Activity Report 2013

Team CRYPT

Cryptanalysis

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Team CRYPT

Keywords: Security, Cryptography, Algorithmic Number Theory, Computer Algebra, Complexity

CRYPT is one of the projects of the LIAMA consortium [1]. It is joint between Inria, Tsinghua University and the Academy of Mathematics and System Sciences from the Chinese Academy of Sciences, and located at Tsinghua University, Beijing, China.

Creation of the Team: 2012 July 01.

1. Members

Research Scientist

Phong-Quang Nguyen [Team leader, Inria, Senior Researcher, HdR]

Faculty Members

Xiaoyun Wang [Tsinghua, Professor, HdR]
Yingpu Deng [CAS, Professor, HdR]
Yanbin Pan [CAS, Associate professor]
Hongbo Yu [Tsinghua, Associate professor]
Keting Jia [Tsinghua, Associate professor]

PhD Students

Yuanmi Chen [ENS, PhD student]
Wei Wei [Tsinghua, PhD student]
Dan Ding [Tsinghua, PhD student]
Jianwei Li [Tsinghua, PhD student]
Dianyan Xiao [Tsinghua, PhD student]
Jiayang Liu [Tsinghua, PhD student]
Yang Yu [Tsinghua, PhD student]
Feng Zhang [CAS, PhD student]
Gengran Hu [CAS, PhD student]
Chang Lv [CAS, PhD student]
Renzhang Liu [CAS, PhD student]
Dandan Huang [CAS, PhD student]

Post-Doctoral Fellow

Jingguo Bi [Tsinghua, Post-Doctoral Fellow]

Administrative Assistants

Mei Zhang [LIAMA]
Qi Shi [Tsinghua]

[1] http://liama.ia.ac.cn

2. Overall Objectives

2.1. Presentation

The focus of this project is cryptanalysis, which is traditionally defined as the art of code-breaking: cryptanalysis studies the best attacks on cryptographic schemes, from a theoretical point of view (algorithm design) but also from a practical of view (implementation weaknesses, side-channel attacks). Cryptanalysis has a significant impact in the real world, because cryptographic algorithms and protocols, as well as keysizes, are selected based on the state-of-the-art in cryptanalysis. While provable security has made great advances in the past thirty years, it is alone insufficient to select cryptographic parameters: in general, choosing parameters based purely on security proofs leads to rather inefficient schemes. Cryptanalysis is therefore complementary of provable security, and both are essential to our understanding of security.

We consider cryptanalysis in the two worlds of cryptography: public-key cryptography (also called asymmetric cryptography) and secret-key cryptography (also called symmetric cryptography). Secret-key cryptography is much more efficient (and therefore more widespread) than public-key cryptography, but also less powerful because it requires to share secret keys: it encompasses symmetric encryption (stream ciphers, block ciphers), message authentication codes, and hash functions. Public-key cryptography provides more functionalities such as digital signatures, identity-based encryption and more generally functional encryption. Current public-key cryptographic techniques are based on advanced mathematics such as number theory (*e.g.* elliptic curves and lattices).

Inside public-key cryptanalysis, we focus on lattice techniques in particular, because lattice-based cryptography has been attracting considerable interest in the past few years, due to unique features such as potential resistance to quantum computers and new functionalities such as fully-homomorphic encryption [33] (which allows to compute on encrypted data without requiring secret keys), noisy multi-linear maps [31] and even (indistinguishability) obfuscation [32]. These new functionalities have dramatically increased the popularity of lattice-based cryptography.

Inside secret-key cryptanalysis, we are especially interested in standard hash functions and the five SHA-3 finalists, due to the importance of the SHA-3 competition for a new hash function standard. We are also interested in the security of widespread symmetric ciphers, such as the AES block cipher standard (implemented in Intel processors) and the RC4 stream cipher (widely deployed in wireless protocols).

This project deals with both public-key cryptanalysis and secret-key cryptanalysis. Most of the researchers working in cryptanalysis only study one of the two, but there seems to be more and more interaction between the two fields, despite their apparent independence:

- For instance, coding theory techniques are now used in both secret-key cryptanalysis and public-key cryptanalysis: as an example, several standard hash functions implicitly use a linear code, and the properties of this code are related to the security of the hash function; and public-key cryptosystems based on coding theory problems have been studied for more than thirty years.
- Similarly, Groëbner bases and related techniques are now used in both secret-key cryptanalysis and public-key cryptanalysis: algebraic attacks on stream ciphers and block ciphers are now well-established, and there are still a few multivariate public-key cryptosystems, more than twenty years after the Matsumoto-Imai cryptosystem. Recently, techniques to solve systems of polynomial equations have been used in breakthrough results for solving the discrete logarithm problem over special finite fields and elliptic curves.
- As another example, time/memory tradeoffs are routinely used in both secret-key cryptanalysis and public-key cryptanalysis.

As a side objective, this project also aims at developing European-Chinese collaboration in cryptologic research.

2.2. State of the Art

Cryptanalysis has a long history, dating back to secret writing. Until the seventies, most of the work on cryptanalysis was kept secret, but it is has now evolved from art to science, thanks to the liberalization of cryptologic research. In general, cryptanalysis tries to answer the following question: what is the best attack against a given cryptosystem, and how much does it cost? There is generally no definite answer to this question, and the state-of-the-art regularly evolves over time. Cryptanalysis is a field mixing theory and practice: while more and more advanced techniques are used, one is also concerned with very applied issues such as hardware/software efficiency.

In the past fifteen years, a new kind of attacks have appeared in the research literature: side-channel attacks. Such attacks arguably existed long before 1996, but were not advertised in public research. In a side-channel attack, the attacker exploits physical information which can sometimes be obtained in a concrete implementation, such as the power consumption of the cryptographic device, or the running time of the cryptographic process, etc. The attack could be either passive or active: for instance, in a so-called fault attack, the attacker physically perturbates the cryptographic device, and depending on the type of perturbations, the faulty outputs may disclose valuable information which may leak the whole secret key. Side-channel attacks have had a huge impact in industry: many cryptographic certifications now require more or less strong resistance to side-channel attacks, and there is an annual international conference dedicated to side-channel attacks, namely the CHES conference organized by IACR.

Cryptanalysis is particularly important in secret-key cryptography, due to the lack of provable security techniques. In public-key cryptanalysis, studying the best attack often consists in answering the following two questions:

- What is the best algorithm to solve the computational problem (integer factoring, discrete logarithm, etc.) related to the security of the public-key cryptosystem? In particular, industry is very interested in a practical version of this question: which keysizes are recommended? How much computational effort would be required exactly to break a given keysize? This question is arguably well-understood for integer factoring and discrete logarithm: there is more or less a consensus on what is the security level provided by a given RSA modulus or ECC elliptic curve. But it is more difficult to answer for alternative (post-quantum) problems such as lattice reduction, solving systems of polynomial equations over finite fields, and coding theory problems. Traditionally, there are more parameters for these problems.
- Is there a short-cut to attack the public-key cryptosystem, rather than trying to solve the underlying computational problem stated by the designer(s)? This is especially relevant when the public-key cryptosystem does not have provable security guarantees. And this question is also related to side-channel attacks.

2.3. Highlights of the Year

Phong Nguyen and Xiaoyun Wang obtained a 973 grant from China's Ministry of Science and Technology (MOST): the so-called 973 grants are China's largest grants for fundamental research.
BEST PAPER AWARD :
[19] **Sub-linear root detection, and new hardness results, for sparse polynomials over finite fields in ISSAC '13 - 38th international symposium on International symposium on symbolic and algebraic computation**. J. BI, Q. CHENG, M. ROJAS.

3. Research Program

3.1. Public-Key Cryptanalysis

This project is interested in any public-key cryptanalysis, in the broad sense.

3.1.1. Mathematical Foundations

Historically, one useful side-effect of public-key cryptanalysis has been the introduction of advanced mathematical objects in cryptology, which were later used for cryptographic design. The most famous examples are elliptic curves (first introduced in cryptology to factor integer numbers), lattices (first introduced in cryptology to attack knapsack cryptosystems) and pairings over elliptic curves (first introduced in cryptology to attack the discrete logarithm problem over special elliptic curves). It is therefore interesting to develop the mathematics of public-key cryptanalysis. In particular, we would like to deepen our understanding of lattices by studying well-known mathematical aspects such as packing problems, transference theorems or random lattices.

3.1.2. Lattice Algorithms

Due to the strong interest surrounding lattice-based cryptography at the moment, our main focus is to attack lattice-based cryptosystems, particularly the most efficient ones (such as NTRU), and the ones providing new functionalities such as fully-homomorphic encryption or noisy multi-linear maps: recent cryptanalysis examples include [3], [4] for the latter, and [6] for the former. We want to assess the concrete security level of lattice-based cryptosystems, as has been done for cryptosystems based on integer factoring or discrete logarithms: this has been explored in [29], but needs to be developed. This requires to analyze and design the best algorithms for solving lattice problems, either exactly or approximately. In this area, much progress has been obtained the past few years (such as [30]), but we believe there is still more to come. We are working on new lattice computational records.

We are also interested in lattice-based cryptanalysis of non-lattice cryptosystems, by designing new attacks or improving old attacks. A well-known example is RSA for which the best attacks in certain settings are based on lattice techniques, following a seminal work by Coppersmith in 1996: recently [2], we improved the efficiency of some of these attacks on RSA, and we would like to extend this kind of results.

3.1.3. New Assumptions

In the past few years, new cryptographic functionalities (such as fully-homomorphic encryption, noisy multinear maps, indistinguishability obfuscation, etc.) have appeared, many of which being based on lattices. They usually introduce new algorithmic problems whose hardness is not well-understood. It is extremely important to study the hardness of these new assumptions, in order to evaluate the feasability of these new functionalities. Sometimes, the problem itself is not new, but the (aggressive) choices of parameters are: for instance, several implementations of fully-homorphic encryption used well-known lattice problems like LWE or BDD but with very large parameters which have not been studied much.

Currently, there are very few articles studying the concrete hardness of these new assumptions, especially compared to the articles using these new assumptions.

3.2. Secret-Key Cryptanalysis

Though secret-key cryptanalysis is the oldest form of cryptanalysis, there is regular progress in this area.

3.2.1. Hash Functions

In the past few years, the most important event has been the SHA-3 competition for a new hash function standard. This competition ended in 2012, with Keccak selected as the winner. We intend to study Keccak, together with the four other SHA-3 finalists (such as in [12]). New cryptanalytical techniques designed to attack SHA-3 candidates are likely to be useful to attack other schemes. For instance, this was the case for the so-called rebound attack.

However, it is also interesting not to forget widespread hash functions: while it is now extremely easy to generate new MD5 collisions, a collision for SHA-1 has yet to be found, despite the existence of theoretical collision attacks faster than birthday attacks. Besides, there are still very few results on the SHA-2 standards family.

We may also be interested in related topics such as message authentication codes, especially those based on hash functions, which we explored in the past.

3.2.2. Symmetric Ciphers

Symmetric ciphers are widely deployed because of their high performances: a typical case is disk encryption and wireless communications.

We intend to study widespread block ciphers, such as the AES (now implemented in Intel processors) and Kasumi (used in UMTS) standards, as illustrated in recent publications [7], [9], [10] of the team. Surprisingly, new attacks [28], [27] on the AES have appeared in the past few years, such as related-key attacks and single-key attacks. It is very important to find out if these attacks can be improved, even if they are very far from being practical. An interesting trend in block cipher cryptanalysis is to adapt recent attacks on hash functions: this is the reciprocal of the phenomenon of ten years ago, when Wang's MD5 collision attack was based on differential cryptanalysis.

Similarly to block ciphers, we intend to study widespread stream ciphers, such as RC4. The case of RC4 is particularly interesting due to the extreme simplicity of this cipher, and its deployment in numerous applications such as wireless Internet protocols. In the past few years, new attacks on RC4 based on various biases (such as [34]) have appeared, and several attacks on RC4 are used in WEP-attack tools.

4. Application Domains

4.1. Security Estimates for Cryptography

An important application of cryptanalysis is to evaluate the concrete security of a given cryptosystem, so that key sizes and parameters are chosen appropriately. In some sense, cryptanalysis is the crash test of cryptography. When one uses cryptography, the first thing that one does is to select parameters and key sizes: in the real world, several well-known cryptographic failures happened due to inappropriate key sizes. Cryptanalysis analyzes the best attacks known: it assesses their cost (depending on the platform) and their performances (such as success probability). Sometimes the exact cost of an attack cannot be evaluated accurately nor rigorously, but fortunately, it is often possible to give an order of magnitude, which allows to select key sizes with a reasonable security margin.

On the other hand, it must be stressed that cryptanalysis depends on the state of the art: today's best attack may be completely different from tomorrow's best attack. The case of MD5 is a good reminder of this well-known fact.

4.2. Algorithmic Number Theory

Algorithms developed for cryptanalysis have sometimes applications outside cryptanalysis, especially in algorithmic number theory. This has happened for lattices and elliptic curves, and is not surprising, considering that some of the problems studied by cryptanalysis are very basic (like integer factoring), and therefore ubiquitous. Cryptanalysis motivates the search of truly-efficient algorithms, and experiments are common in public-key cryptanalysis, which allows to really verify improvements.

5. Partnerships and Cooperations

5.1. National Initiatives

5.1.1. MOST's 973 Grant

Grant 2013CB834205
PIs Phong Nguyen and Xiaoyun Wang
Duration 2013-17

MOST is China's Ministry of Science and Technology.

5.1.2. NSFC Grant

Grant NSFC Key Project 61133013

PIs Phong Nguyen and Xiaoyun Wang

Duration 2013-16

NSFC is the National Natural Science Foundation of China.

5.2. European Initiatives

5.2.1. FP7 Projects

Phong Nguyen was leader of the Virtual Lab MAYA of FP7's ECRYPT-II Network of Excellence, which finished in 2013.

5.2.2. Collaborations with Major European Organizations

CWI: Ronald Cramer's crypto team (Netherlands). In December 2013, Cramer's crypto team officially became a partner of LIAMA's CRYPT international project: in particular, Marc Stevens expects to do joint work on the cryptanalysis of hash functions.

5.3. International Initiatives

5.3.1. Inria International Labs

- CRYPT is an international project from LIAMA in China, located at Tsinghua University in Beijing. It is a joint project between Inria, Tsinghua University and CAS Academy of Mathematics and System Sciences.
- Phong Nguyen is the new European director of LIAMA, since December 2013: previously, he was the scientific coordinator of LIAMA in 2013.

5.4. International Research Visitors

5.4.1. Visits of International Scientists

Shi Bai (Univ. of Auckland, New-Zealand)

Nicolas Gama (UVSQ and CNRS, France)

Ming-Deh Huang (Univ. Southern California, USA)

Gaëtan Leurent (UCL, Belgium)

Cheng Qi (Univ. Oklahoma, USA)

Marc Stevens (CWI, Netherlands)

Guangwu Xu (Univ. Wisconsin, USA)

6. Dissemination

6.1. Scientific Animation

6.1.1. Editorial Boards

- Advances in Mathematics of Communications: Xiaoyun Wang
- Journal of Cryptology: Phong Nguyen and Xiaoyun Wang
- Journal of Mathematical Cryptology: Phong Nguyen
- Natural Science Review: Xiaoyun Wang

6.1.2. Program Committees of International Conferences

- EUROCRYPT '13 - May, Athens, Greece: Phong Nguyen (Program co-chair)
- ASIACRYPT '13 - December, Bengaluru, India: Phong Nguyen and Xiaoyun Wang

6.2. Teaching - Supervision - Juries

6.2.1. Teaching

PhD: Phong Nguyen, Advanced Cryptanalysis and Lattice Algorithms, 12h, CAS, China

6.2.2. Supervision

PhD: Léo Ducas, Signatures fondées sur les réseaux euclidiens: attaques, analyses et optimisations, Univ. Paris 7, November 12th 2013, Phong Nguyen

PhD: Yuanmi Chen, Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe, Univ. Paris 7, November 13th 2013, Phong Nguyen

PhD: Aurore Guillevic, Étudie de l'arithmétique des couplages sur les courbes algébriques pour la cryptographie, ENS, December 20th 2013, Damien Vergnaud and Phong Nguyen

PhD: Yupeng Jiang, CAS, Summer 2013, Yingpu Deng

6.2.3. Juries

PhD: Léo Ducas, Signatures fondées sur les réseaux euclidiens: attaques, analyses et optimisations, Univ. Paris 7, November 12th 2013, Phong Nguyen (supervisor)

PhD: Yuanmi Chen, Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe, Univ. Paris 7, November 13th 2013, Phong Nguyen (supervisor)

6.3. Popularization

Phong Nguyen gave several invited talks:

- [17] at the Workshop on Number Theory, Geometry and Cryptography in UK.
- [16] at the Workshop on Algebraic Aspects of Cryptography in Japan.

7. Bibliography

Major publications by the team in recent years

[1] J. BI, Q. CHENG, M. ROJAS. *Sub-linear root detection, and new hardness results, for sparse polynomials over finite fields*, in "ISSAC '13 - 38th international symposium on International symposium on symbolic and algebraic computation", Boston, United States, M. B. MONAGAN, G. COOPERMAN, M. GIESBRECHT (editors), ACM, June 2013, pp. 61-68 [*DOI :* 10.1145/2465506.2465514], http://hal.inria.fr/hal-00922224

[2] J. BI, J.-S. CORON, J.-C. FAUGÈRE, P. Q. NGUYEN, G. RENAULT, R. ZEITOUN. *Rounding and Chaining LLL: Finding Faster Small Roots of Univariate Polynomial Congruences*, in "PKC 2014 - 17th IACR International Conference on Practice and Theory of Public-Key Cryptography", Buenos Aires, Argentina, Springer, 2014, http://hal.inria.fr/hal-00926902

[3] J. BI, M. LIU, X. WANG. *Cryptanalysis of a homomorphic encryption scheme from ISIT 2008*, in "ISIT 2012 - IEEE International Symposium on Information Theory", Cambridge, États-Unis, IEEE, July 2012, pp. 2152 - 2156 [*DOI :* 10.1109/ISIT.2012.6283832], http://hal.inria.fr/hal-00922226

[4] Y. CHEN, P. Q. NGUYEN. *Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers*, in "EUROCRYPT 2012", Cambridge, Royaume-Uni, D. POINTCHEVAL, T. JOHANSSON (editors), Lecture Notes in Computer Science, Springer, April 2012, vol. 7237, pp. 502-519 [*DOI :* 10.1007/978-3-642-29011-4_30], http://hal.inria.fr/hal-00864374

[5] L. DUCAS, P. Q. NGUYEN. *Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic*, in "ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security", Beijing, Chine, X. WANG, K. SAKO (editors), Lecture Notes in Computer Science, Springer, December 2012, vol. 7658, pp. 415-432 [*DOI :* 10.1007/978-3-642-34961-4_26], http://hal.inria.fr/hal-00864360

[6] L. DUCAS, P. Q. NGUYEN. *Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures*, in "ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security", Beijing, Chine, X. WANG, K. SAKO (editors), Lecture Notes in Computer Science, Springer, December 2012, vol. 7658, pp. 433-450 [*DOI :* 10.1007/978-3-642-34961-4_27], http://hal.inria.fr/hal-00864359

[7] K. JIA, L. LI, C. RECHBERGER, J. CHEN, X. WANG. *Improved Cryptanalysis of the Block Cipher KASUMI*, in "SAC 2012 - 19th International Conference Selected Areas in Cryptography", Windsor, Canada, L. R. KNUDSEN, H. WU (editors), Lecture Notes in Computer Science, Springer, August 2012, vol. 7707, pp. 222-233 [*DOI :* 10.1007/978-3-642-35999-6_15], http://hal.inria.fr/hal-00922230

[8] T. JOHANSSON, P. Q. NGUYEN. , *Advances in Cryptology – EUROCRYPT 2013*, Lecture Notes in Computer Science, Springer, May 2013, vol. 7881, 736 p. [*DOI :* 10.1007/978-3-642-38348-9], http://hal.inria.fr/hal-00922221

[9] L. LI, K. JIA, X. WANG. *Improved Single-Key Attacks on 9-Round AES-192/256*, in "FSE 2014 (21st International Workshop on Fast Software Encryption)", Londres, United Kingdom, Lecture Notes in Computer Science, Springer, March 2014, http://hal.inria.fr/hal-00936032

[10] Y. LIU, L. LI, D. GU, X. WANG, Z. LIU, J. CHEN, W. LI. *New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia*, in "FSE 2012 - 19th International Workshop Fast Software Encryption", Washington, États-Unis, A. CANTEAUT (editor), Lecture Notes in Computer Science, Springer, March 2012, vol. 7549 [*DOI :* 10.1007/978-3-642-34047-5_6], http://hal.inria.fr/hal-00922229

[11] X. WANG, K. SAKO. , *Advances in Cryptology - ASIACRYPT 2012*, Lecture Notes in Computer Science, Springer, December 2012, vol. 7658, 780 p. [*DOI :* 10.1007/978-3-642-34961-4], http://hal.inria.fr/hal-00922232

[12] H. YU, J. CHEN, X. WANG. *The Boomerang Attacks on the Round-Reduced Skein-512*, in "SAC 2012 - 19th International Conference Selected Areas in Cryptography", Windsor, Canada, L. R. KNUDSEN, H. WU (editors), Lecture Notes in Computer Science, Springer, August 2012, vol. 7707, pp. 287-303 [*DOI :* 10.1007/978-3-642-35999-6_19], http://hal.inria.fr/hal-00922231

Publications of the year

Articles in International Peer-Reviewed Journals

[13] M. LIU, X. WANG, G. XU, X. ZHENG. *A note on BDD problems with λ2-gap*, in "Information Processing Letters", 2014, vol. 114, n° 1-2, pp. 9-12 [*DOI :* 10.1016/J.IPL.2013.10.004], http://hal.inria.fr/hal-00922234

[14] A. WANG, M. CHEN, Z. WANG, X. WANG. *Fault Rate Analysis: Breaking Masked AES Hardware Implementations Efficiently*, in "IEEE Transactions on Circuits and Systems. Part II, Express Briefs", July 2013, vol. 60-II, n° 8, pp. 517-521 [*DOI :* 10.1109/TCSII.2013.2268379], http://hal.inria.fr/hal-00922227

[15] W. WEI, C. TIAN, X. WANG. *New transference theorems on lattices possessing nϵ-unique shortest vectors*, in "Discrete Mathematics", February 2014, vol. 315-316, pp. 144-155 [*DOI :* 10.1016/J.DISC.2013.10.020], http://hal.inria.fr/hal-00922225

Invited Conferences

[16] P. Q. NGUYEN. *Abstracting Lattice-based Cryptography*, in "Workshop on Algebraic Aspects of Cryptography", Fukuoka, Japan, August 2013, http://hal.inria.fr/hal-00932567

[17] P. Q. NGUYEN. *Lattices and Finite Groups: Mathematics, Complexity and Cryptography*, in "Workshop on Number Theory, Geometry and Cryptography", Warwick, United Kingdom, July 2013, http://hal.inria.fr/hal-00932569

International Conferences with Proceedings

[18] D. BAI, H. YU, G. WANG, X. WANG. *Improved Boomerang Attacks on SM3*, in "ACISP 2013 - 18th Australasian Conference Information Security and Privacy", Brisbane, Australia, C. BOYD, L. SIMPSON (editors), Lecture Notes in Computer Science, Springer, July 2013, vol. 7959, pp. 251-266 [*DOI :* 10.1007/978-3-642-39059-3_17], http://hal.inria.fr/hal-00922228

[19] *Best Paper*
J. BI, Q. CHENG, M. ROJAS. *Sub-linear root detection, and new hardness results, for sparse polynomials over finite fields*, in "ISSAC '13 - 38th international symposium on International symposium on symbolic and algebraic computation", Boston, United States, M. B. MONAGAN, G. COOPERMAN, M. GIESBRECHT (editors), ACM, June 2013, pp. 61-68 [*DOI :* 10.1145/2465506.2465514], http://hal.inria.fr/hal-00922224.

[20] J. BI, J.-S. CORON, J.-C. FAUGÈRE, P. Q. NGUYEN, G. RENAULT, R. ZEITOUN. *Rounding and Chaining LLL: Finding Faster Small Roots of Univariate Polynomial Congruences*, in "PKC 2014 - 17th IACR International Conference on Practice and Theory of Public-Key Cryptography", Buenos Aires, Argentina, Springer, 2014, http://hal.inria.fr/hal-00926902

[21] G. HU, Y. PAN. *Improvements on Reductions among DIfferent Variants SVP and CVP*, in "WISA 2013 - 14th International Workshop on Information Security Applications", Jeju Island, Korea, Republic Of, Y. KIM, H. LEE, A. PERRIG (editors), Lecture Notes in Computer Science, Springer, August 2013, http://hal.inria.fr/hal-00932449

[22] G. HU, Y. PAN, F. ZHANG. *Solving Random Subset Sum Problem by l_p-norm SVP Oracle*, in "PKC 2014 - 17th IACR International Conference on Practice and Theory of Public-Key Cryptography (2014)", Buenos Aires, Argentina, Springer, March 2014, http://hal.inria.fr/hal-00936030

[23] L. LI, K. JIA, X. WANG. *Improved Single-Key Attacks on 9-Round AES-192/256*, in "FSE 2014 (21st International Workshop on Fast Software Encryption)", Londres, United Kingdom, Lecture Notes in Computer Science, Springer, March 2014, http://hal.inria.fr/hal-00936032

[24] M. LIU, P. Q. NGUYEN. *Solving BDD by Enumeration: An Update*, in "CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013", San Francisco, United States, E. DAWSON (editor), Lecture Notes in Computer Science, Springer, February 2013, vol. 7779, pp. 293-309 [*DOI :* 10.1007/978-3-642-36095-4_19], http://hal.inria.fr/hal-00864361

[25] F. ZHANG, Y. PAN, G. HU. *A Three-Level Sieve Algorithm for the Shortest Vector Problem*, in "SAC 2013 - 20th International Conference on Selected Areas in Cryptography", Burnaby, Canada, T. LANGE, K. LAUTER, P. LISONEK (editors), Springer, August 2013, vol. Lecture Notes in Computer Science, http://hal.inria.fr/hal-00932455

Books or Proceedings Editing

[26] T. JOHANSSON, P. Q. NGUYEN (editors). , *Advances in Cryptology – EUROCRYPT 2013*, Lecture Notes in Computer Science, Springer, May 2013, vol. 7881, 736 p. [*DOI :* 10.1007/978-3-642-38348-9], http://hal.inria.fr/hal-00922221

References in notes

[27] A. BIRYUKOV, D. KHOVRATOVICH. *Related-Key Cryptanalysis of the Full AES-192 and AES-256*, in "Proc. ASIACRYPT '09", Lecture Notes in Computer Science, Springer, 2009, vol. 5912, pp. 1-18

[28] A. BIRYUKOV, D. KHOVRATOVICH, I. NIKOLIC. *Distinguisher and Related-Key Attack on the Full AES-256*, in "Proc. CRYPTO '09", Lecture Notes in Computer Science, Springer, 2009, vol. 5677, pp. 231-249

[29] Y. CHEN, P. Q. NGUYEN. *BKZ 2.0: Better Lattice Security Estimates*, in "Advances in Cryptology - Proc. ASIACRYPT '11", Lecture Notes in Computer Science, Springer, 2011

[30] N. GAMA, P. Q. NGUYEN, O. REGEV. *Lattice Enumeration Using Extreme Pruning*, in "Advances in Cryptology - Proc. EUROCRYPT '10", Lecture Notes in Computer Science, Springer, 2010, vol. 6110, pp. 257-278

[31] S. GARG, C. GENTRY, S. HALEVI. *Candidate Multilinear Maps from Ideal Lattices*, in "Advances in Cryptology - Proc. EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic", Lecture Notes in Computer Science, Springer, 2013, vol. 7881, pp. 1-17

[32] S. GARG, C. GENTRY, S. HALEVI, M. RAYKOVA, A. SAHAI, B. WATERS. *Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits*, in "54th Annual IEEE Symposium on Foundations of Computer Science, Proc. FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA", IEEE Computer Society, 2013, pp. 40-49

[33] C. GENTRY. *Fully homomorphic encryption using ideal lattices*, in "Proc. STOC '09", ACM, 2009, pp. 169-178

[34] P. SEPEHRDAD, S. VAUDENAY, M. VUAGNOUX. *Statistical Attack on RC4 - Distinguishing WPA*, in "Proc. EUROCRYPT '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6632, pp. 343-363