UMR IRISA

Team EMSEC

Embedded Security and Cryptography

Rennes

Activity Report

2016

1 Team

Head of the team

Gildas Avoine, Professor, INSA Rennes
Pierre-Alain Fouque, Professor, Université Rennes 1

Administrative assistant

Cécile Bouton

Université Rennes 1 personnel

Patrick Derbez, Assistant Professor

INSA Rennes personnel

Barbara Kordy, Assistant Professor

CNRS personnel

Stéphanie Delaune, Researcher (since September 2016)
Adeline Roux-Langlois, Researcher

Postdocs

Cristina Onete, since September 2015
Cyrille Wiedling, since January 2016

PhD students

Pauline Bert, since October 2016
Raphaël Bost, since September 2014
Claire Delaplace (also affiliated to Université Lille 1), since September 2015
Loic Ferreira (also affiliated to Orange Labs Caen), since October 2016
Thomas Gougeon (also affiliated to ENSICAEN), since September 2014
Pierre Karpman, 09/2013 - 09/2016
Baptiste Lambin, since October 2016
Pierre Lestringant (also affiliated to Amossys), since October 2013
Brice Minaud, 10/2014 - October 2016
Chen Qian, since October 2016
Benjamin Richard (also affiliated to Orange Labs), since December 2013
Alban Siffer (also affiliated to Amossys), since October 2016
Florent Tardif, since January 2016
Wojciech Wideł, since November 2016

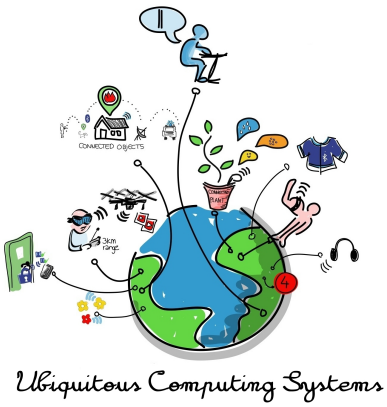
Associate members

Benoît Gérard, DGA, part-time (20%).

2 Overall Objectives

2.1 Overview

Recent technological advances in hardware and software have irretrievably affected the classical picture of computing systems. Today, these systems no longer consist only of connected servers, but involve a wide range of pervasive devices. This new paradigm, where information processing is embedded into everyday objects, has brought the concept of "ubiquitous computing systems". Such pervasive devices perform actions on behalf of their users for access control in mass transportation, payment, building access control, vehicle ignition systems, and many others.



Three distinctive characteristics of pervasive devices have a strong impact on their security: (1) they suffer from low memory and processing capabilities, which makes the use of highly secure building blocks difficult, (2) they mostly rely on hardware and embedded software, which causes longer life-cycles and make much harder to integrate up-to-date components, (3) they frequently contain collected personal data, which raises the problem of privacy.

Only recently researchers started to focus on the security of ubiquitous devices. Despite this, they already managed to find critical flaws in several widely deployed devices. For example, Texas Instruments' Digital Signature Transponder was successfully attacked in 2005 [BGS+05]; Mifare Classic was completely "dismantled" by several research teams [NESP08,GdKGM+08]; critical flaws in the KeeLoq ignition car system were revealed [Bog07];

[BGS+05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydlo, "Security Analysis of a Cryptographically-Enabled RFID Device", *in : 14th USENIX Security Symposium – USENIX'05*, USENIX, p. 1–16, Baltimore, Maryland, USA, July–August 2005.

[NESP08] K. Nohl, D. Evans, Starbug, H. Plotz, "Reverse-Engineering a Cryptographic RFID Tag", *in : 17th USENIX Security Symposium – USENIX'08*, P. C. van Oorschot (editor), USENIX, p. 185–194, San Jose, California, USA, July 2008.

[GdKGM+08] F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. Wichers Schreur, "Dismantling MIFARE Classic", *in : 13th European Symposium on Research in Computer Security – ESORICS 2008*, S. Jajodia, J. López (editors), *Lecture Notes in Computer Science*, *5283*, Springer, p. 97–114, Malaga, Spain, October 2008.

[Bog07] A. Bogdanov, "Attacks on the KeeLoq Block Cipher and Authentication Systems", *in : Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.

serious weaknesses were found in iClass [GdKGV11] and Hitag2 [VGB12]; DESFire MF3ICD40 suffers from side-channel attacks [OKP11]; etc. This enumeration could be long and quite worrying because applications from which we expect high security are not immune to security problems. For example, a "fatal" flaw in the random number generator of Taiwan's ID cards has very recently been discovered [BCC+13].

The scientific challenges in ubiquitous computing touch many research fields as telecommunication, microelectronics, computer networks, social science, etc. Improving the security in this domain is one of tomorrow's challenges that will enable its large-scale deployment in applications more innovative than ever. If secure countermeasures evolved slower than attacks, this deployment would be endangered. The provided examples demonstrate that the margin between knowledge to secure systems and those to break systems is thin.

The research team emsec will address the security of ubiquitous computing systems from a cryptographic perspective. We indeed aim to design, develop, and apply cryptographic primitives and protocols in order to analyze and improve the security of ubiquitous computing systems. Such systems are the expected application domain of emsec's research activities, and they include (but are not limited to) hardware devices (smartcards, RFID, FPGA, etc.) and software implementations (smartphones, embedded systems, etc.)

2.2 Key Issues

The work plan of the team is divided into four fully complementary layers, hereafter named "axis", and organized from theory to practice, in order to address security with a vertical approach.

1. Axis 1: Security Models
2. Axis 2: Design and Cryptanalysis of Primitives, Schemes, and Protocols
3. Axis 3: Hardware and Software Security
4. Axis 4: Security Analysis of Real-world Systems

Security Models

One of the major concerns of information security is to establish security proofs. Such proofs only make sense if they are done in a well-established model with strong enough security

[GdKGV11] F. D. Garcia, G. de Koning Gans, R. Verdult, "Exposing iClass Key Diversification", *in: WOOT*, p. 128–136, 2011.

[VGB12] R. Verdult, F. Garcia, J. Balasch, "Gone in 360 Seconds: Hijacking with Hitag2", *in: 21th USENIX Security Symposium – USENIX'12*, USENIX, USENIX Association, p. 237–252, Bellevue, WA, USA, August 2012.

[OKP11] D. Oswald, T. Kasper, C. Paar, "Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation", *in: Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.

[BCC+13] D. J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, T. Lange, N. van Someren, "Factoring RSA keys from certified smart cards: Coppersmith in the wild", Rump Session of CRYPTO'13, August 2013.

assumptions. The field of security dedicated to ubiquitous computing systems is not yet mature and many topics are currently intensively addressed by the research community without well-established models.

A few short-term objectives:

- One important topic concerns the study of cryptographic assumptions used to construct cryptosystems. Nowadays, the security of lattice cryptosystems is crucial and many problems related to the Learning With Errors (LWE) problems have been proposed. For instance, some schemes are been proved secure if the Binary-LWE and Learning With Rounding (LWR) problems are hard. We are interested in looking at the security of these new cryptographic assumptions by finding new algorithms to solve them and by studying the security of cryptographic constructions based on these problems.

- Another topic is the study of security models. Following Maurer's work on random systems, we also consider the constructive method to propose security proof. Cristina Onete is a postdoc researcher collaborating with us on this topic and she is currently studying the security of TLS 1.2 and 1.3 in this new theoretical model.

- Being able to analyze the security of a system by taking its digital, physical as well as social aspects into account is also an important issue in information security. Models based on attack trees [KPCS14] allow a security analyst to represent attacks exploiting socio-technical vulnerabilities of systems and to evaluate them in a quantitative way. However, the current formal analysis methods for such models are not powerful enough to represent all aspects that are relevant to perform a fully-fledged security analysis. The short-term objectives include the enhancement of attack–defense trees [KMRS14] recently introduced by Barbara Kordy et al., with cause-consequence dependencies between their nodes in order to augment the modeling capabilities of the formalism.

Design and Analysis of Primitives, Schemes, and Protocols

The next axis concerns the construction and analysis of cryptographic systems. The first topic will study the design of new cryptosystems based on a security proof.

A few short-term objectives:

- Cloud security based on symmetric searchable encryptions which reduce the amount of leakage that is revealed to the servers (PhD student with the Cloud Security ERC Project of David Pointcheval)

[KPCS14] B. Kordy, L. Piètre-Cambacédès, P. Schweitzer, "DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees", *Computer Science Review 13–14*, 0, 2014, p. 1–38.

[KMRS14] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, "Attack–Defense Trees", *Journal of Logic and Computation 24*, 1, 2014, p. 55–87.

- Conception of secure countermeasures for masking symmetric cryptosystems. Here, we already proposed efficient compiler that takes as input a non-protected algorithm and outputs a protected algorithm in C code using masking techniques. It will be interesting to study the security of the latter compiled code or executed code with its environment. (PhD Student with Michel Abdalla - Joint-Project with IMDEA team)
- Design of distance bounding protocols that match the practical constraints of low-cost contactless devices, especially NFC-based payment systems and access control systems.
- The security of lattice-based cryptosystems with applications to Fully Homomorphic Encryption (FHE) schemes and multi-linear maps is an actual hot topic in Cryptography. The recent CNRS position of Adeline Langlois will bring the EMSEC team in a good position regarding this active research area.

The second topic of this axis concerns the cryptanalysis, which constitutes the main research expertise of several EMSEC members, as well as logical methods for the verification of communication protocols.

A few short-term objectives:

- Cryptanalysis of schemes used for building white-box cryptography.
- Cryptanalysis of hash functions and encryption schemes (lightweight block ciphers) and authenticated encryption schemes (CAESAR competition).
- Cryptanalysis of multi-linear maps.
- Improvement of the cryptanalytic time-memory trade-off techniques, which allow a brute force to be performed faster when precalculations can be used.
- Symbolic verification, using tools like ProVerif, Tamarin or Scyther, will be employed to study logical attacks against communication protocols. One of the goals of this work will be to define the attacker model capturing the characteristics relevant for the security analysis of ubiquitous systems, such as time or distance.

Hardware and Software Security

Hardware and software security engineering is the study of security and privacy of practical systems. It basically deals with the design of robust systems and the evaluation of the required security policies. emsec will consider tools, processes, and methods of security engineering that enable security assessment of ubiquitous computing systems. This requires expertise in many areas such as cryptography, embedded devices, hardware designs, software implementations, testing and evaluation processes, tamper resistance, reverse-engineering, side-channel analyzes, and fault attacks.

In ubiquitous computing systems, security through obscurity is a common practice where cryptographic mechanisms are kept secret to make attacks harder to perform and to protect the manufacturer's innovation. So recovering the details of implemented mechanisms in an

embedded system is usually the first step before being able to assess the security of the system. emsec will exploit well-known reverse-engineering techniques and tools that exist in the field of software security to analyze ubiquitous computing systems, including side-channel analysis-based reverse engineering to gain information of the implemented algorithms.

Side-channel attacks are very powerful attacks with frequently devastating effects. They exploit existing flaws in the implementation of algorithms or can extract secret-key dependent information by measuring physical characteristics such as the power consumption or the electromagnetic emanation. Such attacks are highly promising and not sufficiently known by the community of ubiquitous computing. Even more important is the fact that especially ubiquitous computing devices are omnipresent and pervasive such that an adversary can easily extract them from insecure environments and to perform attacks at home or open labs.

A few short-term objectives:

- Develop a reverse-engineering tool to interpret data extracted from embedded devices (PhD student with Christophe Rosenberger, GREYC, Caen, France)
- Develop a reverse-engineering tool for recovering cryptographic implementations based on a static and/or dynamic analysis of a program (CIFRE PhD student Amossys)
- Study the security of lattice-based cryptosystems such as (NTRU, BLISS, ...)
- Side-Channel Attack on Pairing Schemes

Security Analysis of Real-world Systems

In spite of well-known good practices in the field of security engineering, many real-world systems suffer from critical weaknesses. Many examples are provided in the introduction of this document. Even though the quoted research seems destructive at first glance, the approach of finding vulnerabilities in real-world systems has given extremely valuable feedback to the security community. In fact, many of the successful attacks have led to much better security designs coming from industry and academia. We will apply the models studied in Axis 1 and the methodologies and tools developed in Axis 3 to real-world systems.

A few short-term objectives:

- Study a possibility of integrating attack–defense trees into practical risk assessment techniques based on EBIOS (joint master internship co-supervised by Orange Cyberdefense and Barbara Kordy).
- Evaluate the security of SSL/TLS implementations and figure out how poor they are used to be in embedded environments.
- Study the security of the authentication and key exchange EPS-AKA used in the 3GPP mobile phone standard (CIFRE PhD student).
- Study the security of some cryptographic library used in mobile phone (Android library based on electro-magnetic radiation with a CIFRE PhD student Orange Labs).

3 Scientific Foundations

3.1 Cryptography and Cryptanalysis

In the EMSEC team, we study the security of lattice-based cryptosystems from a cryptanalytical point of view, by providing attacks on the underlying hard problems, by evaluating the security assumptions, and by proposing new schemes based on these assumptions. We are also interested in new applications such as Fully Homomorphic Encryption schemes and multilinear maps. In symmetric cryptography, we are mainly interested in providing automatic tools to assess the security of symmetric primitives such as block ciphers. We study the security of white-box implementations as well. We also propose and analyze schemes with provable security for symmetric searchable encryptions and real-world protocols such as TLS to secure internet communications, AKA protocol to secure GSM communications, Lorawan for the Internet of Things, and SCP from GlobalPlatform for smardcards. Finally, we consider cryptanalytic tools, for example cryptanalytic time-memory trade-off techniques.

Keywords: Algebraic Number theory (Euclidean Lattices), Provable Security, Automatic tools for symmetric-key cryptanalysis, cryptographic protocols..

3.2 Formal Methods

One of the topics addressed by the EMSEC team is the application of formal methods for security modeling and analysis. In this context, we are conducting research mainly in two directions: symbolic specification and verification of security protocols and security modeling and analysis using graphical models originating from attack trees.

One successful approach when designing and analyzing security protocols, is the use of formal symbolic methods. The purpose of formal verification is to provide rigorous frameworks and techniques to analyse protocols and find their flaws. The techniques used in symbolic models have become mature and several tools for protocol verification are nowadays available, *e.g.* Avantssar platform [A+12], ProVerif tool [Bla01].

Keywords: Symbolic specification and verification of security protocols, ProVerif, Tamarin.

Attack trees have been originally introduced by Bruce Schneier in [Sch99] in 1999. Since then, they have become one of the most popular security model used in industrial setting [KPCS14].

[A+12] A. Armando *et al.*, "The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures", *in : Proc. 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'12), 7214*, Springer, p. 267–282, 2012.

[Bla01] B. Blanchet, "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules", *in : Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, IEEE Computer Society Press, p. 82–96, 2001.

[Sch99] B. Schneier, "Attack Trees: Modeling Security Threats", *Dr. Dobb's Journal of Software Tools 24*, 12, 1999, p. 21–29.

[KPCS14] B. Kordy, L. Piètre-Cambacédès, P. Schweitzer, "DAG-Based Attack and Defense

An attack tree is an intuitive illustration of an attacker's goal recursively refined into subgoals represented by the labels of the attack tree nodes. Due to the flexibility regarding the labels, attack trees are especially well-suited to reason about security of socio-technical and cyber-physical systems which combine digital, physical, and human dimensions.

In order to use any modeling framework in practice, formal foundations are necessary. Formal semantics for attack trees provide clear, mathematical meaning to this intuitive model [JKM+15,KMRS14]. Furthermore, a simple, tree-like structure of attack trees allows to propose methods for efficient quantification of security i.e., algorithms to quantify security-relevant aspects, such as attack probability, impact, cost, etc. [KMS16,AN15]. Techniques based on model checking and verification constitute formal foundations for automated generation of attack trees [PAV15].

Keywords: Attack trees, attack–defense trees, formal semantics, quantitative analysis of security.

3.3 Security of Software and Hardware Systems

We have described many attacks either on the implementations of Authenticated encryption schemes as AES-GSM, or on the implementations of ECDSA on Android and ECDSA with efficient morphisms and we describe some tools to automatically find fault attacks on RSA and EC signatures. We also study the security of countermeasures such as masking and implement some tools to check the security of to securely compile C code. Finally, more recently we look at the security of lattice-based signature schemes. From a more system-oriented view, we consider forensics on smartcards, and traceability through Web browsers.

Keywords: Side-Channel Analysis on embedded processors: Attacks (Fault attack, Power Analysis) and Countermeasures (Masking), Browser fingerprinting, Smartcard forensics..

Modeling: Don't Miss the Forest for the Attack Trees", *Computer Science Review 13–14*, 0, 2014, p. 1–38.

[JKM+15] R. Jhawar, B. Kordy, S. Mauw, S. Radomirovic, R. Trujillo-Rasua, "Attack Trees with Sequential Conjunction", *in : IFIP SEC 2015, IFIP AICT, 455*, Springer, p. 339–353, 2015.

[KMRS14] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, "Attack–Defense Trees", *Journal of Logic and Computation 24*, 1, 2014, p. 55–87.

[KMS16] B. Kordy, P. Marc, P. Schweitzer, "Probabilistic reasoning with graphical security models", *Information Sciences 342*, May 2016, p. 111–131, `https://hal.inria.fr/hal-01289186`.

[AN15] Z. Aslanyan, F. Nielson, "Pareto Efficient Solutions of Attack-Defence Trees", *in : POST, Lecture Notes in Computer Science, 9036*, Springer, p. 95–114, 2015.

[PAV15] S. Pinchinat, M. Acher, D. Vojtisek, "ATSyRa: An Integrated Environment for Synthesizing Attack Trees", *in : GraMSec 2015, LNCS, 9390*, Springer, 2015.

4 Application Domains

4.1 Lattice-based cryptography

Participants: Adeline Roux-Langlois, Pierre-Alain Fouque, Pauline Bert, Chen Qian, Paul Kirchner, Brice Minaud.

Collaborations: Martin R. Albrecht (Royal Holloway), Mehdi Tibouchi (NTT Japan).

- Lattice-based security foundation and constructions
  - Using Rényi divergence (Best paper award at ASIACRYPT 2015)
  - Implementing Multilinear maps (ASIACRYPT 2015)
- Cryptanalysis
  - Fully Homomorphic Encryption (COCOON 2016, CRYPTO 2015)
  - Attack on Multilinear map (EUROCRYPT 2016)
  - Attack on LWE (CRYPTO 2015)

Lattice-based cryptography is a good candidate for modern cryptography, this branch of cryptography is exploiting the presumed hardness of lattice problems. Its main advantages are simplicity, efficiency, and apparent security against quantum computers. The lattice-based cryptographic protocols also often enjoy security proofs based on the hardness of worst case problems. Moreover, lattice-based cryptography allows to construct a wide range of primitives from basic ones to most advanced ones. But it seems that there is a gap between what we can prove to be secure, and what is implemented in practice, and the biggest challenge in lattice-based cryptography today is to produce primitives that are both secure and efficient.

Another fascinating aspect of lattice-based cryptography is to make possible new primitives, which for now can only be constructed with lattices. The first one was the fully homomorphic encryption, constructed by Gentry [Gen09]. Another construction is cryptographic multilinear maps, first constructed in 2013 by Garg et al. [GGH13a]. This construction has many applications, it allows, for example, to obtain indistinguishability obfuscation [GGH+13b]. But the security of all the candidates of cryptographic multilinear maps is today very uncertain.

[Gen09] C. Gentry, "Fully homomorphic encryption using ideal lattices", *in: Proc. of STOC*, ACM, p. 169–178, 2009.

[GGH13a] S. Garg, C. Gentry, S. Halevi, "Candidate Multilinear Maps from Ideal Lattices", *in: Proc. of EUROCRYPT, LNCS, 7881*, Springer, p. 1–17, 2013.

[GGH+13b] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, B. Waters, "Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits", *in: Proc. of FOCS*, p. 40–49, 2013.

Security foundations. One of the main interest in lattice-based cryptography is that the security of protocols is proven under the hardness of worst-case problems on lattices. Studying the hardness of those problems is one of the research topic of members of the team.

In our ASIACRYPT 2015 paper [BLL+15], we show that the Rényi divergence can often be used as an alternative to the statistical distance in security proofs for lattice-based cryptography. The techniques used lead to security proofs for schemes with smaller parameters, and sometimes to simpler security proofs than the existing ones. We have several applications, in particular giving an alternative proof that the LWE problem with noise chosen uniformly in an interval is no easier than the Learning With Errors problem with Gaussian noise.

Practical Identity-based encryption. An Identity Based Encryption is an advance cryptographic construction where any arbitrary string can be used as a public key. The advantages of an IBE scheme are that we no longer need certificates, PKI etc. but we still need to trust an authority, the Public Key Generator, and we have to establish a secure channel between it and any user. Identity-based encryption is typically one of the cryptographic construction which is possible to build on lattice assumptions and which is close to be efficient and possible to use in practice. One of our project is to work on a variant of the IBE scheme proposed by Agrawal, Boneh and Boyen in 2010. We improved this scheme by reducing the size of some important parameters and we currently work on an implementation of this scheme.

Fully Homomorphic Encryption. Optimizing performance of Fully Homomorphic Encryption (FHE) is nowadays an active trend of research in cryptography. One way of improvement is to use a hybrid construction with a classical symmetric encryption scheme to transfer encrypted data to the Cloud. However, such a construction requires the decryption circuit of the symmetric scheme to be easy to evaluate homomorphically. In our COCOON 2016 paper [FHK16], we aim at minimizing the cost of the homomorphic evaluation of the decryption of symmetric encryption schemes. To do so, we focus on schemes based on learning problems: Learning With Errors (LWE), Learning Parity with Noise (LPN) and Learning With Rounding (LWR). We show that they have lower multiplicative depth than usual block ciphers, and hence allow more FHE operations before a heavy bootstrapping becomes necessary. Moreover, some of them come with a security proof. Finally, we implement our schemes in HElib.

Multilinear Maps. Multilinear maps serve as a basis for a wide range of cryptographic applications. The first candidate construction of multilinear maps was proposed by Garg, Gentry, and Halevi in 2013, and soon afterwards, another construction was suggested by Coron, Lepoint, and Tibouchi (CLT13). In our Asiacrypt 2015 paper [ACLL15], we provide the first implementation of the candidate construction proposed by GGH13 based on ideal lattices.

[BLL+15] S. Bai, A. Langlois, T. Lepoint, D. Stehlé, R. Steinfeld, "Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance", *in: ASIACRYPT*, 2015.

[FHK16] P. Fouque, B. Hadjibeyli, P. Kirchner, "Homomorphic Evaluation of Lattice-Based Symmetric Encryption Schemes", *in: COCOON*, p. 269–280, 2016.

[ACLL15] M. R. Albrecht, C. Cocis, F. Laguillaumie, A. Langlois, "Implementing Candidate Graded Encoding Schemes from Ideal Lattices", *in: ASIACRYPT, Part II*, p. 752–775, 2015.

Implementing GGH-like schemes naively would not allow instantiating it for non-trivial parameter sizes. We hence propose a strategy which reduces parameter sizes further and several technical improvements to allow for an efficient implementation.

However, both of these were found to be insecure in the face of so-called zeroizing attacks, by Hu and Jia, and by Cheon, Han, Lee, Ryu and Stehlé. To improve on CLT13, Coron, Lepoint, and Tibouchi proposed another candidate construction of multilinear maps over the integers at Crypto 2015 (CLT15). In our EUROCRYPT 2016 paper [CFL+16], we present two polynomial attacks on the CLT15 multilinear map, which share ideas similar to the cryptanalysis of CLT13. Our attacks allow recovery of all secret parameters in time polynomial in the security parameter, and lead to a full break of the CLT15 multilinear map for virtually all applications.

Cryptanalysis. At ACM-CCS 2014, Cheon, Lee and Seo introduced a new number-theoretic assumption, the Co-Approximate Common Divisor (Co-ACD) assumption, based on which they constructed several cryptographic primitives, including a particularly fast additively homomorphic encryption scheme. Unfortunately, it turns out that those parameters, originally aiming at 128-bit security, can be broken in a matter of seconds. Indeed, our CRYPTO 2015 paper [FLLT15] presents several lattice-based attacks against the Cheon-Lee-Seo (CLS) homomorphic encryption scheme and of the underlying Co-ACD assumption that are effectively devastating for the proposed constructions. A few known plaintexts are sufficient to decrypt any ciphertext in the symmetric-key CLS scheme, and small messages can even be decrypted without any known plaintext at all. This breaks the security of both the symmetric-key and the public-key variants of CLS encryption as well as the underlying decisional Co-ACD assumption. Moreover, Coppersmith techniques can be used to solve the search variant of the Co-ACD problem and mount a full key recovery on the CLS scheme.

In our CRYPTO 2015 paper [KF15], we study the Learning With Errors problem and its binary variant, where secrets and errors are binary or taken in a small interval. We introduce a new variant of the Blum, Kalai and Wasserman algorithm, relying on a quantization step that generalizes and fine-tunes modulus switching. In general this new technique yields a significant gain in the constant in front of the exponent in the overall complexity. We then introduce variants of BDD, GapSVP and UniqueSVP, and show how the previous algorithm is able to solve these variants in subexponential time. Moreover, we also show how the previous algorithm can be used to solve the BinaryLWE problem with n samples in subexponential time $2^{(\ln 2/2+o(1))n/\log\log n}$. This makes it possible to asymptotically and heuristically break the NTRU cryptosystem in subexponential time (without contradicting its security assumption). We are also able to solve subset sum problems in subexponential time for density $o(1)$, which is of independent interest: for such density, the previous best algorithm is in exponential time.

[CFL+16] J. H. Cheon, P. Fouque, C. Lee, B. Minaud, H. Ryu, "Cryptanalysis of the New CLT Multilinear Map over the Integers", *in: EUROCRYPT*, p. 509–536, 2016.

[FLLT15] P. Fouque, M. S. Lee, T. Lepoint, M. Tibouchi, "Cryptanalysis of the Co-ACD Assumption", *in: CRYPTO*, p. 561–580, 2015.

[KF15] P. Kirchner, P. Fouque, "An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices", *in: CRYPTO*, p. 43–62, 2015.

4.2 White-Box Cryptography

Participants: Patrick Derbez, Pierre-Alain Fouque, Brice Minaud, Pierre Karpman.

- Attacks on ASASA (ASIACRYPT 2015)
- New space-hard construction (ASIACRYPT 2016)
- New attacks on white-box construction

The ASASA construction is a new design scheme introduced at Asiacrypt 2014 by Biruykov, Bouillaguet and Khovratovich. Its versatility was illustrated by building two public-key encryption schemes, a secret-key scheme, as well as super S-box subcomponents of a white-box scheme. However one of the two public-key cryptosystems was recently broken at Crypto 2015 by Gilbert, Plût and Treger. In our main contribution at ASIACRYPT 2015 [MDFK15], we propose a new algebraic key-recovery attack able to break at once the secret-key scheme as well as the remaining public-key scheme, in time complexity 2^{63} and 2^{39} respectively (the security parameter is 128 bits in both cases). Furthermore, we present a second attack of independent interest on the same public-key scheme, which heuristically reduces its security to solving an LPN instance with tractable parameters. This allows key recovery in time complexity 2^{56}. Finally, as a side result, we outline a very efficient heuristic attack on the white-box scheme, which breaks an instance claiming 64 bits of security under one minute on a single desktop computer. This article has been considered as one of the best three article in this conference.

Recently, there have been several attempts to build white-box block ciphers whose implementations aim to be incompressible. This includes the weak white-box ASASA construction by Bouillaguet, Biryukov and Khovratovich from Asiacrypt 2014, and the recent space-hard construction by Bogdanov and Isobe from CCS 2015. In our ASIACRYPT'16 paper [FKKM16], we propose the first constructions aiming at the same goal while offering provable security guarantees. Moreover we propose concrete instantiations of our constructions, which prove to be quite efficient and competitive with prior work. Thus provable security comes with a surprisingly low overhead.

Finally, we recently broke a white-box scheme for AES proposed by Baek et al. in 2016. Our attack allows us to invert the scheme as well as to recover the key in matter of seconds. We are currently working on protecting the scheme by adding extra layers of security.

[MDFK15] B. Minaud, P. Derbez, P. Fouque, P. Karpman, "Key-Recovery Attacks on ASASA", *in: ASIACRYPT*, p. 3–27, 2015.

[FKKM16] P. Fouque, P. Karpman, P. Kirchner, B. Minaud, "Efficient and Provable White-Box Primitives", *in: ASIACRYPT*, p. 159–188, 2016.

4.3 Audit Tool to Find Attacks on Symmetric Primitives

Participants: Patrick Derbez, Pierre-Alain Fouque.

- Audit Tool for *block ciphers* (CRYPTO 2016)

Tracking bits through block ciphers and optimizing attacks at hand is one of the tedious task symmetric cryptanalysts have to deal with. It would be nice if a program will automatically handle them at least for well-known attack techniques, so that cryptanalysts will only focus on finding new attacks. However, current automatic tools cannot be used as is, either because they are tailored for specific ciphers or because they only recover a specific part of the attacks and cryptographers are still needed to finalize the analysis. At CRYPTO 2016 [DF16], we describe a generic algorithm exhausting the best meet-in-the-middle and impossible differential attacks on a very large class of block ciphers from byte to bit-oriented, SPN, Feistel and Lai-Massey block ciphers. Contrary to previous tools that target to find the best differential / linear paths in the cipher and leave the cryptanalysts to find the attack using these paths, we automatically find the best attacks by considering the cipher and the key schedule algorithms. The building blocks of our algorithm led to two algorithms designed to find the best simple meet-in-the-middle attacks and the best impossible truncated differential attacks respectively. We recover and improve many attacks on AES, mCRYPTON, SIMON, IDEA, KTANTAN, PRINCE and ZORRO. We show that this tool can be used by designers to improve their analysis.

We also study impossible differential attacks at FSE 2016 [Der16]. While impossible differential cryptanalysis is a well-known and popular cryptanalytic method, errors in the analysis are often discovered and many papers in the literature present flaws. Wishing to solve that, Boura et al. presented at ASIACRYPT'14 a generic vision of impossible differential attacks with the aim of simplifying and helping the construction and verification of this type of cryptanalysis. In particular, they gave generic complexity analysis formulas for mounting such attacks and develop new ideas for optimizing them. In our paper we carefully study this generic formula and show impossible differential attacks for which the real time complexity is much higher than estimated by it. In particular, we show that the impossible differential attack against 25-round TWINE-128, presented at FSE '15 by Biryukov et al., actually has a complexity higher than the natural bound of exhaustive search.

[DF16] P. Derbez, P. Fouque, "Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks", *in : CRYPTO*, p. 157–184, 2016.

[Der16] P. Derbez, "Note on Impossible Differential Attacks", *in : FSE*, p. 416–427, 2016.

4.4 Time-Memory Trade-Off (TMTO)

Participants: Gildas Avoine, Barbara Kordy, Florent Tardif.

Collaborations: UC Irvine (USA).

A cryptanalytic time-memory trade-off (TMTO) is a technique introduced by Martin Hellman in 1980 to reduce the time needed to perform an exhaustive search. The key-point of the technique resides in the precomputation of tables that are then used to speed up the attack itself. Given that the precomputation phase is much more expensive than an exhaustive search, a TMTO makes sense in a few scenarios, e.g., when the adversary has plenty of time for preparing the attack while she has a very little time to perform it, the adversary must repeat the attack many times, or the adversary is not powerful enough to carry out an exhaustive search but she can download precomputed tables. Problems targeted by TMTOs mostly consist in retrieving the preimage of a hashed value or, similarly, recovering a cryptographic key through a chosen plaintext attack. EMSEC collaborates with UC Irvine (USA) on TMTO techniques[AC17][ACL15][ACHC16]. We aim to provide improvements on the techniques to build and store tables, and we also consider practical issues, for example the benefit of using an SSD instead of RAM.

[AC17] G. Avoine, X. Carpent, "Heterogeneous Rainbow Table Widths Provide Faster Cryptanalyses", *in: Asia Conference on Computer and Communications Security – ASIACCS'17*, ACM, p. To Appear, Abu Dhabi, UAE, April 2017.

[ACL15] G. Avoine, X. Carpent, C. Lauradoux, "Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform Distributions", *in: European Symposium on Research in Computer Security – ESORICS*, G. Pernul, P. Y. A. Ryan, E. R. Weippl (editors), *Lecture Notes in Computer Science, 9326*, Springer-Verlag, p. 165–184, Vienna, Austria, September 2015.

[ACHC16] G. Avoine, X. Carpent, J. Hernandez-Castro, "Pitfalls in Ultralightweight Authentication Protocol Designs", *IEEE Transactions on Mobile Computing 15*, 9, September 2016, p. 2317–2332.

4.5 Security of 3G/4G Network Protocols

Participants: Pierre-Alain Fouque, Cristina Onete, Benjamin Richard.

Secure communications between mobile subscribers and their associated operator networks require mutual authentication and key derivation protocols. The 3GPP standard provides the AKA protocol for just this purpose. Its structure is generic, to be instantiated with a set of seven cryptographic algorithms. The currently-used proposal instantiates these by means of a set of AES-based algorithms called MILENAGE; as an alternative, the ETSI SAGE committee submitted the TUAK algorithms, which rely on a truncation of the internal permutation of Keccak. In our ACNS 2016 paper [AFM+16], we provide a formal security analysis of the AKA protocol in its complete three-party setting. We formulate requirements with respect to both Man-in-the-Middle (MiM) adversaries, i.e. key-indistinguishability and impersonation security, and to local untrusted serving networks, denoted "servers", namely state-confidentiality and soundness. We prove that the unmodified AKA protocol attains these properties as long as servers cannot be corrupted. Furthermore, adding a unique server identifier suffices to guarantee all the security statements even in in the presence of corrupted servers. We use a modular proof approach: the first step is to prove the security of (modified and unmodified) AKA with generic cryptographic algorithms that can be represented as a unitary pseudorandom function PRF keyed either with the client's secret key or with the operator key. A second step proceeds to show that TUAK and MILENAGE guarantee this type of pseudorandomness, though the guarantee for MILENAGE requires a stronger assumption. Our paper provides the first complete, rigorous analysis of the original AKA protocol and these two instantiations.

At PETS 2016 [FOR16], we study some privacy issue of the AKA protocol providing a mutually-authenticated key-exchange between clients and associated network servers. As a result AKA must guarantee the indistinguishability from random of the session keys (key-indistinguishability), as well as client- and server-impersonation resistance. A paramount requirement is also that of client privacy, which 3GPP defines in terms of: user identity confidentiality, service untraceability, and location untraceability. Moreover, since servers are sometimes untrusted (in the case of roaming), the AKA protocol must also protect clients with respect to these third parties. Following the description of client-tracking attacks e.g. by using error messages or IMSI catchers, van den Broek et al. and respectively Arapinis et al. each proposed a new variant of AKA, addressing such problems. In this paper we use the approach of provable security to show that these variants still fail to guarantee the privacy of mobile clients. We propose an improvement of AKA, which retains most of its structure and respects practical necessities such as key-management, but which provably attains security with respect to servers and Man-in-the- Middle (MiM) adversaries. Moreover, it is impossible to link client sessions in the absence of client-corruptions. Finally, we prove that any variant of AKA retaining its mutual authentication specificities cannot achieve client-unlinkability in the presence of corruptions. In this sense, our proposed variant is optimal.

[AFM+16] S. Alt, P. Fouque, G. Macario-Rat, C. Onete, B. Richard, "A Cryptographic Analysis of UMTS/LTE AKA", *in: ACNS*, p. 18–35, 2016.

[FOR16] P. Fouque, C. Onete, B. Richard, "Achieving Better Privacy for the 3GPP AKA Protocol", *PoPETs 2016*, 4, 2016, p. 255–275.

4.6 Cloud Protocol Security

Participants: Pierre-Alain Fouque, Raphaël Bost, Olivier Sanders (Orange Labs, Rennes).

- Symmetric Searchable Encryption: Externalize database on the cloud with privacy issues

Symmetric Searchable Encryption (SSE) is a very efficient and practical way for data owners to outsource storage of a database to a server while providing privacy guarantees. Such SSE schemes enable clients to encrypt their database while still performing queries for retrieving documents matching some keyword. This functionality is interesting to secure cloud storage, and efficient schemes have been designed in the past. However, security against malicious servers has been overlooked in most previous constructions and these only addressed security against honest-but-curious servers. We study and design the first efficient SSE schemes provably secure against malicious servers in [BFP16]. First, we give lower bounds on the complexity of such verifiable SSE schemes. Then, we construct generic solutions matching these bounds using efficient verifiable data structures. Finally, we modify an existing SSE scheme that also provides forward secrecy of search queries, and make it provably secure against active adversaries, without increasing the computational complexity of the original scheme.

Then, at ACM CCS [Bos16] we describe a new SSE scheme. Recent work shows that dynamic schemes - in which the data is efficiently updatable - leaking some information on updated keywords are subject to devastating adaptive attacks breaking the privacy of the queries. The only way to thwart this attack is to design forward private schemes whose update procedure does not leak if a newly inserted element matches previous search queries. This work proposes Sophos as a forward private SSE scheme with performance similar to existing less secure schemes, and that is conceptually simpler (and also more efficient) than previous forward private constructions. In particular, it only relies on trapdoor permutations and does not use an ORAM-like construction. We also explain why Sophos is an optimal point of the security/performance tradeoff for SSE.

After the development of practical searchable encryption construction, allowing for secure searches over an encrypted dataset outsourced to an untrusted server, at the expense of leaking some information to the server, new attacks have been developed, targeting this leakage in order to break the confidentiality of the dataset or of the queries, through leakage abuse attacks. These recent works helped to understand the importance of considering leakage when analyzing the security of searchable encryption schemes, but did not give an explanation either of why these attacks were so powerful despite the existence of rigorous security definitions and proofs, or how they could be mitigated. Our work addresses these questions by first proposing an analysis of existing leakage abuse attacks and a way to capture them in new security definitions. These new definitions also help us to devise a way to thwart these attacks and we apply it to the padding of datasets, so to hide the number of queries' results. Finally, we give experimental evidence that this approach is successful.

[BFP16] R. Bost, P. Fouque, D. Pointcheval, "Verifiable Dynamic Symmetric Searchable Encryption: Optimality and Forward Security", *2016*, p. 62, 2016.

[Bos16] R. Bost, "$\sum o\varphi o\varsigma$: Forward Secure Searchable Encryption", *in: ACM CCS*, p. 1143–1154, 2016.

4.7 Distance Bounding Protocols

Participants: Gildas Avoine, Cristina Onete.

Collaborations: TÜBİTAK BİLGEM (Turkey), University of Luxembourg, UQAM (Canada), ETS Montréal (Canada), Université Clermont Auvergne (France).

A *mafia fraud* is a man-in-the-middle attack applied against an authentication protocol where the adversary simply relays the exchanges without neither manipulating nor understanding them. The earliest version of this attack was introduced by Conway in 1976 and is known as the *chess grandmaster problem* (See Figure 1). In this problem, a little girl is able to compete with two chess grandmasters during a postal chess game, where she transparently relays the moves between the two grandmasters. She eventually wins a game or draws both. In modern cryptography, mafia frauds can typically be used against authentication protocols. The adversary relays the messages between the prover and the verifier, who think they communicate together, while there is an adversary in the middle. This so-called mafia fraud was actually suggested by Desmedt, Bengio and Goutier in 1987 to defeat the Fiat-Shamir protocol. Brands and Chaum proposed in 1994 a *distance-bounding protocol* that aims to thwart mafia fraud. The distance estimation relies on the measurement of the Round-Trip-Time (RTT) of single bit exchanges between the verifier and the prover. Considering the physical impossibility to travel faster than the speed of light, RTT bounds the distance between the parties. EMSEC designs distance bounding protocols that either benefit from a proof or improve existing ones in terms of performance[ABG+17,ABK+11].

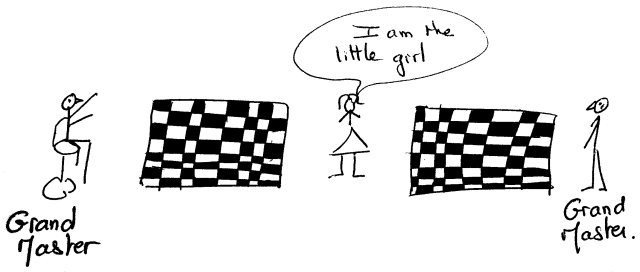


Figure 1: Chess Grand Master Problem

[ABG+17] G. Avoine, D. Bultel, S. Gambs, D. Gérault, P. Lafourcade, C. Onete, J.-M. Robert, "A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol", *in: Asia Conference on Computer and Communications Security – ASIACCS'17*, ACM, p. To Appear, Abu Dhabi, UAE, April 2017.

[ABK+11] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, B. Martin, "A Framework for Analyzing RFID Distance Bounding Protocols", *Journal of Computer Security – Special Issue on RFID System Security 19*, 2, March 2011, p. 289–317.

4.8 Security and Privacy of Communication Protocols

Participants: Stéphanie Delaune, Barbara Kordy.

Collaborations: LSV (Cachan, France), LORIA (Nancy, France).

One successful approach when designing and analyzing security protocols, is the use of formal symbolic methods. The purpose of formal verification is to provide rigorous frameworks and techniques to analyze protocols and find their flaws. For example, a flaw has been discovered in the Single-Sign-On protocol used *e.g.* by Google Apps. It has been shown that a malicious application could very easily get access to any other application (*e.g.* Gmail or Google Calendar) of their users [ACC+08]. Another example is a flaw on vote-privacy discovered during the formal and manual analysis of an electronic voting protocol [CS13]. All these results have been obtained using *formal symbolic models*, where most of the cryptographic details are ignored using abstract structures, and the communication network is assumed to be entirely controlled by an omniscient attacker. The techniques used in symbolic models have become mature and several tools for protocol verification are nowadays available, *e.g.* Avantssar platform [A+12], ProVerif tool [Bla01].

The complexity of the verification problem comes from the protocols themselves, as well as the need to clearly state the intended protocol goals and characterize the environment and the attacker capabilities. EMSEC contributes to this area of research in several ways, e.g. designing algorithms and automatic verification tools for analyzing privacy-type properties (e.g. unlinkability, anonymity) [HD16]; designing conditions to allow a modular approach for formal verification. These results are applied to several case studies like e-passport, e-voting, and various RFID protocols.

[ACC+08] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, M. L. Tobarra, "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for Google apps", *in: Proc. 6th ACM Workshop on Formal Methods in Security Engineering (FMSE'08)*, ACM, p. 1–10, 2008.

[CS13] V. Cortier, B. Smyth, "Attacking and fixing Helios: An analysis of ballot secrecy", *Journal of Computer Security 21*, 1, 2013, p. 89–148.

[A+12] A. Armando *et al.*, "The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures", *in: Proc. 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'12), 7214*, Springer, p. 267–282, 2012.

[Bla01] B. Blanchet, "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules", *in: Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, IEEE Computer Society Press, p. 82–96, 2001.

[HD16] L. Hirschi, S. Delaune, "A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols", *Journal of Logical and Algebraic Methods in Programming*, 2016.

4.9 Identification of Crypto. Algorithms in Binaries

Participants: Pierre-Alain Fouque, Pierre Lestringant.

- CIFRE PhD with AMOSSYS
- Reverse engineering : identification of symmetric primitives and mode of operation
- Black-box Audit: Analysis using an execution trace

Software tools use cryptographic algorithms to secure their communications and to protect their internal data. However the algorithm choice, its implementation design and the generation methods of its input parameters may have dramatic consequences on the security of the data it was initially supposed to protect. Therefore to assess the security of a binary program involving cryptography, analysts need to check that none of these points will cause a system vulnerability. It implies, as a first step, to precisely identify and locate the cryptographic code in the binary program. Since binary analysis is a difficult and cumbersome task, it is interesting to devise a method to automatically retrieve cryptographic primitives and their parameters. In our ASIACCS 2015 paper [LGF15], we present a novel approach to automatically identify symmetric cryptographic algorithms and their parameters inside binary code. Our approach is static and based on DFG isomorphism. To cope with binary codes produced from different source codes and by different compilers and options, the DFG is normalized using code rewrite mechanisms. Our approach differs from previous works, that either use statistical criteria leading to imprecise results, or rely on heavy dynamic instrumentation. To validate our approach, we present experimental results on a set of synthetic samples including several cryptographic algorithms, binary code of well-known cryptographic libraries and reference source implementation compiled using different compilers and options.

Later at ACNS 2016 [LGF16], we try to recover more information about the operating mode that has been used. Indeed, this allows us to recover MAC function such as HMAC, CTR, CBC encryption schemes and Authenticated Encryption schemes. With our method, we are also able to detect if the key is used to derive initialization vector and is used as a key in the cipher, which is a classical technique to do mass surveillance attacks. We have also been able to recover pseudo random generators that use many calls to some hash functions, that is the case in the Linux RNG, and to automatically recover the key derivation process used in the Telegram applications. Since the source code is publicly available, we have been able to verify that our method is correct. Finally, we have compared our method with other techniques and confirm that we are always more precise, very efficient and resistant to some classical obfuscation techniques.

[LGF15] P. Lestringant, F. Guihéry, P. Fouque, "Automated Identification of Cryptographic Primitives in Binary Code with Data Flow Graph Isomorphism", *in: ASIA CCS*, p. 203–214, 2015.

[LGF16] P. Lestringant, F. Guihéry, P. Fouque, "Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing", *in: ACNS*, p. 561–579, 2016.

4.10 Side Channel Attacks

Participants: Pierre-Alain Fouque, Benoit Gérard (DGA.MI & IRISA), Anélie Heuser (Tamis), Mehdi Tibouchi (NTT), Sonia Belaïd (Thales), Gilles Barthe (IMDEA) and Benjamin Grégoire (Inria Sophia-Antipolis).

- Side-Channel (EMA / Fault) on cryptographic implementations (symmetric / Lattice)
- Cryptographic Hardware Embedded Systems (CHES)

We work with the DGA.MI on this subject in order to propose new attacks on symmetric and Lattice-based cryptosystems. Benoît works with us every Wednesday and he is also one of the responsible for the electronic security seminar on the Friday. We are currently working for acquiring a new platform in order to test our attacks at IRISA using the CPER. An Inria engineer will work with us to mount the platform. Finally, we are collaborated with Anélie Heuser from Tamis in this subject. With Mehdi Tibouchi we work on the algorithmic ideas.

We have proposed many attacks since Benoît joined us in 2014. At Asiacrypt 2014, we work on a new kind of attacks against AES-GCM and on ECDSA with specific morphisms. Then, we improve our attack on AES at CHES 2016 using a new observation. At ASIACCS 2016, we also present a fault attack on pairing implementations [FQ16].

We also work on some countermeasures with Sonia Belaïd (a PhD student of Pierre-Alain, graduated in 2015, won in 2016 the Thales price and the best research engineer price in Usine Nouvelle), Gilles Barthe and Benjamin Grégoire. We propose a compiler that allows to securely mask any software implementations. These works have been accepted to Eurocrypt 2015 [BBD+15] and ACM CCS 2016 [BBD+16] . At ACM CCS 2014 [BDF+14], we also propose a tool to detect fault attacks on RSA and DLog based signature scheme. Finally, we also propose some security proof for RSA-CRT at CHES 2014. CHES is the flagship conference in side-channel research area and ACM CCS is one of the most three important conferences in security.

More recently, we work with Mehdi Tibouchi on the security of Lattice-based signature scheme. We propose many fault attacks on every signature schemes proposed that use only one fault [EFGT16]. We also extend these attacks to key exchange protocol and we describe a side-channel attack on the BLISS signature scheme, which is as efficient as the RSA signature scheme using advanced number theory tools.

[FQ16] P. Fouque, C. Qian, "Fault Attacks on Efficient Pairing Implementations", *in: ASIACCS*, p. 641–650, 2016.

[BBD+15] G. Barthe, S. Belaïd, F. Dupressoir, P. Fouque, B. Grégoire, P. Strub, "Verified Proofs of Higher-Order Masking", *in: EUROCRYPT*, p. 457–485, 2015.

[BBD+16] G. Barthe, S. Belaïd, F. Dupressoir, P. Fouque, B. Grégoire, P. Strub, R. Zucchini, "Strong Non-Interference and Type-Directed Higher-Order Masking", *in: ACM CCS*, p. 116–129, 2016.

[BDF+14] G. Barthe, F. Dupressoir, P. Fouque, B. Grégoire, J. Zapalowicz, "Synthesis of Fault Attacks on Cryptographic Implementations", *in: ACM CCS*, p. 1016–1027, 2014.

[EFGT16] T. Espitau, P. Fouque, B. Gérard, M. Tibouchi, "Loop abort Faults on Lattice-Based Fiat-Shamir & Hash'n Sign signatures", *2016*, p. 449, 2016.

4.11 Forensics for Smartcards

Participants: Gildas Avoine, Thomas Gougeon.

Collaborations: ENSICAEN (France).

Smart cards usually gather and store personal data, possibly related to the behavior of their holder. They are typically low-cost devices including (but not limited to) credit cards, mass transportation passes, electronic passports, keyless entry and start systems, and ski passes. In most cases, the personal data contained in these devices are accessible without requiring any authentication. For example, the Mobib card contains sensitive data, including holder's name, zip code, and native language. Interpreting the meaning of the captured data is difficult and time-consuming when neither the data structure nor the data encoding are known, particularly if the number of devices is large. So far, it does not exist any adapted method to automatically retrieve information stored in these devices, whereas there is really a need for a generic method investigating these devices. This kind of investigation is involved in several scenarios: (i) to establish digital evidence in connection with criminal investigations, (ii) to retrieve information about a missing person, or (iii) to verify whether a system complies with the claims of manufacturer or authority. EMSEC aims to develop automatic methods based on machine learning techniques to retrieve text, dates, and cryptographic material [GBL+16] in memory dumps where neither the data structure nor the data encoding are known (see Figure 2).

```
00 00 00 00 00 00 00 04 00 71 B3 00 00 00 00 00 01 B8 B2 4A 02 50 00 33 01 1A 13 43 00
04 00 98 E5 94 C8 02 0D 60 C9 65 C7 D5 90 00 00 00 00 00 00 00 00 19 75 07 10 92 82 D2 CF
F3 6A 68 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08 38 2B 00 08 BD 59 2A 46 60 C4 81 98 E5 94 C8 02 0D 60 C9 65 C6 41 F4 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09 0E E5 92 04 20 60 86 60 00 00 00 00 1C D6 DD 56 40 00 01 C0 00 00 51 08 66 E0 00 00
09 0E E5 7A 04 20 60 86 60 00 00 00 00 1C D6 DD 56 40 00 01 80 00 00 11 08 66 E0 00 00
09 0E E5 5A 04 20 60 86 60 00 00 00 00 1C D6 DD 56 40 00 01 40 00 00 91 08 66 E0 00 00
11 2B 40 01 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Figure 2: Example of Memory Dump

[GBL+16] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Memory carving in embedded devices: separate the wheat from the chaff", *in: Applied Cryptography and Network Security – 14th International Conference – ACNS*, M. Manulis, A. Sadeghi, S. Schneider (editors), *LNCS*, *9696*, Springer-Verlag, p. 592–608, Guildford, UK, June 2016.

4.12 Intrusion Detection with Data Mining Techniques

Participants: Pierre-Alain Fouque, Alban Siffer, Alexandre Termier (IRISA/Lacodam).

- CIFRE PhD with AMOSSYS
- Intrusion Detection by analyzing millions of IP headers
- Machine Learning and Big Data for detecting APT (Advanced Persistent Threats : rare events)

Amossys proposes us to work on this subject with Alexandre Termier and we initiate a new research work. This is very interesting since Machine Learning and Data Mining are very exciting algorithms and DGA.MI will invest a large amount of funds in these tools.

Intrusion detection is a well-known difficult problem in security and signature-based or behavioral approaches have been used with various success rate. The challenge is to detect APT which are very efficient attacks that are not detected using signature based approach since they are not known today. Furthermore, the information flows are now encrypted using TLS, in two years all internet traffic will be encrypted, and we cannot use plaintext method that relies on reading the payload. We consequently only look at the information coming from the headers of the TCP/IP packets.

We have propose a new algorithm to detect SYN flooding attack in a network using a new algorithm that detect rare events. We use extreme value theory to detect a drift in the distribution function independently of the original function and detect rare event. This statistical tool is well suited for our problem when one dimensional problem is used. This theory uses a quite of law of large numbers for the max function instead of the average function: independently of the initial distribution, the law of rare event follows a distribution that depends on only one parameter. If we can evaluate this parameter, we can predict the values of the max function. We propose a streaming algorithm in this context that works for univariate distribution. Currently, we are trying to adapt it to multivariate distribution since usually attacks can be detected using 2 or 3-dimensional distributions.

4.13 Browser Fingerprinting

Participants: Gildas Avoine, Pierre Laperdrix, Benoît Baudry (IRISA/DIVERSE).

Browser fingerprinting has emerged in the past few years as a strong alternative to cookie-based tracking: the collection of device-specific attributes through the browser, allows one to build a signature, which uniquely identifies a device. Yet, very few works have explored the use of browser fingerprinting for authentication and none of them have tried to quantify the provided protection. The main challenge for authentication is that most collected attributes of a browser are static (e.g., they are constant and do not depend on any input) and they can easily be modified and replayed, opening the door to attackers impersonating other devices. The key insight of this work is that canvas fingerprinting can be used for challenge/response-based authentication. EMSEC investigates this approach to strengthen the security of multifactor authentication schemes. To address this question, Pierre Laperdrix launched a website to gather browser fingerprints, known as `www.amiunique.org`, which is illustrated in Figure 3.

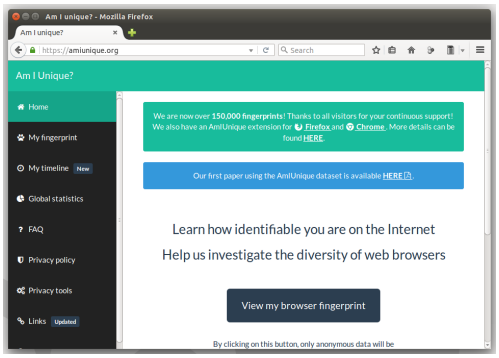


Figure 3: Am I unique?

4.14 Security Modeling with Attack–Defense Trees

Participants: Barbara Kordy, Wojciech Wideł.

An *attack–defense tree* (ADTree) is an AND-OR tree representing how an attacker may compromise a system and how a defender can defend it against potential attacks. Nodes of ADTrees are labeled with (collections of) actions that the attacker and the defender need to perform in order to reach their goals. ADTrees extend the industrially recognized model of attack trees with nodes representing countermeasures. Classical attack trees, however, take only attacker's actions into account. This makes them unsuitable to reason about the impact of the countermeasures that could be deployed. In contrast, ADTrees explicitly model possible countermeasures and potential counterattacks against these countermeasures, as illustrated in Figure 4. One can thus quantify the effect of deploying a countermeasure, analyze its consequences, and thus study the security of a system or infrastructure already during its design phase (security by design).

We develop mathematical foundations (semantics) for ADTrees [KMRS14], algorithms for their quantitative analysis [KMS16], as well as tools for their automated handling and management [KPY16]. Our current research directions focus on extending the ADTree formalism with additional modeling features allowing to better capture real-life aspects important for security analysis. This includes ADTrees with dependent nodes, ADTrees with repeated labels, ADTrees distinguishing between preventive and reactive countermeasures.

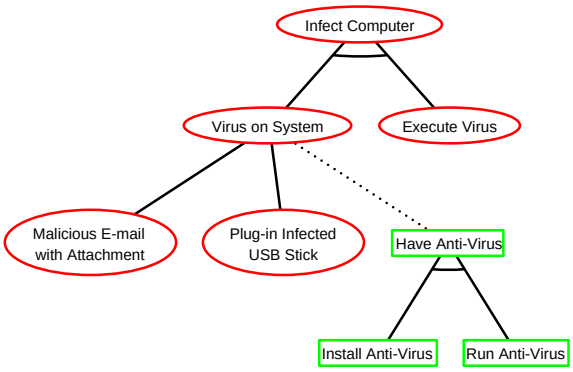


Figure 4: Attack–defense tree for infecting a computer

Barbara Kordy is the initiator and one of the main organizers of the *International Workshop on Graphical Models for Security* GraMSec http://www.gramsec.uni.lu/. GraMSec is the first initiative to bring researchers from various graphical security modeling domains together. By involving scientists as well as R&D experts from industry and government, the workshop bridges the gap between formal foundations and practical requirements which both need to be addressed in order to develop sound and usable solutions for security analysis and risk assessment. GraMSec has been a satellite event of the *Computer Security Foundations Symposium* CSF, since 2015.

[KMRS14] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, "Attack–Defense Trees", *Journal of Logic and Computation 24*, 1, 2014, p. 55–87.

[KMS16] B. Kordy, P. Marc, P. Schweitzer, "Probabilistic reasoning with graphical security models", *Information Sciences 342*, May 2016, p. 111–131, https://hal.inria.fr/hal-01289186.

[KPY16] B. Kordy, K. Piotr, v. d. B. Yoann, "SPTool - Equivalence Checker for SAND Attack Trees", *in: Risks and Security of Internet and Systems - 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers, Risks and Security of Internet and Systems - 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers, LNCS*, 10158, Springer , p. 105–113, Roscoff, France, September 2016, https://hal.inria.fr/hal-01483163.

5 Contracts and Grants with Industry

5.1 Phd thesis in collaboration with Orange Labs Caen

Participants: Gildas Avoine, Loïc Ferreira, Sébastien Carnard (Orange Labs).

The objective of this collaborative work is to analyze and design lightweight cryptographic primitives and protocols for the Internet of Things. In particular, we aim to design a protocol to allow two connected parties to establish secure channels, typically between a server and a smartcard. Such a channel should take the capacities into account, in terms of computation, communication, and storage. At this stage, we analyze existing solutions, and we submited to a conference an attack against the protocol Lorawan 1.0.

5.2 Phd thesis in collaboration with Orange Labs Châtillon

Participants: Pierre-alain Fouque, Benjamin Richard, Gilles Macario-Rat.

The objective of this collaboration work is to analyze the security of the authenticated Key Agreement (AKA) protocol used in the 3GPP mobile communication. In particular, we analyze the security of this protocol in the presence of a malicious intermediate server in the case of roaming. Then, we propose a new protocol which provides more privacy for the users in the presence of IMSI-catchers.

5.3 Phd theses in collaboration with Amossys

Participants: Pierre-alain Fouque, Pierre Lestringant, Alban Siffer, Frédéric Guihéry, Alexandre Termier.

The objective of this collaboration work has been with Pierre to study the security of binaries. The work of Amossys consists in analyzing the security of softwares. Sometimes, the analysts have the specifications but they are incomplete and analysts have to perform reverse engineer in order to understand which algorithms have been used. We have provide some automatic tools that allow the analysts to recover as much information as we can. Using Pin Tools we can instrument binaries and recover some cipher and more general protocol and modes of operations.

With Alban Siffer and Alexandre Termier we study Data Mining technique in order to detect some attacks since october 2016. Currently, we have provide a technique to detect SYN floading attack.

5.4 Phd theses in collaboration with DGA-MI

Participants: Pierre-alain Fouque, Raphaël Bost, Benoît Gérard and Victor Cauchois.

I co-supervise the PhD thesis of Raphaël Bost with David Pointcheval on Cloud security. We have propose to add integrity of the Symmetric Searchable Encryption schemes. Since many attacks have been recently propose on provable schemes, we have tried to understand what was wrong in the security model. We understand some mistakes and we propose to fix

the definition and prove the security of some scheme. More recently, we work on more active adversaries.

With Benoît Gérard, I work on side-channel attacks. Currently, we are working on some attack against lattice-based signature schemes.

With Victor Cauchois and Patrick Derbez we initiated a new research work on the security of the SHA-3 hash function.

6 Other Grants and Activities

6.1 International Collaborations

- COST Action Cryptacus

  Gildas Avoine is the Chair of the Management Committee of the COST Action IC1403 Cryptacus. A COST Action is a 4-year H2020 networking project. Cryptacus was launched in December 2014 and it will consequently end in December 2018.

  Topic: Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these no longer consist only of connected servers, but involve a wide range of pervasive and embedded devices, leading to the concept of "ubiquitous computing systems". The objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems.

- ERC POPSTAR

  Stéphanie Delaune is the PI of the ERC POPSTAR (starting grant). This is 5-year project. POPSTAR was launched in February 2017, and it will consequently end in January 2022. Budget: 1,499,750 euros.

  Topic: Whereas traditional security protocols achieve their security goals relying solely on cryptographic primitives like encryptions and hash functions, the protocols employed to secure contactless devices establish and rely in addition on properties of the physical world. For instance, they may use, as basic building blocks, protocols for ensuring physical proximity, secure localization, or secure neighborhood discovery.

  The main objective of the POPSTAR project is to develop foundations and practical tools to analyze modern security protocols that establish and rely on physical properties. The POPSTAR project will significantly advance the use of formal verification to contribute to the security analysis of protocols that rely on physical properties. This project is bold and ambitious, and answers the forthcoming expectation from consumers and citizens for high level of trust and confidence about contactless nomadic devices.

- Researchers who visited EMSEC.

  - Ioana Boureanu, Imperial College London, (24-29 April 2016)
  - Mehdi Tibouchi, NTT, June 2016
  - Sasa Radomirović, ETH Zurich (2-6 May 2016)
  - Rolando Trujillo, University of Luxembourg (9-20 May 2016)
  - Martin Albrecht, Royal Holloway (4-7 Oct. 2016)
  - Zhi Guan, Mannheim University, Germany (13-17 Sep. 2016) (19-21 Dec. 2016)

- EMSEC's members who visited another laboratory.
  - In September 2016, Pierre-Alain visited Dagstuhl for seminar 16371 *Public-Key Cryptography*.
  - In November, Barbara Kordy participated in the Dagstuhl seminar 16461 *Assessing ICT Security Risks in Socio-Technical Systems*
  - In December 2015, Adeline Roux-Langlois visited Steven Galbraith in University of Auckland, New Zealand and Ron Steinfeld in Monash University, Australia.

6.2 National Collaborations

- ANR Brutus. The goal of this ANR project is to study Authenticated Encryption (AE), side-channel attack of AE scheme and white-box implementation of block ciphers. We follow the CAESAR international competition with our partners in Inria Paris, Inria Sophia-Antipolis, Université Versailles-Saint-Quentin-en-Yvelines, Université Lille 1, ANSSI and Orange Labs. We broke many schemes in white-box implementations and AE schemes.

- ANR SafeTLS. The goal of this ANR project is to study the security of the new TLS 1.3 protocol that will be released in April 2017. We look at the security in various case studies such as Keyless SSL, MC-TLS, reverse-firewall and the security of implementations with our partners in Inria Sophia-Antipolis, Inria Paris, ANSSI, INSA. Indeed, since all internet communications will be encrypted in 2/3 years, new functionalities have to be designed or taken into account with TLS.

- Projet BPI - Grands défis du numérique. The goal of this project is to regroup the french laboratories and companies to develop post-quantum cryptography and cyber-security. Lead by the ANSSI, this project is with many collaborators: CEA, ENS Paris, Inria Paris, Inria Rhones Alpes, Paris Centre for Quantum Computing, University Versailles Saint-Quentin-en-Yvelines, and Airbus Group, Cryptoexperts, CS Communications et Systèmes, Gemalto, Orange, Secure-IC S.A.S and Thales Communications and Security.

7 Dissemination

7.1 Scientific Responsabilities

- Gildas Avoine was in 2016 a member of the PhD committees of Amira Barki (reviewer), Amrit Kumar (reviewer), and Cédric Marchand (president). He is the director of the CNRS' GDR (research groupment) in computer security, the chair of the COST Action IC1403 (Cryptacus), a member of the steering committee of the "Défi 9" of the ANR (French funding agency). In 2016, Gildas Avoine was also a member of evaluation committees for the Research Grant Council of Hong-Kong and the Seoul National University.
- Pierre-Alain Fouque was in 2016 a reviewer for the HDR thesis of Hoeteck Wee (ENS), President of the HDR committee of Ludovic Perret (Paris 6), reviewer for HDR of Guénaël Renault (Paris 6), reviewer of the PhD of Houda Ferradi (ENS), President for the PhD committee of Alain Passelègue (ENS) and Mario Cornejo (ENS), member of the PhD committee of Chrysanthi Mavromati (Paris 6), member of the PhD committee of Brice Minaud (UR1), Pierre Karpman (EDX), Benoît Cogliati (UVSQ), Virginie Lallemand (Paris 6). He is also member of the CFRG (Cryptographic Research Group of the IRTF). He is PI for the 2 ANR Projects (BRUTUS and SafeTLS). He was member of the PC of PKC and Crypto 2016. He is a member of the board of the crypto seminar at IRMAR and the responsible for the transverse axis "Security" at IRISA.
- Patrick Derbez was in 2016 a member of the program committee of ToSC 2016 and actively work for the BRUTUS ANR Project.
- In 2016, Barbara Kordy was the genral chair of the GraMSec'16 workshop (http://gramsec.uni.lu/2016/), PC member of the CRiSIS'16 conference (https://conferences.telecom-bretagne.eu/crisis/2016/), and a member of the selection committee for an assistant professor (MCF) position at the Université de Technologie of Troyes.
- Stéphanie Delaune joined the team in September 2016. She is member of the ANR Sequoia (2014-2019), and PI of the ERC POPSTAR (2017-2022). She is also member of the IFIP WG-1.7 Foundations of Security Analysis since 2016.

7.2 Involvement in the Scientific Community

- The EMSEC team is co-chairing the *Software and Systems Security seminar* SoSySec (http://seminaire-dga.gforge.inria.fr/) organized jointly by DGA-MI and INRIA. In 2016, Barbara Kordy has been the main organizer and co-chair of SoSySec.
- The EMSEC team is co-chairing the seminar *Security of Embedded Electronic Systems* (http://securite-elec.irisa.fr/) organized jointly by DGA-MI and IRISA. In 2016, Benoît Gérard has been one of the main organizers of this seminar.
- The EMSEC team is co-chairing the *Cryptography* seminar (https://webmath.univ-rennes1.fr/crypto/) organized jointly by DGA-MI and IRMAR. In 2016, Adeline Roux-Langlois has been one of the main organizers of this seminar.

7.3 Teaching

- Gildas Avoine is in charge of the 10-hour course “Network Security” (4th-year students) and the 26-hour course “Cryptographic Engineering” (4th-year students) both at INSA Rennes. He also teaches “Advanced Security” at the UCL Belgium.
- Patrick Derbez is in charge of a 32-hour course on "Security Challenges" in M2 based on Root-Me, responsible for the course on Network Security in M2, TA for the course in Cryptography and in Programming Language with Java for bachelor students.
- Pierre-Alain Fouque is responsible for the Master "Sécurité des Systèmes d'Information" at Rennes 1 University where 15 students are graduated each year. He is also in charge of the Introduction to Security course in M1 and of the cryptographic course in M2.
- Barbara Kordy is in charge of the 26-hour course “Functional programming” (3rd-year students), the 26-hour course “Introduction to security” (3rd-year students), the 32-hour course “Languages and grammars” (4th-year students), and the 24-hour course “Security” (5th-year students) at INSA Rennes.
- Adeline Roux-Langlois gave in 2016 a 24-hour course "Introduction to cryptography" in L3 at ENS Rennes.

7.4 Science popularization

- In January 2016, Patrick Derbez and Adeline Roux-Langlois introduced research in cryptography to high school students, at IRISA. Adeline Roux-Langlois also supervised a 3-day internship of an high school student.
- In October 2016, Adeline Roux-Langlois introduced cryptography to elementary school teachers during the "Graine de sciences" week organized by the foundation *La main à la pâte*.

8 Bibliography

Major publications by the team in recent years

[1] G. Avoine, D. Bultel, S. Gambs, D. Gérault, P. Lafourcade, C. Onete, J.-M. Robert, "A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol", *in: Asia Conference on Computer and Communications Security – ASIACCS'17*, ACM, p. To Appear, Abu Dhabi, UAE, April 2017.

[2] G. Avoine, X. Carpent, C. Lauradoux, "Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform Distributions", *in: European Symposium on Research in Computer Security – ESORICS*, G. Pernul, P. Y. A. Ryan, E. R. Weippl (editors), *Lecture Notes in Computer Science, 9326*, Springer-Verlag, p. 165–184, Vienna, Austria, September 2015.

[3] G. Avoine, X. Carpent, "Heterogeneous Rainbow Table Widths Provide Faster Cryptanalyses", *in: Asia Conference on Computer and Communications Security – ASIACCS'17*, ACM, p. To Appear, Abu Dhabi, UAE, April 2017.

[4] S. Bai, A. Langlois, T. Lepoint, D. Stehlé, R. Steinfeld, "Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance", *in: ASIACRYPT*, 2015.

[5] G. Barthe, S. Belaïd, F. Dupressoir, P. Fouque, B. Grégoire, P. Strub, R. Zucchini, "Strong Non-Interference and Type-Directed Higher-Order Masking", *in: ACM CCS*, p. 116–129, 2016.

[6] R. Bost, "$\sum o\varphi o\varsigma$: Forward Secure Searchable Encryption", *in: ACM CCS*, p. 1143–1154, 2016.

[7] J. H. Cheon, P. Fouque, C. Lee, B. Minaud, H. Ryu, "Cryptanalysis of the New CLT Multilinear Map over the Integers", *in: EUROCRYPT*, p. 509–536, 2016.

[8] P. Derbez, P. Fouque, "Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks", *in: CRYPTO*, p. 157–184, 2016.

[9] P. Kirchner, P. Fouque, "An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices", *in: CRYPTO*, p. 43–62, 2015.

[10] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, "Attack–Defense Trees", *Journal of Logic and Computation 24*, 1, 2014, p. 55–87.

[11] B. Kordy, L. Piètre-Cambacédès, P. Schweitzer, "DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees", *Computer Science Review 13–14*, 0, 2014, p. 1–38.

[12] B. Minaud, P. Derbez, P. Fouque, P. Karpman, "Key-Recovery Attacks on ASASA", *in: ASIACRYPT*, p. 3–27, 2015.

Books and Monographs

[1] B. Kordy, M. Ekstedt, D. S. Kim (editors), *Graphical Models for Security*, *Graphical Models for Security*, *LNCS*, 9987, Barbara Kordy and Mathias Ekstedt and Dong Seong Kim, Lisbon, Portugal, Springer International Publishing, September 2016, `https://hal.inria.fr/hal-01365806`.

[2] S. Mauw, B. Kordy, S. Jajodia (editors), *Graphical Models for Security*, *Graphical Models for Security*, *LNCS*, 9390, Sjouke Mauw and Barbara Kordy and Sushil Jajodia, Verona, Italy, Springer, February 2016, `https://hal.inria.fr/hal-01289203`.

Articles in referred journals and book chapters

[3] M. Abdalla, P. Fouque, V. Lyubashevsky, M. Tibouchi, "Tightly Secure Signatures From Lossy Identification Schemes", *J. Cryptology 29*, 3, 2016, p. 597–631.

[4] E. Andreeva, C. Bouillaguet, O. Dunkelman, P. Fouque, J. J. Hoch, J. Kelsey, A. Shamir, S. Zimmer, "New Second-Preimage Attacks on Hash Functions", *J. Cryptology 29*, 4, 2016, p. 657–696.

[5] G. Avoine, A. Beaujeant, J. Hernandez-Castro, L. Demay, P. Teuwen, "A Survey of Security and Privacy Issues in the ePassports Protocols", *ACM Computing Surveys 48*, 3, February 2016, p. 1–47.

[6] G. Avoine, X. Carpent, J. Hernandez-Castro, "Pitfalls in Ultralightweight Authentication Protocol Designs", *IEEE Transactions on Mobile Computing 15*, 9, September 2016, p. 2317–2332.

[7] P. Fouque, C. Onete, B. Richard, "Achieving Better Privacy for the 3GPP AKA Protocol", *PoPETs 2016*, 4, 2016, p. 255–275.

[8] B. Kordy, P. Marc, P. Schweitzer, "Probabilistic reasoning with graphical security models", *Information Sciences 342*, May 2016, p. 111–131, `https://hal.inria.fr/hal-01289186`.

Publications in Conferences and Workshops

[9] M. R. Albrecht, C. Cocis, F. Laguillaumie, A. Langlois, "Implementing Candidate Graded Encoding Schemes from Ideal Lattices", *in : ASIACRYPT, Part II*, p. 752–775, 2015.

[10] S. Alt, P. Fouque, G. Macario-Rat, C. Onete, B. Richard, "A Cryptographic Analysis of UMTS/LTE AKA", *in : ACNS*, p. 18–35, 2016.

[11] G. Barthe, S. Belaïd, F. Dupressoir, P. Fouque, B. Grégoire, P. Strub, "Verified Proofs of Higher-Order Masking", *in : EUROCRYPT*, p. 457–485, 2015.

[12] G. Barthe, F. Dupressoir, P. Fouque, B. Grégoire, J. Zapalowicz, "Synthesis of Fault Attacks on Cryptographic Implementations", *in : ACM CCS*, p. 1016–1027, 2014.

[13] R. Bost, P. Fouque, D. Pointcheval, "Verifiable Dynamic Symmetric Searchable Encryption: Optimality and Forward Security", *2016*, p. 62, 2016.

[14] X. Bultel, S. Gambs, D. Gérault, P. Lafourcade, C. Onete, J.-M. Robert, "A Prover-Anonymous and Terrorist-Fraud Resistant Distance-Bounding Protocol", *in : Security & Privacy in Wireless and Mobile Networks (WiSec), Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ACM, p. 121–133, Darmstadt, Germany, July 2016.

[15] J. H. Cheon, P. Fouque, C. Lee, B. Minaud, H. Ryu, "Cryptanalysis of the New CLT Multilinear Map over the Integers", *in : EUROCRYPT*, p. 509–536, 2016.

[16] P. Derbez, "Note on Impossible Differential Attacks", *in : FSE*, p. 416–427, 2016.

[17] T. Espitau, P. Fouque, B. Gérard, M. Tibouchi, "Loop abort Faults on Lattice-Based Fiat-Shamir & Hash'n Sign signatures", *2016*, p. 449, 2016.

[18] P. Fouque, B. Hadjibeyli, P. Kirchner, "Homomorphic Evaluation of Lattice-Based Symmetric Encryption Schemes", *in : COCOON*, p. 269–280, 2016.

[19] P. Fouque, P. Karpman, P. Kirchner, B. Minaud, "Efficient and Provable White-Box Primitives", *in : ASIACRYPT*, p. 159–188, 2016.

[20] P. Fouque, M. S. Lee, T. Lepoint, M. Tibouchi, "Cryptanalysis of the Co-ACD Assumption", *in : CRYPTO*, p. 561–580, 2015.

[21] P. Fouque, C. Qian, "Fault Attacks on Efficient Pairing Implementations", *in : ASIACCS*, p. 641–650, 2016.

[22] T. Gougeon, M. Barbier, P. Lacharme, G. Avoine, C. Rosenberger, "Memory carving in embedded devices: separate the wheat from the chaff", *in : Applied Cryptography and Network Security – 14th International Conference – ACNS*, M. Manulis, A. Sadeghi, S. Schneider (editors), *LNCS*, *9696*, Springer-Verlag, p. 592–608, Guildford, UK, June 2016.

[23] B. Kordy, K. Piotr, v. d. B. Yoann, "SPTool - Equivalence Checker for SAND Attack Trees", *in : Risks and Security of Internet and Systems - 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers*, *Risks and Security of Internet and Systems - 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers*, *LNCS*, 10158, Springer , p. 105–113, Roscoff, France, September 2016, `https://hal.inria.fr/hal-01483163`.

[24] P. Lestringant, F. Guihéry, P. Fouque, "Automated Identification of Cryptographic Primitives in Binary Code with Data Flow Graph Isomorphism", *in : ASIA CCS*, p. 203–214, 2015.

[25] P. Lestringant, F. Guihéry, P. Fouque, "Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing", *in : ACNS*, p. 561–579, 2016.