.K., eds.: Encyclopedia of Biometrics. Springer US (2009)
26. Sukarno, P., Phu, M., Bhattacharjee, N., Srinivasan, B.: Increasing error tolerance in biometric systems. In: Proc. MoMM'10, New York, NY, USA, ACM (2010) 50–55
27. Juels, A., Sudan, M.: A fuzzy vault scheme. Jrnl Designs, Codes & Cryptography **38**(2) (February 2006) 237–257
28. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing **38**(1) (March 2008) 97–139
29. Tuyls, P., Skoric, B., Kevenaar, T., eds.: Security with Noisy Data — On Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer Berlin/Heidelberg (April 2007)
30. Une, M., Otsuka, A., Imai, H.: Wolf attack probability: A new security measure in biometric authentication systems. In Lee, S.W., Li, S., eds.: Advances in Biometrics. Volume 4642 of LNCS. (2007) 396–406
31. Tresadern, P., Cootes, T.F., Poh, N., Matejka, P., Hadid, A., Levy, C., McCool, C., Marcel, S.: Mobile biometrics: Combined face and voice verification for a mobile platform. IEEE Pervasive Computing **12**(1) (2013) 79–87
32. Clarke, N., Furnell, S.: Authentication of users on mobile telephones – a survey of attitudes and practices. Computers & Security **24**(7) (2005) 519 – 527
33. Ahn, L.V., Blum, M., Hopper, N.J., Langford, J.: Captcha: using hard ai problems for security. In: Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques. EUROCRYPT'03, Berlin, Heidelberg, Springer-Verlag (2003) 294–311
34. T. Baignères, P. Sepehrdad, S.V.: Distinguishing distributions using chernoff information. In: 4th International Conference on Provable ÄProvSecSecurity 2010 (ProvSec 2010), Malacca, Malaysia, Springer-Verlag (13-15 October 2010)
35. Sadeghi, A.R., Visconti, I., Wachsmann, C.: Enhancing RFID Security and Privacy by Physically Unclonable Functions. In Sadeghi, A.R., Naccache, D., eds.: Towards Hardware-Intrinsic Security, Information Security and Cryptography – THIS 2010, Springer (November 2010) 281–305
36. Sjouke, M., Piramuthu, S.: A PUF-based authentication protocol to address ticket-switching of RFID-tagged items. In: 8th International Workshop on Security and Trust Management – STM 2012, Pisa, Italy (September 2012)
37. Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: Fpga intrinsic pufs and their use for ip protection. In: Proceedings of the 9th international workshop on

Cryptographic Hardware and Embedded Systems. CHES '07, Berlin, Heidelberg, Springer-Verlag (2007) 63–80
38. Kumar, S.S., Guajardo, J., Maes, R., Schrijen, G.J., Tuyls, P.: Extended abstract: The butterfly PUF protecting IP on every FPGA. In: Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust. HST '08, Washington, DC, USA, IEEE Computer Society (2008) 67–70
39. Tuyls, P., Batina, L.: Rfid-tags for anti-counterfeiting. In: Proceedings of the 2006 The Cryptographers' Track at the RSA conference on Topics in Cryptology. CT-RSA'06, Berlin, Heidelberg, Springer-Verlag (2006) 115–131
40. Li, N., Zhang, N., Das, S.K., Thuraisingham, B.: Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Networks **7**(8) (Nov. 2009) 1501–1514
41. Vaudenay, S.: On privacy models for rfid. In: Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security. ASIACRYPT'07, Berlin, Heidelberg, Springer-Verlag (2007) 68–87
42. Agrawal, R., Evfimievski, A., Srikant, R.: Information sharing across private databases. In: Proc. of ACM SIGMOD'03, NY, USA, ACM (2003) 86–97
43. Agrawal, R., Srikant, R.: Privacy-preserving data mining. In: Proc. of ACM SIGMOD'00, NY, USA, ACM (2000) 439–450
44. Rasmussen, K., Čapkun, S.: Location Privacy of Distance Bounding. In: Proc. CCS'08, ACM (2008) 149–160
45. Mitrokotsa, A., Onete, C., Vaudenay, S.: Location leakage in distance bounding: Why location privacy does not work. Computers & Security **45** (2014) 199–209
46. Linnartz, J.P., Tuyls, P.: New shielding functions to enhance privacy and prevent misuse of biometric templates. In: Proc. of AVBPA'03, Berlin, Heidelberg, Springer-Verlag (2003) 393–402
47. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Proc. of CCS'99, NY, USA (1999) 28–36
48. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4) (2007) 561–572
49. Rabin, M.O.: How to exchange secrets with oblivious transfer. IACR Cryptology ePrint Archive **2005** (2005) 187
50. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: EUROCRYPT 1999. Volume 1592 of LNCS. Springer (1999) 223–238
51. Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M.: Private information retrieval. J. ACM **45**(6) (November 1998) 965–981
52. Bringer, J., Chabanne, H., Izabachène, M., Pointcheval, D., Tang, Q., Zimmer, S.: An application of the goldwasser-micali cryptosystem to biometric authentication. In: ACISP 2007. LNCS, Springer-Verlag (2007) 96–106
53. Stoianov, A.: Cryptographically secure biometrics. In: Proc. SPIE 7667, Biometric Technology for Human Identification VII. Volume 76670C. (April 2010) 76670C–76670C–12
54. Barbosa, M., Brouard, T., Cauchie, S., Sousa, S.M.: Secure biometric authentication with improved accuracy. In Mu, Y., Susilo, W., Seberry, J., eds.: ACISP 2008. Volume 5107 of LNCS., Springer (2008) 21–36
55. Simoens, K., Bringer, J., Chabanne, H., Seys, S.: A framework for analyzing template security and privacy in biometric authentication systems. IEEE Transactions on Information Forensics and Security **7**(2) (2012) 833–841

56. Simoens, K., Tuyls, P., Preneel, B.: Privacy weaknesses in biometric sketches. In: IEEE Symp. Sec. & Priv. (May 2009) 188–203
57. Abidin, A., Mitrokotsa, A.: Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-lwe. In: Proceedings of the IEEE Workshop on Information Forensics and Security 2014 (WIFS 2014), Atlanta, USA (Dec. 2014)
58. Abidin, A., Matsuura, K., Mitrokotsa, A.: Security of a privacy-preserving biometric authentication protocol revisited. In: Cryptology and Network Security - 13th International Conference, CANS 2014, Heraklion, Crete, Greece, October 22-24, 2014. Proceedings. (2014) 290–304
59. Abidin, A., Pagnin, E., Mitrokotsa, A.: Attacks on privacy-preserving biometric authentication. In: Proceedings of the 19th Nordic Conference on Secure IT Systems (NordSec 2014), Tromso, Norway (October 2014) 293–294
60. Pagnin, E., Dimitrakakis, C., Abidin, A., Mitrokotsa, A.: On the leakage of information in biometric authentication. In: Proceedings of the 15th International Conference on Cryptology in India INDOCRYPT 2014, New Delhi, India (December 2014) 265–280
61. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Proc. of TCC'06. (2006) 265–284
62. Blum, A., Ligett, K., Roth, A.: A learning theory approach to non-interactive database privacy. In: STOC'08. (2008) 609–618
63. Kasiviswanathan, S.P., Lee, H.K., Nissim, K., Raskhodnikova, S., Smith, A.: What can we learn privately? In: Proc. of FOCS'08. (2008) 531–540
64. Dimitrakakis, C., Nelson, B., Mitrokotsa, A., Rubinstein, B.I.P.: Robust and private bayesian inference. In: Proceedings of the 25th International Conference in Algorithmic Learning Theory ALT 2014. Volume 8776 of Lecture Notes in Computer Science., Bled, Slovenia, Springer (October 2014) 291–305
65. Chaudhuri, K., Monteleoni, C., Sarwate, A.D.: Differentially private empirical risk minimization. JMLR **12** (2011) 1069–1109