Mathematisches Forschungsinstitut Oberwolfach

Report No. 5/2017

DOI: 10.4171/OWR/2017/5

Cryptography

Organised by
Johannes Buchmann, Darmstadt
Shafi Goldwasser, Cambridge MA

15 January – 21 January 2017

Abstract. The Oberwolfach workshop Cryptography brought together scientists from cryptography with mathematicians specializing in the algorithmic problems underlying cryptographic security. The goal of the workshop was to stimulate interaction and collaboration that enables a holistic approach to designing cryptography from the mathematical foundations to practical applications. The workshop addressed fundamental research results leading to innovative cryptography for protecting security and privacy.

Mathematics Subject Classification (2010): 94A60.

Introduction by the Organisers

The goal of the workshop Cryptography, organized by Johannes Buchmann (Darmstadt) and Shafi Goldwasser (Boston) was to stimulate interaction and collaboration between mathematicians and computer scientists that enables a holistic approach to designing cryptography from the theoretical foundations to practical applications. The topic of the workshop is highly relevant for both research and application. Cryptography has long been an integral building block of many cyber security solutions and has therefore been of critical importance to modern IT security. On the other hand technological progress presents multiple new scientific challenges. For instance the rise of cloud computing requires novel cryptographic approaches and constructions. Additionally future developments in quantum computing threaten current schemes, which shows the need for quantum resistant cryptography.

The talks given at the workshop covered important recent results in the areas relevant for the workshop. The talks on the mathematical foundations addressed both traditional and more recent algorithmic problems that serve as the security basis of modern cryptography. A major topic of the workshop were obfuscation schemes. These primitives allow to hide the the source code of a given program against a computationally bounded adversary, while preserving the functionality of the program. It is possible to construct such schemes from multilinear maps or graded encoding schemes. The presented results showed that there is progress in the construction of obfuscation from multilinear maps, but for certain applications there are still powerful attacks on the underlying encoding schemes.

The talks on post quantum cryptography covered both new constructions and new cryptanalysis. In light of a recent call for proposals for post quantum schemes by NIST, new constructions for public key encryption and key exchange were presented from both lattices and codes. Furthermore there were talks on new attack both classical and quantum on certain schemes. The presentations on advanced cryptographic constructions included new constructions in attribute based encryption, updatable encryption and spooky encryption. These techniques allow for further functionalities, required to address the challenges of outsourced data. Multiple session dealt with the topic of secure multi-party computation, which enables multiple entities to jointly compute on data in a privacy preserving way. Novel constructions such as function secret sharing were very well presented during the talks of the workshop.

There were also several talks dealing with practical challenges, such as the possibility of trapdoored public parameters in widely used cryptographic libraries and privacy preserving operations on genomic data.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, “US Junior Oberwolfach Fellows”.

Workshop: Cryptography

Table of Contents

Abstracts

Rethinking Large-Scale Consensus Through Blockchain

Rafael Pass

We revisit classic questions in distributed computing in settings where players at any point can go offline.

We ask: Can we design consensus protocols under "sporadic participation" where at any given point only a subset of the players are online.

Program Obfuscation: Outside the Black Box

Omer Paneth

Code is said to be obfuscated if it is intentionally difficult for humans to understand. Obfuscation is often used to conceal sensitive implementation details such as proprietary algorithms or licensing mechanisms.

A general-purpose obfuscator is a compiler that obfuscates arbitrary code (in some particular language) without altering the code's functionality. Ideally, the obfuscated code would hide any information about the original code that cannot be obtained by simply executing it.

The potential applications of general-purpose obfuscators extend beyond software protection. For example, in computational complexity theory, obfuscation is used to establish the intractability of a range of computational problems. Obfuscation is also a powerful tool in cryptography, enabling a variety of advanced applications.

The possibility of general-purpose obfuscation was put into question by Barak et al. [1], who proved that such obfuscation cannot have ideal security. Nevertheless, they leave open the possibility of obfuscation with weaker security properties, which may be sufficient for many applications. Recently, Garg et al. [2] suggested a candidate construction for general-purpose obfuscation conjectured to satisfy these security properties.

We study the feasibility and applicability of different notions of secure obfuscation. In terms of applicability, we prove that finding a Nash equilibrium of a game is intractable, based on a weak notion of obfuscation known as indistinguishability obfuscation [4]. In terms of feasibility, we focus on a variant of the Garg at el. obfuscator that is based on a recent construction of cryptographic multilinear maps [3]. We reduce the security of the obfuscator to that of the underlying multilinear maps.

Our first reduction considers obfuscation and multilinear maps with ideal security [5]. We then study a useful strengthening of indistinguishability obfuscation known as virtual-grey-box obfuscation. We identify security properties of multilinear maps that are necessary and sufficient for this notion [6]. Finally, we explore the possibility of basing obfuscation on weaker primitives. We show that obfuscation is impossible even based on ideal random oracles [7].

References

[1] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, 1–18, 2001.

[2] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, 40–49, 2013.

[3] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In *EUROCRYPT*, 1–17, 2013.

[4] N. Bitansky, O. Paneth, and A. Rosen. On the cryptographic hardness of finding a nash equilibrium. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, 1480–1498, 2015.

[5] B. Barak, S. Garg, Y. Tauman Kalai, O. Paneth, and A. Sahai. Protecting obfuscation against algebraic attacks. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, 221–238, 2014.

[6] N. Bitansky, R. Canetti, Y. Tauman Kalai, and O. Paneth. On virtual grey box obfuscation for general circuits. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, 108–125, 2014.

[7] R. Canetti, Y. Taumann Kalai, and O. Paneth. On obfuscation with random oracles. In *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part II*, 456–467, 2015.

Indistiniguishability Obfuscation from DDH on 5-linear Maps and Locality-5 PRGs

Huija (Rachel) Lin

We present a new construction of Indistinguishability Obfuscation (IO) from the following.

- Asymmetric L-linear map [1, 2] with subexponential Decisional Diffie-Hellman (DDH) assumption
- Locality-L polynomial-stretch pseudorandom generator (PRG) with subexponential security
- The subexponential hardness of learning with errors (LWE)

  When plugging in a candidate PRG with locality 5 (e.g. [3]) we obtain a construction of IO from subexponential DDH on 5-linear maps and LWE. Previous IO constructions rely on multilinear maps or graded encoding schemes with higher degrees, more complex functionalities (e.g. graded encodings with complex label structures), and stronger assumptions (e.g. the joint-SXDH assumption).

References

[1] D. Boneh and A. Silverberg. Applications of Multilinear Forms to Cryptography. Cryptology ePrint Archive, Report 2002/80.

[2] R. Rothblum On the Circular Security of Bit-Encryption. In *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013, Proceedings*, 579–598.

[3] R. O'Donnell and D. Witmer. Goldreich's PRG: Evidence for Near-Optimal Polynomial Stretch. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, 1–12.

Obfuscating Groups

Dennis Hofheinz

(joint work with Martin Albrecht, Pooya Farshim, Julia Hesse, Enrique Larraia, and Kenny Paterson)

We propose to use (indistinguishability) obfuscation to enhance the security and functionality of cryptographically useful groups. For instance, by attaching an encryption of the respective discrete logarithm to each group element, it is possible to efficiently implement a multilinear map over that group. The corresponding multilinear map is an obfuscated algorithm that knows the decryption trapdoor, and thus can extract and multiply the discrete logarithms of all involved group elements. Still, we can show that cryptographically useful computational assumptions hold in that group. Moreover, we show that similar constructions can be used to construct groups in which very strong computational assumptions (such as variants of the "Uber assumption" due to Boneh, Boyen, and Goh hold).

Our results imply new and abstract constructions of multilinear maps that allow, e.g., for multilinear variants of Groth-Sahai proof systems. However, while our constructions are abstract and modular, we use a number of strong building blocks: we use (subexponentielly secure) indistinguishability obfuscation, fully homomorphic encryption, dual-mode zero-knowledge proof systems, and cyclic groups in which the Strong Diffie-Hellman assumption holds. (Of course, for our construction of groups in which Uber assumptions hold, we do not require Strong Diffie-Hellman groups.)

This talk surveys our results, and the main ideas from our constructions. In particular, this talk covers the results from [1, 2, 3].

References

[1] M. R. Albrecht, P. Farshim, D. Hofheinz, E. Larraia, and K. G. Paterson. Multilinear maps from obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, 446–473. Springer, Heidelberg, January 2016.

[2] P. Farshim, J. Hesse, D. Hofheinz, and E. Larraia. Graded Encoding Schemes from Obfuscation. Manuscript, 2016.

[3] T. Agrikola and D. Hofheinz. Interactively Secure Groups from Obfuscation. Manuscript, 2016.

From Search to Approximate-Decision, Locally, and while Preserving Exponential Hardness

Benny Applebaum

The Gap-ETH assumption (Dinur 2016; Manurangsi and Raghavendra 2016) asserts that it is exponentially-hard to distinguish between a satisfiable 3-CNF formula and one which is only $(1-\delta)$-satisfiable. We show that this assumption follows from the exponential-hardness of solving *smooth* 3-CNF's. Here smoothness means that the number of satisfying assignments is not much smaller than the number of "almost-satisfying" assignments. We further show that the latter ("smooth-ETH") assumption follows from the exponential-hardness of solving constraint satisfaction problems over well-studied planted distributions, and, more generally, from the existence of an exponentially-hard locally-computable one-way function.

We also prove an analogous result in the cryptographic setting. Namely, we show that the existence of exponentially-hard locally-computable pseudorandom generator with linear stretch (EL-PRG) follows from the existence of an exponentially-hard locally-computable regular one-way functions.

None of the above assumptions (Gap-ETH and EL-PRG) was previously known to follow from the hardness of a search problem. Our results are based on a new construction of general (GL-type) hard-core functions which outputs linearly many hard-core bits, can be locally-computed, and uses only a linear amount of random bits.

Cryptanalyses of Candidate Branching Program Obfuscators

Shai Halevi
(joint work with Yilei Chen and Craig Gentry)

We describe new cryptanalytic attacks on the candidate branching program obfuscator proposed by Garg, Gentry, Halevi, Raykova, Sahai and Waters (GGHRSW) [8] using the GGH13 graded encoding [7], and its variant using the GGH15 graded encoding as specified by Gentry, Gorbunov and Halevi [9]. All our attacks require very specific structure of the branching programs being obfuscated, which in particular must have some input-partitioning property. Common to all our attacks are techniques to extract information about the "multiplicative bundling" scalars that are used in the GGHRSW construction.

For GGHRSW over GGH13, we show how to recover the ideal generating the plaintext space when the branching program has input partitioning. Combined with the information that we extract about the "multiplicative bundling" scalars, we get a distinguishing attack by an extension of the annihilation attack of Miles, Sahai and Zhandry [10]. Alternatively, once we have the ideal we can solve the principle-ideal problem (PIP) in classical subexponential time or quantum polynomial time, hence obtaining a total break.

For the variant over GGH15, we show how to use the left-kernel technique of Coron, Lee, Lepoint and Tibouchi [5] to recover ratios of the bundling scalars. Once we have the ratios of the scalar products, we can use factoring and PIP solvers (in classical subexponential time or quantum polynomial time) [1, 4, 2, 3, 6] to find the scalars themselves, then run mixed-input attacks to break the obfuscation.

References

[1] M. R. Albrecht, S. Bai, and L. Ducas. A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes. In *CRYPTO (1)*, volume 9814 of *LNCS*, 153–178. Springer, 2016.

[2] J. -F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A):385–403, 2014.

[3] J. -F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, 893–902. SIAM, 2016.

[4] J. H. Cheon, J. Jeong, and C. Lee. An algorithm for CSPR problems and cryptanalysis of the GGH multilinear map without an encoding of zero. Cryptology ePrint Archive, Report 2016/139.

[5] J. -S. Coron, M. S. Lee, T. Lepoint, and M. Tibouchi. Cryptanalysis of GGH15 multilinear maps. In *CRYPTO (2)*, volume 9815 of *LNCS*, 607–628. Springer, 2016.

[6] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT (2)*, volume 9666 of *LNCS*, 559–585. Springer, 2016.

[7] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *LNCS*, 1–17. Springer, 2013.

[8] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM J. Comput.* 45(3): 882–929 (2016).

[9] C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices. In *Theory of Cryptography*, volume 9015 of *LNCS*, 498–527. Springer, 2015.

[10] E. Miles, A. Sahai, and M. Zhandry. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13. In *CRYPTO (2)*, volume 9815 of *LNCS*, 629–658. Springer, 2016.

Nipped in the Bud: Graded Encoding Schemes that Did Not Make It

Zvika Brakerski

(joint work with Craig Gentry, Shai Halevi, Tancrède Lepoint, Amit Sahai, Mehdi Tibouchi)

Zeroizing attacks [4, 1, 2, 7] were shown to be a potent line of attacks against existing graded encoding candidates [4, 3, 5]. Although some applications do not seem to be affected by these attacks, they were used to break a number of applications (and many hardness assumptions on) these graded encoding candidates.

Roughly speaking, zeroizing attacks proceed by honestly computing many top-level encoding of zero, then using the prescribed zero-testing procedure to setup and solve a system of multilinear equations in the secret parameters of the scheme.

These attacks rely crucially on the linearity of the zero-testing procedure, and so some attempts were made recently to devise alternative zero-testing procedures that are non-linear. In one of these attempts [6], Gentry, Halevi and Lepoint recently described a variant of the GGH13 candidate scheme [4], in which the linear zero-testing procedure from [4] is replaced by a quadratic (or higher-degree) procedure.

We show that the Gentry-Halevi-Lepoint (GHL) variant remains susceptible to the same zeroizing attacks as the original GGH13. In particular, we show how to construct a native GGH13 zero-test parameter from the GHL quadratic zero-test parameter. In a nutshell, this is done by computing the "derivative" of the quadratic zero-test polynomial at a top-level encoding of zero, thus obtaining a linear zero-test polynomial that can be transformed into a native GGH13 zero-test parameter.

1. GGH with High-Degree Zero-Test

The GGH13 graded encoding candidate [4] works over the quotient ring $R_q = R/qR$ where $R = \mathbb{Z}[x]/(x^n + 1)$ is the $2n$-th cyclotomic polynomial ring (n a power of two) and q is a large modulus.[1] The plaintext space is $R_g = R/gR$ where $g \in R$ is a small (secret) element. A level-k encoding u of $m \in R_g$ is such that $u = [c/z^k]_q$ where $c \in m + gR$ is small and $z \leftarrow R_q$ is a random (secret) multiplicative mask. Encodings at the same levels can be added (and the encoded values get added modulo R_g), and encodings can be multiplied as long as the sum of the levels remains smaller than the multi-linearity level κ (and the encoded values get multiplied modulo R_g).

The GGH13 Zero-Testing. The zero-testing procedure of GGH13 consists in multiplying a level-κ encoding $u = [c/z^\kappa]_q$ by a public value $p_{zt} = [h/g \cdot z^\kappa]_q$, where h is a somewhat small secret value, so that

$$w = [u \cdot p_{zt}]_q = [h \cdot (c/g)]_q \tag{1}$$

has norm smaller than (say) $q^{3/4}$ if and only if $c \in gR$, i.e. if and only if u is a top-level encoding of $0 \in R_g$. Now when $c = gr$ over R, Eq. (1) holds over R and gives $w = h \cdot r$ which is linear in r. This R-linearity can then be exploited in zeroizing attacks [4, 7].

Quadratic Zero-Testing. During the invited talk of CRYPTO 2015, Halevi described a tentative fix due to Gentry, Halevi and Lepoint (GHL) aiming at making the zero-testing procedure at least quadratic in the coefficients of the input (and therefore breaking the R-linearity of the zero-testing procedure at the core of the zeroizing attacks) [6]. For any encoding $u = \sum_{i=0}^{n-1} u_i \cdot x^i \in R_q$, denote $\vec{u} = (u_0, \ldots, u_{n-1}) \in \mathbb{Z}_q^n$ its vector of coefficients. The GHL zero-testing procedure is given by a quadratic polynomial $p\colon \mathbb{Z}_q^n \to \mathbb{Z}_q$ such that

$$|p(\vec{u}) \bmod q| < q^{3/4} \iff u \text{ is a top-level encoding of } 0\,.$$

[1] Our attack extends to any cyclotomic polynomial ring $R = \mathbb{Z}[x]/(\Phi(x))$ when Φ has small enough coefficients. For ease of simplicity we restrict our description to $\Phi(x) = x^n + 1$ for n a power of 2.

The key idea is to define p as $p(\vec{u}) = \sum_{i,j} \alpha_{ij} \cdot \ell_i(\vec{u}) \cdot \ell_j(\vec{u})$ where the $\alpha_{i,j}$'s are small (say, $\|\alpha_{ij}\|_\infty < q^{1/4}$) and the ℓ_i's are the linear equations corresponding to the multiplication by a native GGH13 zero-test parameter p_{zt} over R_q, i.e. such that $w = [u \cdot p_{zt}]_q$ has coefficient-vector $\vec{w} = (\ell_0(\vec{u}), \ldots, \ell_{n-1}(\vec{u}))$ and (say) $\|w\|_\infty < q^{1/4}$. It is easy to generalize the GHL zero-testing procedure to a polynomial of higher degree d by considering monomials of the form $\ell_{i_1}(\vec{u}) \cdots \ell_{i_d}(\vec{u})$. Note, however, that describing the new zero-test polynomial takes $\Theta(n^d)$ terms, hence for this zero-test procedure to be polynomial-time we need the degree d to be a constant.

2. Cryptanalysis

The key idea of the attack will be to compute the "derivative" of the high-degree polynomial in a top-level encoding of 0, reducing its degree until we get back a linear polynomial.

Definition. Let $p(x_0, \ldots, x_{n-1}) \in \mathbb{Z}_q[x_0, \ldots, x_{n-1}]$ be a polynomial. For all $\vec{a} = (a_1, \ldots, a_{n-1}) \in \mathbb{Z}_q^n$, we define $p'_{\vec{a}} \in \mathbb{Z}_q[x_1, \ldots, x_n]$ the derivative of p in $\vec{a}$ as

$$p'_{\vec{a}}(x_0, \ldots, x_{n-1}) = p(x_0 + a_0, \ldots, x_{n-1} + a_{n-1}) - p(x_0, \ldots, x_{n-1}) \bmod q\,.$$

Note that if $p(\vec{x})$ is of total degree $t \geq 1$ in the x_i's, then $p'_{\vec{a}}(\vec{x})$ is of total degree at most $t-1$.

Reducing the Degree. Let $p_d(\cdot)$ be the degree-d zero-testing polynomial of GHL, so for every top-level encoding of zero x we have $|p_d(\vec{x}) \bmod q| < q^{3/4}$ (say). Also let $u \in R_q$ be some fixed top-level encoding of zero. For $i = 1, 2, \ldots, d-1$ we compute $p_{d-i}(\cdot)$ by deriving $p_{d+1-i}(\cdot)$ at u, setting

$$p_{d-i}(\vec{x}) = p_{d+1-i}(\vec{x} + \vec{u}) - p_{d+1-i}(\vec{x}) \bmod q\,.$$

Clearly the total degree of each p_j is (at most) j, and in particular the last polynomial $p_1(\vec{x})$ has degree (at most) 1.

Moreover, we can prove by induction on i that for every top-level encoding of zero v we have $|p_{d-i}(\vec{v}) \bmod q| < 2^i \cdot q^{3/4}$. This clearly holds for p_d, so now assume that it holds for p_{d+1-i} and we prove for p_{d-i}. Note that since both u, v are top-level encoding of zero then so is $v + u$, and therefore

$$\begin{aligned} |p_{d-i}(\vec{v})| &= |p_{d+1-i}(\vec{v} + \vec{u}) - p_{d+1-i}(\vec{v})| \\ &\leq |p_{d+1-i}(\vec{v} + \vec{u})| + |p_{d+1-i}(\vec{v})| < 2^{i-1} q^{3/4} + 2^{i-1} q^{3/4} = 2^i \cdot q^{3/4}. \end{aligned}$$

We conclude that for every top-level encoding of zero v we have $|\rho + \sum_{i=1}^{n-1} \rho_i \cdot v_i| < 2^{d-1} \cdot q^{3/4}$ (and note that since d is a constant then $2^{d-1} \cdot q^{3/4} \ll q$).

We note that the native GGH13 zero-test is linear whereas the polynomial p_1 is above is affine, so recovering a native GGH13 zero-test parameter seem to require that we ignore the free term. Indeed, below we show that the free term ρ from above must be small, and therefore we can ignore it without affecting the zero-test result.

Recovering a Native GGH13 Zero-Test Parameter. Finally, we use the structure of the ring R_q to recover a native GGH13 zero-test parameter, i.e. a ring element $r \in R_q$ such that $\|r \cdot v \bmod q\| \ll q$ for every top-level encoding of zero v. Specifically we define $r(X) = \rho_0 - \sum_{i=1}^{n-1} \rho_{n-i} \cdot X^i \in R_q$, and we show that r is a native GGH13 zero-test parameter.

References

[1] J. H. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehlé. Cryptanalysis of the multilinear map over the integers. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, 3–12. Springer, Apr. 2015.

[2] J.-S. Coron, C. Gentry, S. Halevi, T. Lepoint, H. K. Maji, E. Miles, M. Raykova, A. Sahai, and M. Tibouchi. Zeroizing without low-level zeroes: New MMAP attacks and their limitations. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, 247–266. Springer, Aug. 2015.

[3] J.-S. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, 476–493. Springer, Aug. 2013.

[4] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, 1–17. Springer, May 2013.

[5] C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices. In Y. Dodis and J. B. Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, 498–527. Springer, Mar. 2015.

[6] S. Halevi. The state of cryptographic multilinear maps, 2015. Invited Talk of CRYPTO 2015.

[7] Y. Hu and H. Jia. Cryptanalysis of GGH map. Cryptology ePrint Archive, Report 2015/301, 2015. `http://eprint.iacr.org/2015/301`.

Improving Distributed Storage Systems Through Adaptive Social Secret Sharing

Giulia Traverso

(joint work with Denise Demirel, Sheikh M. Habib, Johannes Buchmann)

Due to the increase of digital data in the last years, it might be difficult for a user to have enough resources to store its data. A solution is to outsource these data to the Cloud and let one or multiple Cloud providers manage this storage through their storage servers. However, Cloud providers have to ensure certain guarantees such that for the user it is worth to pay for this service. More precisely, there are two protection aspects that Cloud providers must guarantee in the long-term. On the one hand, the data must remain confidential, i.e. no information should be leaked to a third party. On the other hand, the data must be retrieved efficiently any time it is needed. These two protection goals are clear when thinking of health records. Health records are sensitive data that if revealed can damage the patient (e.g. sexual diseases) but in case of an emergency they have to be retrieved fast and correctly (e.g. the blood group when transfusion is needed).

Confidentiality and retrievability are inherent to the behavior of the storage servers involved: when storage servers are untrustworthy, then confidentiality and retrievability might not be guaranteed any more. More precisely, honest but curious storage servers follow all the protocols correctly but are also prone to leak information to a third party or to collude. In this sense, they are untrustworthy with respect to confidentiality. Faulty storage servers do not respond or respond late when the data have to be retrieved, compromising the entire process. In this sense they are untrustworthy with respect to retrievability.

We provide a solution [6] to this framework, called AS^3, which is a social secret sharing scheme based on adaptive hierarchical secret sharing. Secret sharing [3] is a cryptographic primitive that distributes a document within a storage system by generating shares of that document. Each share is such that it reveals no information about the document itself and is stored within a different storage server. For threshold secret sharing schemes, a subset of a certain size of shares is sufficient to retrieve the document. In this sense, secret sharing is the right primitive for distributed storage systems to be based on because by design it offers confidentiality and retrievability. Social secret sharing [2] is equipped with a trust function which tests the behavior of the storage servers and grants different reconstruction power according to their trustworthiness. That is, more informative shares are distributed for the better behaving storage servers and less informative shares are distributed to the worse behaving storage servers. Hierarchical secret sharing [4] is used in this context as the underlying scheme for social secret sharing: the most trustworthy storage servers are treated as the most powerful participants in a hierarchical structure. However, current solutions [2], [1] fail at providing confidentiality and retrievability of the document outsourced. The first reason is that hierarchical secret sharing schemes are not flexible and thus they cannot rearrange the threshold and generate new shares in accordance to the updated trust values. We overcome this drawback by proposing the first Birkhoff interpolation based hierarchical secret sharing scheme that is dynamic [5]. The second reason is that, previous to our work, the notion of trust was not well defined and, thus, the trustworthiness of the storage servers could not be properly rated since the two different behavior of confidentiality and retrievability were not distinguished yet. In addition, we overcome this second problem by defining a new trust function that tests the storage servers with respect to confidentiality and retrievability in a separate way, outputting two trust values for each storage servers. Thanks to our countermeasures, AS^3 is the first construction of social secret sharing that actually works effectively in the framework of distributed storage systems. Rules and checks for confidentiality and retrievability are given such that each time the trust functions updates the trust values, the threshold of the secret sharing scheme can be adapted such that honest but curious storage servers can never retrieve the document by themselves and the absence of the faulty storage servers cannot prevent the remaining ones from retrieving the document.

References

[1] M. Nojoumian and D. R. Stinson. Social secret sharing in cloud computing using a new trust function. In *Tenth Annual International Conference on Privacy, Security and Trust, PST 2012, Paris, France, July 16-18, 2012*,pages 161–167, 2012.

[2] M. Nojoumian and D. R. Stinson. Brief announcement: secret sharing based on the social behaviors of players. In *Proceedings of the 29th Annual ACM Symposium on Principles of Distributed Computing, PODC 2010, Zurich, Switzerland, July 25-28, 2010*, 239–240, 2010.

[3] A, Shamir. How to Share a Secret. In *Commun. ACM*, volume 22, number 11, 612–613, 1979.

[4] T. Tassa. Hierarchical Threshold Secret Sharing. In *J. Cryptology*, volume 20, number 2, 237–264, 2007.

[5] G. Traverso, D. Demirel, and J. Buchmann, Dynamic and Verifiable Hierarchical Secret Sharing In *Information Theoretic Security - 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers*, 24–43, 2016.

[6] G. Traverso, D. Demirel, S. Habib, and J. Buchmann AS^3: Adaptive Social Secret Sharing for Distributed Storage Systems. In *14th Annual Conference on Privacy, Security, an Trust (PST) 2016, Auckland, New Zealand, 1–20, 2016.*

Atribute Based Encryption and Information-Theoretic Crypto

Hoeteck Wee

Can we encrypt data while enabling fine grained access control? We survey how addressing this question led to new connections and questions in information-theoretic cryptography.

Composition: The Key to Differential Privacy's Success

Guy N. Rothblum

Differential privacy provides a rigorous and robust privacy guarantee to individuals in the context of statistical data analysis. It has sparked a revolution in the study of privacy-preserving data analysis, impacting fields from computer science to statistics to legal scholarship. A key factor underlying this success is robustness under composition: when multiple differentially private algorithms are run on the same individual's data, privacy degrades smoothly and gradually.

It is hard to overstate the importance of robustness under composition. In reality, individuals' data are involved in multiple datasets and analyses. Privacy that does not compose offers only questionable protection. No less important, composition makes Differential Privacy *programmable*: differentially private algorithms for small or common tasks can be used as subroutines in larger more complex algorithms, and inherit the subroutines' privacy guarantees (up to some degradation).

Composition has been key to differential privacy's success, and understanding how privacy degrades under composition is a core issue in the study of privacy-preserving data analysis. The differential privacy community has attempted to achieve a more perfect understanding of composition. Recent works have made significant advances in this study, touching on issues in complexity theory, probability theory, and shedding new light on the behavior of differentially private algorithms.

This talk will survey the study of composition in differentially private data analysis, from basic definitions and guarantees and all the way to the most recent developments and open questions in this exciting frontier.

Accessing Data While Preserving Privacy

Kobbi Nissim

We study the privacy-efficiency tradeoff of secure remote database systems. Such systems allow storing data on an untrusted server and accessing it efficiently while maintaining the privacy of the data. While strong cryptographic tools (e.g. FHE, ORAM,SFE) can be used, implementations experiment with weaker primitives with the hope of striking a good privacy-efficiency balance.

Our approach is implementation independent. We provide abstract models that capture fundamental leakage channels of such systems and provide reconstruction attacks using these leakage channels. We also present a new model- PP- storage, that provably protects data from these and other attacks, and implement DP-storage using ORAM and tools from differential privacy.

The LWE-based key exchange – A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem

Jintai Ding

Key exchange protocol enables two users to exchange keys in untrusted channels without sharing secret materials in advance. The first and celebrated key exchange protocol is the Diffie-Hellman key exchange protocol [16] which is also a fundamental construction in public key cryptography. It is simple and elegant, and, after its invention, countless applications based on Diffie-Hellman key exchange protocol or the Diffie-Hellman problem were proposed.

Diffie and Hellman [16] also introduced the notion of public key encryption, and Rivest, Shamir and Adleman [27] gave the first concrete public key encryption scheme. Namely, the well-known RSA encryption. With public key encryption in hand, one can construct a key exchange protocol. Instantiating with the RSA algorithm, the construction produces a very efficient key exchange protocol. However, the encryption-type key exchange protocol may have an important side-effect in practice: This approach relies on the user's private key to protect all the session keys, anyone with access to a copy of the private key can also uncover the session keys and thus decrypt everything.

The Diffie-Hellman protocol offers an alternative algorithm to RSA for cryptographic key exchange. The Diffie-Hellman protocol generates more secure session keys that can't be recovered simply by knowing the user's private key, a protocol security feature called *forward security.* In order to decrypt all communication, now the adversary can no longer compromise just the user's private key, but the adversary has to compromise the session keys belonging to every individual communication session. In other words, using the Diffie-Hellman protocol, even an adversary knows the session key of some particular session, he still can not learn anything about the session keys established before this particular session. Actually, SSL also uses the Diffie-Hellman protocol to support forward security.

The motivation of this report is to build simple Diffie-Hellman like key exchange protocols based on lattices. Lattice-based public key cryptography has become a promising potential alternative to public key cryptography based on traditional number theory assumptions. One building block of lattice-based cryptography, especially in encryption, is the learning with errors (LWE) problem. After the introduction of LWE problem by Regev [26], it has attracted a lot of attentions in theory and applications due to its usage in cryptographic constructions with good provable secure properties. In a nutshell, the (decisional) LWE problem is to distinguish polynomially many noisy inner-product samples of the form $(\mathbf{a}, b \approx \langle \mathbf{a}, \mathbf{s} \rangle)$ from uniformly random ones, where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ are uniformly random.[1] An attractive property of the LWE problem is that Regev [26] shows that to solve the average-case LWE problem is at least as hard as to (quantumly) solve some worst-case hard lattice problems. Many lattice-based primitives based on LWE have been discovered, such as public-key encryption [26, 18, LP11], (hierarchical) identity-based encryption [18, 1, 15], functional encryption [3, 2, 9, 19] and fully homomorphic encryption [12, 11, 10].

In the constructions mentioned above, a matrix form of the LWE problem is always used (i.e., need sufficient many samples). The drawback of that is it results in large (say quadratic) key size. To further improve the efficiency, Lyubashevsky, Peikert and Regev [24] introduced the ring learning with errors (RLWE) problem, which is to distinguish polynomially many noisy ring multiplications $(a, b \approx a \cdot s)$ from uniform distribution, where " $\cdot$" is the multiplicative operation over some ring. It's shown in [24] that to solve the RLWE problem is at least as hard as to solve some worst-case problems in *ideal* lattices, instead of general lattices.

What motivates the work in this report is to try to build a simple key exchange protocol using the basic idea of Diffie-Hellman protocol but based on the LWE and RLWE problem. There are already related works in [21, 22, 14, 17], but as far as we know there is not yet until very recently any provably secure key exchange protocols based on the LWE problem as a direct generalization of the Diffie-Hellman key exchange protocol, which is elegant in terms of its simplicity. Our work was finished in 2012 [20]. Recent works on LWE-based Key exchange protocols [25], [8], [5], [7] are all variants of our protocol with minor modifications but some with significant contributions in concrete implementations.

To achieve our goal, we use the normal form of LWE problem suggested in [6] and introduce a new randomized method to eliminate bias, which may be of independent interest.

[1] $\mathbf{s}$ is secret and remains the same in all the samples.

The key idea behind our new construction can be viewed as a way to share a secret given by the value of the bilinear function of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{Z}_q^n$, where q, n are some integers, via the bilinear form:

$$Q(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \mathbf{A} \mathbf{y} = (\mathbf{x}^T \mathbf{A})\mathbf{y} = \mathbf{x}^T(\mathbf{A}\mathbf{y}),$$

where $\mathbf{A}$ is an $n \times n$ matrix in $\mathbb{Z}_q$. Surely in order to make the system provably secure, we need to introduce the small errors to achieve our goal. The main contribution of our work is to use this simple idea to build a simple and provably secure key exchange scheme. The idea of such an "noise" or "approximate" KE appeared long time ago like the work of Buchmann and Williams [13], and recently the work [4] using coding theory. A new fundamental contribution of ours, which is something very different from the DH KE is that we developed a new idea of "signal functions" as an additional tool needed to round the approximate value to a shared secret without affecting the security. Furthermore, we extend our construction further based on the RLWE problem. Our construction is a significant additional step in showing how versatile the LWE assumption can be.

Besides, we also give an interactive multiparty key exchange protocol. This protocol can be viewed as a generalization of our two party protocol. Although the provable security of the protocol seems plausible but we do not know how to do it, and we leave it as an open problem.

References

[1] S. Agrawal, D. Boneh, and X. Boyen. Efficient Lattice (H)IBE in the Standard Model. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010, Proceedings*, 553–572, 2010.

[2] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee. Functional Encryption for Threshold Functions (or Fuzzy IBE) from Lattices, In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proceedings*, 280–297, 2012.

[3] S. Agrawal, D. M. Freeman, and V. Vaikuntanathan. Functional Encryption for Inner Product Predicates from Learning with Errors. In *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security Seoul, South Korea, December 4-8, 2011, Proceedings*, 21–40,2011.

[4] C. Aguilar, P. Gaborit, P. Lacharme, J. Schrek, and G. Zemor. Noisy Diffe-Hellman Protocols. PQC2010, Rump Session, 2010. `https://pqc2010.cased.de/rr/03.pdf`.

[5] E: Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2016/1157, 2016 `http://eprint.iacr.org/2016/1157`.

[6] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009, Proceedings*, 595–618, 2009

[7] J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila. Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE. Cryptology ePrint Archive, Report 2016/659,2016. `http://eprint.iacr.org/2016/659`.

[8] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. Cryptology ePrint Archive, Report 2014/599, 2014. `http://eprint.iacr.org/2014/599`.

[9] X. Boyen. Attribute-Based Functional Encryption on Lattices. In *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013, Proceedings*, 122–142, 2013.

[10] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012, Proceedings*, 868–886, 2012.

[11] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In *Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012*, 309–325, 2012.

[12] Z. Brakerski and V. Vaikuntanathan. Efficient Fully Homomorphic Encryption from (Standard) LWE. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS2011, Palm Springs, CA, USA, October 22-25, 2011*, 97–106,2011.

[13] J. A. Buchmann and H. C. Williams. A Key Exchange System Based on Real Quadratic Fields. In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, 335–343, 1989.

[14] R. Canetti, D. Dachman-Soled, V. Vaikuntanathan, and H. Wee. Efficient Password Authenticated Key Exchange via Oblivious Transfer. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proceedings*, 449–466, 2012

[15] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai Trees, or How to Delegate a Lattice Basis. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010, Proceedings*, 523–552, 2010.

[16] W. Diffie and M. E. Hellman. New directions in cryptography. In *IEEE Trans. Information Theory*, volume 22, number 6, 644–654, 1976.

[17] A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama. Strongly Secure Authenticated Key Exchange from Factoring, Codes,and Lattices. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proceedings*, 467–484, 2012.

[18] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, 197–206, 2008.

[19] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Attribute-based encryption for circuits. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, 545–554, 2013.

[20] J. Ding, X. Xie, and X. Lin. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem. Cryptology ePrint Archive, Report 2012/688, 2012. `http://eprint.iacr.org/2012/688`.

[21] J. Katz and V. Vaikuntanathan. Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices. In *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009, Proceedings*, 636–652, 2009.

[22] J. Katz and V. Vaikuntanathan. Round-Optimal Password-Based Authenticated Key Exchange. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011, Proceedings*, 293–310, 2011.

[23] R. Lindner and C. Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. In *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011, Proceedings*, 319–339, 2011.

[24] V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010, Proceedings*, 1–23, 2010.

[25] C. Peikert. Lattice Cryptography for the Internet. Cryptology ePrint Archive, Report 2014/070, 2014. `http://eprint.iacr.org/2014/070`.

[26] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, 84–93, 2005.

[27] R. L. Rivest, A. Shamir, and L. M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. In *Commun. ACM*, volume 21, number 2, 120–126, 1978.

From Minicrypt to Obfustopia via Private-Key Functional Encryption

Ilan Komargodski

(joint work with Gil Segev)

Functional encryption [15, 7, 14] allows tremendous flexibility when accessing encrypted data: Such encryption schemes support restricted decryption keys that allow users to learn specific functions of the encrypted data without leaking any additional information. We focus on the most general setting where the functional encryption schemes support an unbounded number of functional keys in the public-key setting, and an unbounded number of functional keys and ciphertexts in the private-key setting. In the public-key setting, it has been shown that functional encryption is essentially equivalent to indistinguishability obfuscation [3, 11, 1, 2, 6, 16].

When examining the various applications of functional encryption (see, for example, the survey by Boneh et al. [8]), it turns out that *private-key* functional encryption suffices in many interesting scenarios. However, although private-key functional encryption may seem significantly weaker than its public-key variant, constructions of private-key functional encryption schemes are currently known based only on public-key functional encryption.

We settle the problem of positioning private-key functional encryption within the hierarchy of cryptographic primitives by placing it in Obfustopia. First, given any *quasi-polynomially*-secure private-key functional encryption scheme, we construct a (quasi-polynomially-secure) indistinguishability obfuscator for circuits with inputs of poly-logarithmic length and sub-polynomial size.

Theorem 1 (Informal). *Assuming a quasi-polynomially-secure private-key functional encryption scheme for polynomial-size circuits, there exists an indistinguishability obfuscator for the class of circuits of size* $2^{(\log \lambda)^{\epsilon}}$ *with inputs of length* $(\log \lambda)^{1+\delta}$ *bits, for some positive constants* ϵ *and* δ.

Underlying our obfuscator is a new transformation from single-input functional encryption to multi-input functional encryption in the private-key setting. The previously known such transformation of Brakerski et al. [9] required a sub-exponentially-secure single-input scheme, and obtained a multi-input scheme supporting only a slightly super-constant number of inputs. Our transformation both relaxes the underlying assumption and supports more inputs: Given any quasi-polynomially-secure single-input scheme, we obtain a multi-input scheme supporting a poly-logarithmic number of inputs.

We demonstrate the wide applicability of our obfuscator by observing that it can be used to instantiate many natural applications of (full-fledged) indistinguishability obfuscation for polynomial-size circuits. We construct a public-key functional encryption scheme (based on [16]), and a hard-on-average distribution of instances of a PPAD-complete problem (based on [5]).

Theorem 2 (Informal)**.** *Assuming a quasi-polynomially-secure private-key functional encryption scheme for polynomial-size circuits, and a sub-exponentially-secure one-way function, there exists a public-key functional encryption scheme for the class of circuits of size* $2^{(\log\lambda)^\epsilon}$ *with inputs of length* $(\log\lambda)^{1+\delta}$ *bits, for some positive constants* ϵ *and* δ*.*

Theorem 3 (Informal)**.** *Assuming a quasi-polynomially-secure private-key functional encryption scheme for polynomial-size circuits, and a sub-exponentially-secure injective one-way function, there exists a hard-on-average distribution over instances of a PPAD-complete problem.*

Compared to the work of Bitansky at el. [4], Theorem 2 shows that private-key functional encryption implies not just public-key encryption but leads all the way to public-key functional encryption. Furthermore, in terms of underlying assumptions, whereas Bitansky et al. assume a sub-exponentially-secure private-key functional encryption scheme and a (nearly) exponentially-secure one-way function, we only assume a quasi-polynomially-secure private-key functional encryption scheme and a sub-exponentially-secure one-way function.

In addition, recall that average-case PPAD hardness was previously shown based on compact *public-key* functional encryption (or indistinguishability obfuscation) for polynomial-size circuits and one-way permutations [12]. We show average-case PPAD hardness based on quasi-polynomially-secure *private-key* functional encryption and sub-exponentially-secure injective one-way function. In fact, as shown by Hubáček and Yogev [13], our result (as well as [5, 12]) implies average-case hardness for CLS, a proper subclass of PPAD and PLS [10].

References

[1] P. Ananth and A. Jain. Indistinguishability obfuscation from compact functional encryption. In *Advances in Cryptology – CRYPTO '15*, 308–326, 2015.

[2] P. Ananth, A. Jain, and A. Sahai. Achieving compactness generically: Indistinguishability obfuscation from non-compact functional encryption. Cryptology ePrint Archive, Report 2015/730, 2015.

[3] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6, 2012.

[4] N. Bitansky, R. Nishimaki, A. Passelègue, and D. Wichs. From Cryptomania to Obfustopia through secret-key functional encryption. Cryptology ePrint Archive, Report 2016/558, 2016.

[5] N. Bitansky, O. Paneth, and A. Rosen. On the cryptographic hardness of finding a Nash equilibrium. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 1480–1498, 2015.

[6] N. Bitansky and V. Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 171–190, 2015.

[7] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In *Proceedings of the 8th Theory of Cryptography Conference*, 253–273, 2011.

[8] D. Boneh, A. Sahai, and B. Waters. Functional encryption: A new vision for public-key cryptography. *Communiations of the ACM*, 55(11):56–64, 2012.

[9] Z. Brakerski, I. Komargodski, and G. Segev. Multi-input functional encryption in the private-key setting: Stronger security from weaker assumptions. In *Advances in Cryptology – EUROCRYPT '16*, 852–880, 2016.

[10] C. Daskalakis and C. H. Papadimitriou. Continuous local search. In *Proceedings of the 22nd Annual ACM-SIAM Symposium on Discrete Algorithms*, 790–804, 2011.

[11] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science*, 40–49, 2013.

[12] S. Garg, O. Pandey, and A. Srinivasan. Revisiting the cryptographic hardness of finding a Nash equilibrium. In *Advances in Cryptology – CRYPTO '16*, 579–604, 2016.

[13] P. Hubáček and E. Yogev. Hardness of continuous local search: Query complexity and cryptographic lower bounds. *Electronic Colloquium on Computational Complexity*, 23:63, 2016.

[14] A. O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010.

[15] A. Sahai and B. Waters. Slides on functional encryption. Available at `http://www.cs.utexas.edu/~bwaters/presentations/files/functional.ppt`, 2008.

[16] B. Waters. A punctured programming approach to adaptively secure functional encryption. In *Advances in Cryptology – CRYPTO '15*, 678–697, 2015.

Average-Case Fine-Grained Hardness, and what to do with it

Prashant Vasudevan

(joint work with Marshall Ball, Alon Rosen, Manuel Sabin)

We present functions that are hard to compute on average for algorithms running in some fixed polynomial time, assuming widely-conjectured worst-case hardness of certain problems from the study of fine-grained complexity.

We discuss the relevance of such average-case hardness to cryptography and present, as an illustration, an outline of a proof-of-work protocol constructed based on the hardness and certain structural properties of our functions.

The Journey from NP to TFNP Hardness

Moni Naor

We discussed how to how that there are hard problems in the complexity class TFNP- Total Function NP. For this class hardness results based on one way permutations or collision resistant hash functions. On the other hand there are all sorts of barriers for showing reductions based on P $\neq$ NP. We prove hardness based on hard-on-the-average problems in NP (joint work with Eylon Yogev and Pavel Hubácek). On related work we considered the complexity of the Ramsey problem. It was known to be hard for a graph based algorithm. Based on CRH we showed hardness when one is given a program for computing a graph.

Homomorphic Secret Sharing, Part I: Function Secret Sharing from One-Way Functions

Yuval Ishai
(joint work with Elette Boyle and Niv Gilboa)

Fully homomorphic encryption (FHE) is a powerful cryptographic tool that can be used to minimize the communication complexity of secure computation protocols. However, known FHE schemes rely on a relatively narrow set of assumptions and algebraic structures that are all related to lattices. Moreover, the efficiency of known FHE schemes still leaves much to be desired.

This two-part talk covers new techniques for succinct secure computation. The idea is to replace FHE by "homomorphic secret sharing" (HSS), which allows a compact evaluation of a function on a secret shared input, and construct HSS schemes for useful function classes in a way that gets around some of the limitations of known FHE schemes.

The first part covers constructions of Function Secret Sharing (FSS) schemes for simple function classes from one-way functions. FSS can be viewed as a dual version of HSS, where the roles of the function and input are reversed. More concretely, the goal of FSS is to split a function f into succinctly described $f_1, \ldots, f_m$, such that $f(x) = f_1(x) + \ldots + f_m(x)$ for every input x, and every strict subset of the f_i computationally hides f. We present efficient constructions of FSS schemes for point functions and decision trees based on any pseudo-random generator, and survey applications of these constructions in the context of efficient secure access to remote data and secure multi-party computation. The material of this part of the talk is based on [1, 2].

A big open question in the area is that of characterizing the function classes for which efficient FSS schemes can be based on one-way functions, or, more generally, understand the necessary and sufficient cryptographic assumptions for useful instances of FSS. A more concrete open question is the efficiency of one-way function based constructions of FSS schemes for the class of point functions in the case of $m \geq 3$ parties. The best construction from [1] achieves a near-quadratic improvement over the naive solution of secret sharing the truth-table.

References

[1] E. Boyle, N. Gilboa, and Y. Ishai. Function secret sharing. In *EUROCRYPT 2015*, pages 337–367, 2015.

[2] E. Boyle, N. Gilboa, and Y. Ishai. Function secret sharing: Improvements and extensions. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1292-1303, 2016.

Homomorphic Secret Sharing, Part II: Succinct and Round-Efficient Secure Computation from DDH

Elette Boyle
(joint work with Niv Gilboa and Yuval Ishai)

Fully homomorphic encryption (FHE) is a powerful cryptographic tool that can be used to minimize the communication complexity of secure computation protocols. However, known FHE schemes rely on a relatively narrow set of assumptions and algebraic structures that are all related to lattices. Moreover, the efficiency of known FHE schemes still leaves much to be desired.

This two-part talk covers new techniques for succinct secure computation. The idea is to replace FHE by “homomorphic secret sharing” (HSS), which allows a compact evaluation of a function on a secret shared input, and construct HSS schemes for useful function classes in a way that gets around some of the limitations of known FHE schemes.

The second part of the talk presents a construction of a powerful HSS scheme based on discrete-log-type assumptions. More concretely, under the Decisional Diffie-Hellman (DDH) assumption, we construct a 2-out-of-2 secret sharing scheme that supports a compact evaluation of branching programs on the shares. In fact, the output of the homomorphic evaluation is *additively* shared between the parties. We survey different applications of this HSS scheme, including succinct secure computation for NC^1, two-round secure multiparty computation parties, and other DDH-based applications that previously required FHE. The material of this part of the talk is based on [2, 3].

This work gives rise to several interesting open questions. While HSS for all polynomial-time computable functions can be based on the Learning with Errors (LWE) assumption via special types of FHE [1, 4], obtaining a similar result under DDH or other cryptographic assumptions is open. Our DDH-based HSS scheme has an inverse-polynomial error probability, where the running time of the evaluation algorithm grows linearly with the inverse of the error probability. An interesting open question is to eliminate this error or improve the dependence of the running time on the error. Another open question is to obtain similar results for the case of 3 or more parties. Finally, our 2-round protocol for general secure multiparty computation has two limitations that we would like to eliminate: it requires a Public Key Infrastructure (PKI) setup, and it is only efficient when the number of parties is constant.

References

[1] E. Boyle, N. Gilboa, and Y. Ishai. Function secret sharing. In *EUROCRYPT 2015*, pages 337–367, 2015.

[2] E. Boyle, N. Gilboa, and Y. Ishai. Breaking the circuit size barrier for secure computation under DDH. In *Proceedings of CRYPTO 2016, Part I*, pages 509–539, 2016. Full version: IACR Cryptology ePrint Archive 2016: 585 (2016).

[3] E. Boyle, N. Gilboa, and Y. Ishai. Group-based secure computation: Optimizing rounds, communication, and computation. In *Proceedings of Eurocrypt 2017*, to appear.

[4] Y. Dodis, S. Halevi, R. D. Rothblum, and D. Wichs. Spooky Encryption and Its Applications. In *Proc. CRYPTO 2016, Part III*, pages 93–122, 2016.

Equivocating Yao: Constant-Round Adaptively Secure Multiparty Computation in the Plain Model

Muthuramakrishnan Venkitasubramaniam

Yao's circuit garbling scheme is one of the basic building blocks of cryptographic protocol design. Originally designed to enable two-message, two-party secure computation, the scheme has been extended in many ways and has innumerable applications. Still a basic question has remained open throughout the years. Can the scheme be extended to guarantee security inf ace of an adversary that corrupts both parties, adaptively,a s the computation proceeds.

We answer this question in the affirmative. We define a new type of encryption called functionally equivocal encryption (FEE) and show that when Yao's scheme is implemented with an FEE as the underlying encryption mechanism, it becomes secure against adaptive adversaries. We then show how to implement FEE from any one-way function.

Techniques in Lattice-based Cryptography

Vinod Vaikuntanathan

Many recent constructions of advanced lattice-based primitives such as attribute-based encryption, fully homomorphic encryption and signatures, predicate encryption and constrained pseudorandom functions rely on a handful of techniques that play with the learning with errors (LWE) problem and lattice trapdoors. We will present them and show as many constructions as time permits.

Revisiting Non-Malleable Commitments

Rafail Ostrovsky

(joint work with Michele Ciampi, Luisa Siniscalchi, Ivan Visconti)

Commitment schemes are a fundamental primitive in Cryptography. These schemes are protocols between two players: sender and the receiver. There exist two phases, a commitment phase and a decommitment phase. In the commitment phase the sender, with a secret input m, interacts with the receiver. In the end of this interaction we say that a *commitment* of the message m has been computed. Moreover the receiver still does not know what m is (i.e. m is hidden) and at the same time the sender during the decommitment phase can subsequently opens this commitment only to m.

In our work we consider the intriguing question of constructing round-efficient schemes that remain secure even against man-in-the-middle (MiM) attacks: non-malleable (NM) commitments [DDN91]. The round complexity of NM commitments after 25 years of research remains a fascinating open question. The original construction of [DDN91] required a logarithmic number of rounds and the sole use of one-way functions (OWFs). Then, through a long sequence of very exciting positive results [Bar02, PR05, PW10, LP11, Goy11, GLOV12], the above open question has been in part solved obtaining a constant-round (even concurrent) NM commitment scheme by using any OWF in a black-box fashion. On the negative side, Pass proved that NM commitments require at least 3 rounds [Pas13] when security is proved through a black-box reduction to falsifiable (polynomial or subexponential time) hardness assumptions.

More recently forward steps to reduce the round complexity has been made in [GRRV14, GPR16] but only for the (simpler) one-one case (i.e., just one sender and one receiver). In particular, Goyal et al. [GRRV14] showed a *one-one* 4-round NM commitment scheme based on OWFs only. The initial version of [GRRV14] claims concurrent non-malleability. Later on we have found an error in their security proof of the one-one and of the one-many cases (that also applies to the construction of [BGR$^+$15]). The claim on concurrent non-malleability has then been withdrawn in the recent eprint version of [GRRV14] where a variation of their original scheme is presented and proved one-one non-malleable. The more recent work of Goyal et al. [GPR16] shows a 3-round one-one NM commitment scheme based on the black-box use of any 1-to-1 OWF. This claim has however been withdrawn in [GPR15]. Two very recent results of Ciampi et al. [COSV16b, COSV16a] obtain in 3 round, respectively, a concurrent non-malleable commitment and one-one non-malleabile commitment schemes. These constructions both rely on one-way permutations secure against subexponential-time adversaries.

Our Results. We show a 4-round concurrent non-malleable commitment scheme based on the sole existence of OWFs, therefore solving a problem explicitly left open by [GRRV14]. We achieve this result combining two following two notions. 1) We define a new security notion for argument systems on unique-witness instances w.r.t. MiM attacks that we refer to as simulation-witness-independence (SimWI). 2) We consider a weaker form of non-malleability, *weak non-malleability* (wNM), where the MiM is restricted to playing well-formed commitments in the right sessions when receiving well formed commitments from the left sessions.

In our work we construct a 4-round one-many SimWI argument of knowledge (AoK) for unique-witness instances by relying on OWFs only and we prove that a subprotocol of [GRRV14] is a 4-round statistically binding concurrent wNM commitment scheme from OWF. Finally putting these two gadgets together we obtaining our main result: a 4-round concurrent non-malleable commitment scheme. The recent state of the art is summarized in Table 1.

We leave open two important questions. 1) The existence of 3-round concurrent NM commitment from falsifiable assumption against polynomial-time adversaries.

Paper	Rounds	Assumption	Concurrency
Goyal,/ Lin and Pass STOC 2011	≥ 6	OWFs	Yes
Goyal et al., FOCS 2012	≥ 6	BB OWFs	Yes
Goyal et al., FOCS 2014	4	OWFs	No
Ciampi et al + ePrint 2016 Ciampi et al., CRYPTO 2016	3	subexp OWPs	Yes
Our result	4	OWFs	Yes
Goyal et al., STOC 2016	3	BB subexp OWPs	No

Table 1. Comparison with recent positive results.

2) The existence of 4-round fully adaptive-input one-many SimWI argument systems from OWFs.

References

[Bar02] Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. In *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*, 345–355, 2002.

[BGR+15] Hai Brenner, Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. Fast non-malleable commitments. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, 1048–1057, 2015.

[COSV16a] Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. 4-round concurrent non-malleable commitments from one-way functions. Cryptology ePrint Archive, Report 2016/621, 2016. `http://eprint.iacr.org/2016/621`.

[COSV16b] Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Concurrent non-malleable commitments (and more) in 3 rounds. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, 270–299. Springer, 2016.

[CPS+16a] Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti. Improved or-composition of sigma-protocols. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II*, volume 9563 of *Lecture Notes in Computer Science*, 112–141. Springer, 2016.

[CPS+16b] Michele Ciampi, Giuseppe Persiano, Alessandra Scafuro, Luisa Siniscalchi, and Ivan Visconti. Online/offline OR composition of sigma protocols. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, 63–92. Springer, 2016.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, 542–552, 1991.

[GLOV12] Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, and Ivan Visconti. Constructing non-malleable commitments: A black-box approach. In *53rd Annual IEEE Symposium* *on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, 51–60, 2012.

[Goy11] Vipul Goyal. Constant round non-malleable protocols using one way functions. In *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, 695–704, 2011.

[GPR15] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. Cryptology ePrint Archive, Report 2015/1178, 2015. `http://eprint.iacr.org/2015/1178`, Last update: 29-Dec-2016.

[GPR16] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, 1128–1141, 2016.

[GRRV14] Vipul Goyal, Silas Richelson, Alon Rosen, and Margarita Vald. An algebraic approach to non-malleability. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, 41–50, 2014. Full version: Cryptology ePrint Archive, Report 2014/586, Version 20160915:132957 (posted 15-Sep-2016 13:29:57 UTC.

[LP11] Huijia Lin and Rafael Pass. Constant-round non-malleable commitments from any one-way function. In Lance Fortnow and Salil P. Vadhan, editors, *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, 705–714. ACM, 2011.

[Pas13] Rafael Pass. Unprovable security of perfect NIZK and non-interactive non-malleable commitments. In *TCC*, 334–354, 2013.

[PR05] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, 533–542, 2005.

[PW10] Rafael Pass and Hoeteck Wee. Constant-round non-malleable commitments from sub-exponential one-way functions. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, 638–655, 2010.

Practical Key Exchange with Forward Secrecy from Coding Theory

Nicolas Sendrier

1. Introduction

Quasi-Cyclic Moderate Density Parity Check (QC-MDPC) codes allows the design [6] of McEliece-like encryption schemes [5]. Those variants have several advantages, among which

(1) shorter public keys,
(2) a good security reduction.

2. QC-MDPC-McEliece

2.1. **Shorter Keys.** Using quasi-cyclic codes for the McEliece encryption scheme was first proposed by Gaborit [2]. Generator and parity check matrices of quasi-cyclic codes are block circulant and can thus be fully described by giving one or a few rows instead of the whole matrix. The quasi-cyclic codes that we consider here are of length $n = 2p$ with index 2. This means that any generator or parity check matrix can be written in the form $(A \mid B)$ where A and B are $p \times p$ circulant matrices (each row is the cyclic shift of the previous one) and is entirely described by its first row (a, b), a vector of length $2p$.

Moreover, binary $p \times p$ circulant matrices are isomorphic to $\mathcal{R}_p = \mathbf{F}_2[x]/(x^p - 1)$ and thus most statements can be written in terms of polynomials instead of codes or matrices.

2.2. **QC-MDPC codes.** A binary MDPC code admits a sparse parity check matrix H whose rows have a (small) Hamming weight w. A QC-MDPC code of index 2 admits a sparse parity check matrix $H = (H_0, H_1)$ and is fully described by the two sparse circulant blocks H_0 and H_1, or equivalently by two sparse polynomial h_0 and h_1 in $\mathcal{R}_p$. To decode t errors in such a code, one has to solve the following problem ($|\cdot|$ the Hamming weight)

Problem 1 (QC-MDPC Decoding).

input: $s, h_0, h_1 \in \mathcal{R}_p$ with $|h_0| = |h_1| = w/2$

output: $e_0, e_1 \in \mathcal{R}_p$ such that $e_0 h_0 + e_1 h_1 = s$ and $|e_0| + |e_1| \leq t$

This problem can be solved with Gallager's bit flipping algorithm for LDPC codes [3]. The algorithm succeeds with high probability as long as $w \simeq \sqrt{2p}$ and $t \simeq \sqrt{2p}$. Some suitable values of p, w, t are given at the end of this abstract. In Figure 1 we describe the QC-MDPC-McEliece variant in terms of polynomials. The decryption can be achieved with Gallager's algorithm.

Parameters: block size p, row weight w, error weight t, $\mathcal{R}_p = \mathbf{F}_2[x]/(x^p - 1)$
(p a prime, w even, $w/2$ odd, w and t are close to $\sqrt{2p}$)

Key Generation: pick h_0 and h_1 in $\mathcal{R}_p$ both of Hamming weight $w/2$
public key: $g = h_1 h_0^{-1}$
private key: h_0, h_1

Encryption: $\mathcal{R}_p \to \mathcal{R}_p \times \mathcal{R}_p$
$m \mapsto (mg + e_0, m + e_1)$ with $|e_0| + |e_1| = t$

Decryption: given a ciphertext (u_0, u_1)
solve $u_0 h_0 + u_1 h_1 = e_0 h_0 + e_1 h_1$ with $|e_0| + |e_1| \leq t$

Figure 1. QC-MDPC-McEliece Scheme

3. Security Reduction

Following [7], the system is secure on average as long as two assumptions hold:

(1) Decoding t error in a binary quasi-cyclic $[2p, p]$ code is hard on average.
(2) The public key is indistinguishable from a random block circulant matrix of same size.

Those assumptions relate to the following two problems

Problem 2 (QC Generic Decoding).
input: $s, h \in \mathcal{R}_p$, an integer t
output: $e_0, e_1 \in \mathcal{R}_p$ such that $e_0 + e_1 h = s$ and $|e_0| + |e_1| \leq t$

Problem 3 (QC Codeword Weight).
input: $h \in \mathcal{R}_p$, an integer w
question: is there $h_0, h_1 \in \mathcal{R}_p \setminus \{0\}$ such that $h_0 + h_1 h = 0$ and $|h_0| + |h_1| \leq w$?

The Problem 2 is the generic decoding of (index 2) quasi-cyclic codes. It is NP, but its completeness status is unknown. It is widely admitted that the problem is hard on average.

Open problem: extend Alekhnovich's hardness results on average case decoding [1] to the quasi-cyclic case.

The Problem 3 relates to the indistinguishability of QC-MDPC codes. It is worth noting that the two statements are very similar. More, all known algorithms that can solve Problem 3 can solve Problem 2 for essentially the same cost. Even more, in the non quasi-cyclic setting, decoding and finding a word of small weight in a linear code are equivalently hard.

Open problem: prove that Problems 2 and 3 are polynomially equivalent.

4. Key Exchange for QC-MDPC codes

A key agreement procedure easily derives from QC-MDPC-McEliece (see Figure 2). At the end of the protocol, Alice and Bob share the secret error pattern e_0, e_1. The protocol security reduces to the two above problems. In addition, since key generation is easy one can use ephemeral key pairs with two nice features: (1) forward secrecy (if one instance of the protocol is compromised it does not affect past executions), and (2) less vulnerability to side channel attacks (as [4] which exploits decoding failures).

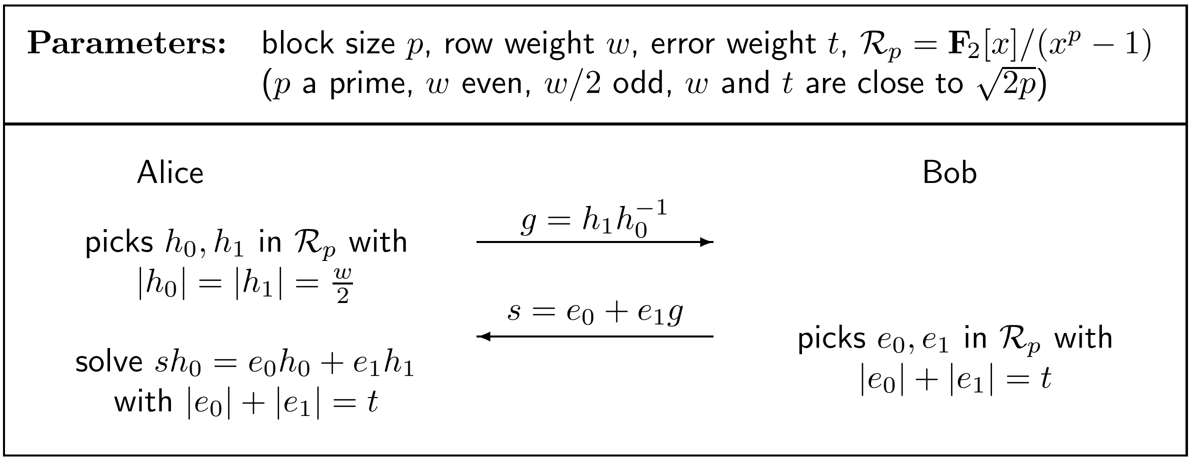
Parameters: block size p, row weight w, error weight t, $\mathcal{R}_p = \mathbf{F}_2[x]/(x^p - 1)$
(p a prime, w even, $w/2$ odd, w and t are close to $\sqrt{2p}$)
Alice
Bob
picks h_0, h_1 in $\mathcal{R}_p$ with $|h_0| = |h_1| = \frac{w}{2}$
$g = h_1 h_0^{-1}$
$s = e_0 + e_1 g$
picks e_0, e_1 in $\mathcal{R}_p$ with $|e_0| + |e_1| = t$
solve $sh_0 = e_0 h_0 + e_1 h_1$ with $|e_0| + |e_1| = t$

Figure 2. QC-MDPC Key Exchange Protocol (Sketch)

4.1. **Parameters.** Parameter selection requires some work. One has to make sure, through analysis and simulations that the designed number of errors can be corrected with high probability. The following table gives some possible values.

security	block size, p	w	t
80 bits	4801	90	84
128 bits	9857	142	134
256 bits	32771	274	264

References

[1] Michael Alekhnovich. More on average case vs approximation complexity. In *FOCS 2003*, 298–307. IEEE, 2003.

[2] P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of WCC 2005*, 81–90, 2005.

[3] Robert G. Gallager. *Low-Density Parity-Check Codes.* M.I.T. Press, 1963.

[4] Qian Guo, Thomas Johansson, and Paul Stankovski. A key recovery attack on MDPC with CCA security using decoding errors. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016*, volume 10031 of *LNCS*, 789–818. Springer, December 2016.

[5] R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol., Pasadena, CA*, 114–116, January 1978.

[6] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *IEEE Conference, ISIT 2013*, 2069–2073, Instanbul, Turkey, July 2013.

[7] N. Sendrier. On the use of structured codes in code based cryptography. In S. Nikova, B. Preneel, and L. Storme, editors, *Coding Theory and Cryptography III*, Contactforum, 59–68. Koninklijke Vlaamse Academie van België voor Wetenschaeppen en Kunsten, 2009.

Short Generators Without Quantum Computers: The Case of Multiquadratics

Daniel J. Bernstein, Christine van Vredendaal

Finding a short element g of a number field, given the ideal generated by g is a classic problem in computational algebraic number theory. Solving this problem recovers the private key in cryptosystems introduced by e.g. Buchmann-Maurer-Mller, Gentry, Smart-Vercauteren, Gentry-Halevi, and Garg-Gentry-Halevi. Work over te last ten years has shown that for some number fields this problem has a surprisingly low post-quantum security level. In this talk we will present an algorithm showing that for multiquadratic number fields this problem has a surprisingly low pre-quantum security level. Experimental results confirm the analysis.

Interactive Coding with Nearly Optimal Round and Communication Blowup

Yael Tauman Kalai
(joint work with Klim Efremenko, Elad Haramaty)

The problem of constructing error-resilient interactive protocols was introduced in the seminal works of Schulman (FOCS 1992, STOC 1993). These works show how to convert any two-party interactive protocol into one that is resilient to constant-fraction of error, while blowing up the communication by only a constant factor. Since these seminal works, there have been many follow-up works which improve the error rate, the communication rate, and the computational efficiency.

All these works assume that in the underlying protocol in each round each party sends a single bit. This assumption is without loss of generality, since one can efficiently convert any protocol into one which sends one bit per round. However, this conversion may cause a substantial increase in *round* complexity, which is what we wish to minimize in this work. Moreover, all previous works assume that the communication complexity of the underlying protocol is *fixed* and a priori known, an assumption that we wish to remove.

In this work, we consider protocols whose messages may be of *arbitrary* lengths, and where the length of each message and the length of the protocol may be *adaptive*, and may depend on the private inputs of the parties and on previous communication. We show how to efficiently convert any such protocol into another protocol with comparable efficiency guarantees, that is resilient to adversarial error (for some fixed constant e¿0), while blowing up both the *communication* complexity and the *round* complexity by at most a constant factor. As opposed to most previous work, our error model not only allows the adversary to toggle with the corrupted bits, but also allows the adversary to *insert* and *delete* bits. In addition, our transformation preserves the computational efficiency of the protocol. Finally, we try to minimize the blowup parameters, and give evidence that our parameters are nearly optimal.

References

[1] L. J. Schulman. Communication on Noisy Channels: A Coding Theorem for Computation. In *33rd Annual Symposium on Foundations of Computer Science, Pittsburgh, Pennsylvania, USA, 24-27 October 1992*, 724–733.

[2] L. J. Schulman. Deterministic coding for interactive communication. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, May 16-18, 1993, San Diego, CA, USA*, 747–756.

Privacy Preserving Search of Similar Patients in Genomic Data

Tal Rabin

We described the results of the iDash Competition which we participated in. Showing the approximation algorithm that was optimized for the multiparty computation.

Revisiting the NP-Hardness of Lattice Problems

Silas Richelson

In this talk we state what is known about the NP-hardness of the two most well studied computational lattice problems: *shortest vector problem* (SVP) and the *closest vector problem* (CVP). Despite the syntactic similarities between SVP and CVP, currently hardness of approximation theorems for SVP are proven very differently than theorems for CVP. Proving hardness of CVP is easier and techniques used for CVP break down for SVP. This results in SVP having slightly worse approximation factors, randomized reductions and more complicated and difficult proofs. In this talk we will survey what is known and we present a framework for reductions to SVP which, if instantiated, would yield a hardness of approximation theorem for SVP analogous to what is currently known for CVP.

References

[1] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The Hardness of Approximate Optimia in Lattices, Codes, and Systems of Linear Equations. In *34th Annual Symposium on Foundations of Computer Science, Palo Alto, California, USA, 3-5 November 1993*, 724–733, 1993.

[2] I. Dinur, G. Kindler, R. Raz. and S. Safra Approximating CVP to Within Almost-Polynomial Factors is NP-Hard. In *Combinatorica*, volume 23, number 2, 205–243, 2003.

[3] D. Micciancio. The Shortest Vector in a Lattice is Hard to Approximate to Within Some Constant. In *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*, 92–98, 1998.

[4] S. Khot Hardness of Approximating the Shortest Vector Problem in Lattices. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, 126–135, 2004.

[5] I. Haviv and O. Regev Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, 469–477, 2007.

Cryptography with Updates

Aloni Cohen

(joint work with Prabhanjan Ananth and Abhishek Jain)

The last decade has seen the advent of a vast array of advanced cryptographic primitives such as attribute-based encryption [1, 2], predicate encryption [3, 4, 5, 6], fully homomorphic encryption [7], fully homomorphic signatures [8, 9, 10], functional encryption [1, 11, 12, 13], constrained pseudorandom functions [14, 15, 16], witness encryption [17, 18], witness PRFs [19], indistinguishability obfuscation [20, 21], and many more. Most of these primitives can be viewed as "cryptographic circuit compilers" where a circuit C can be compiled into an encoding $\langle C\rangle$ and an input x can be encoded as $\langle x\rangle$ such that they can be evaluated together to compute $C(x)$. For example, in a functional encryption scheme, circuit compilation corresponds to the key generation process whereas input encoding corresponds to encryption. Over the recent years, cryptographic circuit compilers have revolutionized cryptography by providing non-interactive means of computing over inputs/data.

A fundamental limitation of these circuit compilers is that they only support *static* compilation. That is, once a circuit is compiled, it can no longer be modified. In reality, however, compiled circuits may need to undergo several updates over a period of time. For example, consider an organization where each employee is issued a decryption key SK_P of an attribute-based encryption scheme where the predicate P corresponds to her access level determined by her employment status. However, if her employment status later changes, then we would want to update the predicate P associated with her decryption key. Known schemes, unfortunately, do not support this ability.

Motivated by the necessity of supporting updates in applications, in this work, we study and build *dynamic* circuit compilers. In a dynamic circuit compiler, it is possible to update a compiled circuit $\langle C \rangle$ into another compiled circuit $\langle C' \rangle$ by using an *encoded update string* whose size only depends on the "difference" between the plaintext circuits C and C'. For example, if the difference between C and C' is simply a single gate change, then this should be reflected in the size of the encoded update. Note that this rules out the trivial solution of simply releasing a new compiled circuit at the time of update.

Background: Incremental Cryptography. The study of cryptography with updates was initiated by Bellare, Goldreich and Goldwasser [22] under the umbrella of *incremental cryptography.* They studied the problem of incremental digital signatures, where given a signature of a message m, it should be possible to efficiently compute a signature of a related message m', without having to recompute the signature of m' from scratch. Following their work, the study of incremental cryptography was extended to other basic cryptographic primitives such as encryption and hash functions [22, 23, 25, 24, 26, 27, 28], and more recently, indistinguishability obfuscation [29, 30].

Our Goal. In this work, we continue this line of research, and perform a systematic study of updatable cryptographic primitives. We take a unified approach towards adding updatability features to recently studied primitives such as attribute-based encryption, functional encryption and more generally, cryptographic circuit compilers. We, in fact, go further and also study updatability for classical protocols such as zero-knowledge proofs and secure multiparty computation.

To accomplish this goal, we introduce a new notion of *updatable randomized encodings* that extends the standard notion of randomized encoding [31] to incorporate updatability features. We show that updatable randomized encodings can be used to generically transform cryptographic primitives (discussed above) to their updatable counterparts.

Updatable Randomized Encodings. The notion of randomized encoding [31] allows one to encode a "complex" computation $C(x)$ into a "simple" randomized function $\mathsf{Encode}(C, x; r)$ such that given its output $\langle C(x) \rangle$, it is possible to evaluate a public Decode algorithm to recover the value $C(x)$ without learning anything else about C and x. The typical measure of "simplicity" studied in the literature dictates that the parallel-time complexity of the Encode procedure be smaller than that of computing $C(x)$. Such randomized encodings are known to exist for general circuits based on only one-way functions [32] (also referred to as Yao's garbled circuits [33], where the encoding complexity is in $\mathbf{NC}^1$).

In this work, we study *updatable* randomized encodings (URE): given a randomized encoding $\langle C(x)\rangle$ of $C(x)$, we want the ability to update it to an encoding $\langle C'(x')\rangle$ of $C'(x')$, where C' and x' are derived from C and x by applying some update $\mathbf{u}$. We require that the update $\mathbf{u}$ can be encoded as $\langle \mathbf{u}\rangle$ which can then be used to transform $\langle C(x)\rangle$ into $\langle C'(x')\rangle$, a randomized encoding of $C'(x')$.

The key efficiency requirement is that the running time of the GenUpd algorithm must be a fixed polynomial in the security parameter and the size of the update, and independent of the size of the circuit and input being updated. This, in particular, implies that the size of an update encoding $\langle \mathbf{u}\rangle$ is also a fixed polynomial in the security parameter and the size of $\mathbf{u}$.

Constructions. In this work, we initiate the study of updatable randomized encodings. Our first result is a construction of multi-evaluation URE for general circuits that supports an unbounded polynomial number of sequential updates. The underlying assumption is a secret-key compact functional encryption scheme for general circuits that supports a single function key query. For the case of polynomially bounded updates, we can, in fact, relax our assumption to only *one-way functions*. We obtain this result by using a single-key compact secret-key FE scheme for an a priori *bounded* number of ciphertexts that is constructed from one-way functions [34, 35].

To the best of our knowledge, such an FE scheme has not been explicitly stated in the literature. However, it follows easily from prior work. Very roughly, a modified version of [34] FE scheme where the encryption and key generation algorithms are "flipped" yields a compact secret-key FE scheme with security for a single ciphertext based on one-way functions. We additionally construct updatable garbled circuits that supports an unbounded number of sequential updates from the family of bit-wise updates. We build such a scheme from worst-case lattice assumptions.

At the heart of this result is a new notion of *puncturable symmetric proxy re-encryption scheme* that extends the well-studied notion of proxy re-encryption [36]. For the case of polynomially bounded updates, we can relax our assumption to only *one-way functions*. We obtain this result by using a puncturable PRF scheme that can be based on one-way functions [37, 38].

Applications. We show how to use URE to transform any (key-policy) attribute-based encryption (ABE) scheme into *updatable ABE*. The same idea can be used in a generic way to build dynamic circuit compilers and obtain updatable functional encryption, updatable indistinguishability obfuscation, and so on. We describe two concrete applications, namely, *updatable non-interactive zero-knowledge proofs* (UNIZK) and *updatable multiparty computation* (UMPC). A notable feature of these constructions is that they only require a URE scheme with *non-output-compact* updates and simulation-based security. Below, we briefly describe our main idea for constructing UNIZKs.

References

[1] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *roceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, 89–98.

[3] D. Boneh and B.Waters. Conjunctive, subset, and range queries on encrypted data. In *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings*, 535–554.

[4] E. Shi, J. Bethencourt, T. Chan, D. Song, and A. Perrig. Multi-dimensional range query over encrypted data. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*, 350–364.

[5] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings* , 146–162.

[6] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Predicate encryption for circuits from LWE. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, 503–523.

[7] C. Gentry. Computing on encrypted data. In *Cryptology and Network Security, 8th International Conference, CANS2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*, 477–477.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song. Provable data possession at untrusted stores. ACM conference on Computer and communications security (2007), 598–609.

[9] D. Boneh and D. M. Freeman. Homomorphic signatures for polynomial functions. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011, Proceedings*, 149–168.

[10] S. Gorbunov, V. Vaikuntanathan, D. Wichs. Leveled Fully Homomorphic Signatures from Standard Lattices. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, 469–477.

[11] D. Boneh, A. Sahai, B. Waters. Functional Encryption: Definitions and Challenges. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC2011, Providence, RI, USA, March 28-30, 2011, Proceedings*, 253–273.

[12] A. O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010.

[13] S. Goldwasser, S. D. Gordon, V. Goyal, A. Jain, J. Katz, F. -H. Liu, A. Sahai, E. Shi, H. -S. Zhou. Multi-input Functional Encryption. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014, Proceedings*, 578–602.

[14] D. Boneh and B. Waters. Constrained Pseudorandom Functions and Their Applications. In *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II*, 280–300.

[15] E. Boyle, S. Goldwasser, and I. Ivan. Functional Signatures and Pseudorandom Functions. In *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014, Proceedings*, 501–519.

[16] A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias. Delegatable pseudorandom functions and applications. In *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, 669–68.

[17] S. Garg, C. Gentry, A. Sahai, B. Waters. Witness encryption and its applications. *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, 467–476.

[18] C. Gentry, A. B. Lewko, B. Waters. Witness Encryption from Instance Independent Assumptions. *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, 426–443.

[19] Mark Zhandry. How to Avoid Obfuscation Using Witness PRFs. In *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II*, 421–448.

[20] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, 1–18, 2001.

[21] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, 40–49.

[22] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental Cryptography: The Case of Hashing and Signing. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, 216–233.

[23] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental cryptography and application to virus protection. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, 29 May-1 June 1995, Las Vegas, Nevada, USA*, 45–56.

[24] M. Fischlin. Incremental Cryptography and Memory Checkers. In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, 293–408.

[25] Da. Micciancio. Oblivious Data Structures: Applications to Cryptography In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997*, 456–464.

[26] M. Bellare and D. Micciancio. A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost. In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, 163–192.

[27] E. Buonanno, J. Katz, and M. Yung. Incremental Unforgeable Encryption. *Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers*, 109–124.

[28] I. Mironov, O. Pandey, O. Reingold, and G. Segev. Incremental Deterministic Public-Key Encryption. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings* , 628–644.

[29] S. Garg, O. Pandey. Incremental Program Obfuscation. Cryptology ePrint Archive, Report 2015/997.

[30] P. Ananth, A. Jain, and A. Sahai. Achieving Compactness Generically: Indistinguishability Obfuscation from Non-Compact Functional Encryption. Cryptology ePrint Archive, Report 2015/730.

[31] Y. Ishai and E. Kushilevitz. Randomizing Polynomials: A New Representation with Applications to Round-Efficient Secure Computation. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, 294–304.

[32] B. Applebaum, Y. Ishai, and E. Kushilevitz. Computationally Private Randomizing Polynomials and Their Applications. In *Computational Complexity*, **15(2)**, 115–162, 2006.

[33] A. Yao. How to Generate and Exchange Secrets. *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986* 162–167.

[34] A. Sahai and H. Seyalioglu. Worry-free encryption: functional encryption with public keys. In *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, 463–472.

[35] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Functional Encryption with Bounded Collusions via Multi-party Computation. In *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, 162–179.

[36] M. Blaze, G. Bleumer, and M. Strauss. Divertible Protocols and Atomic Proxy Cryptography In *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, 127–144.

[37] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions (Extended Abstract). FOCS (1984), 464–479.

[38] A. Sahai and B. Waters: How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, 2014 475–484.

The Hybrid Lattice-Reduction and Meet-in-the-Middle Attack: Improved Analysis and New Directions

Thomas Wunderer

(joint work with Florian Göpfert, Christine van Vredendaal)

Over the past decade, the hybrid lattice reduction and meet-in-the middle attack [14] (called the Hybrid Attack in the following) has been used to evaluate the security of many lattice-based cryptographic schemes such as the NTRU encryption scheme [13, 14, 11, 10, 12, 19], its recently proposed variant NTRU prime [2], a lightweight encryption scheme based on Ring-LWE with binary error [6, 5], and the signature schemes BLISS [7] and GLP [9, 7]. However, unfortunately none of the previous runtime analyses of the Hybrid Attack is entirely satisfactory: they are based on simplifying assumptions that may distort the security estimates. Such simplifying assumptions include setting probabilities equal to 1, which, for the parameter sets that have been analyzed in previous works, are in fact as small as 2^{-80}. Many of these assumptions lead to underestimating the scheme's security. However, some lead to security overestimates, and without further analysis, it is not clear which is the case. Therefore, the current security estimates against the Hybrid Attack are not reliable and the actual security levels of many lattice-based schemes are unclear.

In our work [21], we present a unified framework for the Hybrid Attack and give an improved runtime analysis of the attack that gets rid of incorrect simplifying assumptions. In addition, we apply our analysis to evaluate the security against the Hybrid Attack for the NTRU, NTRU prime, and R-BinLWEEnc encryption schemes as well as for the BLISS and GLP signature schemes. Our results show that there exist in fact security over- and underestimates across the literature.

In our ongoing work [8], we present an improved quantum version of the Hybrid Attack, based on an idea sketched by Schanck [19], that replaces the meet-in-the-middle phase of the attack by a generalized version of Grover's quantum search algorithm for non-uniform distributions over the search space [4]. Therefore, our new Quantum Hybrid Attack can be applied to the Learning with Errors (LWE) problem [18, 16, 17] with arbitrary error distribution – a problem whose hardness is the foundation of many modern lattice-based cryptographic constructions. We provide a detailed analysis of the runtime complexity of our Quantum Hybrid Attack and apply it to the New Hope [1] and Frodo [3] key exchange schemes and the Lindner-Peikert [15] encryption scheme, which are based on LWE with discrete Gaussian (or Gaussian-like) error distributions. Our results show, that the Quantum Hybrid Attack outperforms all other Attacks covered by the LWE estimator with a restricted number of LWE samples [20] for most instances we analyzed, and is comparable for the remaining ones. Furthermore, we analyze the runtime of the Quantum Hybrid Attack on the R-BinLWEEnc [5] encryption scheme, which is based on LWE with binary error distribution, in order to showcase its improvement over the classical Hybrid Attack [6, 21].

References

[1] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - a new hope. *IACR Cryptology ePrint Archive*, 2015:1092, 2015.

[2] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. NTRU prime. *IACR Cryptology ePrint Archive*, 2016:461, 2016.

[3] J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24–28, 2016*, 1006–1018. ACM, 2016.

[4] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*, 53–74. American Mathematical Society, 2002. Earlier version in arxiv:quant-ph/0005055.

[5] J. A. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann. High-performance and lightweight lattice-based public-key encryption. In R. Chow and G. Saldamli, editors, *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, CPSS@AsiaCCS, Xi'an, China, May 30 - June 3, 2016*, 2–9. ACM, 2016.

[6] J. A. Buchmann, F. Göpfert, R. Player, and T. Wunderer. On the hardness of LWE with binary error: Revisiting the hybrid lattice-reduction and meet-in-the-middle attack. In D. Pointcheval, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, 24–43. Springer, 2016.

[7] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, 40–56, 2013.

[8] F. Göpfert, C. van Vredendaal, and T. Wunderer. A quantum attack on LWE with arbitrary error distribution, 2017.

[9] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In E. Prouff and P. Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, 530–547. Springer, 2012.

[10] P. S. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, and W. Whyte. Choosing ntruencrypt parameters in light of combined lattice reduction and MITM approaches. In M. Abdalla, D. Pointcheval, P. Fouque, and D. Vergnaud, editors, *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009. Proceedings*, volume 5536 of *Lecture Notes in Computer Science*, 437–455, 2009.

[11] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. Hybrid lattice reduction and meet in the middle resistant parameter selection for ntru-encrypt. *Submission/contribution to ieee p1363*, 1:2007–02, 2007.

[12] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang. Choosing parameters for ntruencrypt. *IACR Cryptology ePrint Archive*, 2015:708, 2015.

[13] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In J. Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21–25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, 267–288. Springer, 1998.

[14] N. Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In A. Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, 150–169. Springer, 2007.

[15] R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In A. Kiayias, editor, *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, volume 6558 of *Lecture Notes in Computer Science*, 319–339. Springer, 2011.

[16] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In M. Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, 333–342. ACM, 2009.

[17] C. Peikert and B. Waters. Lossy trapdoor functions and their applications. *SIAM J. Comput.*, 40(6):1803–1844, 2011.

[18] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, 84–93. ACM, 2005.

[19] J. Schanck. Practical lattice cryptosystems: Ntruencrypt and ntrumls. 2015.

[20] M. Schmidt. Estimation of the hardness of the learning with errors problem with a restricted number of samples. 2017.

[21] T. Wunderer. Revisiting the hybrid attack: Improved analysis and refined security estimates. IACR Cryptology ePrint Archive, Report 2016/733, 2016.

Delegation with minimal time/space overhead

Justin Holmgren

Assuming the existence of somewhat homomorphic encryption, we construct a (2-message)d elegation scheme withan improved asymptotic prover efficiency relative to the prior state of the art. Namely, if the udnerlying computation is a time-T, space-S computation, our prover runs in time $T \cdot poly(\lambda)$ and space $S + poly(\lambda)$, where λ is a parameter determining the soundness of our protocol. The efficiency gap compared to prior work is especially pronounced when we restrict our attention to schemes where soundness is based on "standard" cryptographic assumptions. Our main technical contribution is showing that one can efficiently compute an arbitrary symbol of a classical PCP due to Babai, Fortnow, Levin, and Szegedy ([1]).

References

[1] L. Babai, L. Fortnow, L. A. Levin, and M. Szegedy. Checking Computations in Polylogarithmic Time. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, 21–31.

Beyond Hellman's Time-Space Trade-Offs

Krzysztof Pietrzak

(joint work with Hamza Abusalah, Joel Alwen, Bram Cohen, Danylo Khilko and Leonid Reyzin)

Proofs of space (PoS) were suggested in [DFKP15, RD16] as more ecological and economical proof systems to replace proofs of work, which are currently used in blockchain designs like Bitcoin. Existing PoS [DFKP15] are based on graph pebbling, much simpler and in several aspects more efficient schemes based on inverting random functions have been suggested, but they fail to give meaningful security guarantees due to existing time-memory trade-offs.

In particular, Hellman [Hel80] showed that any permutation over a domain of size N can be inverted in time T by an algorithm which is given S bits of auxiliary information, whenever $N \approx S \cdot T$ (e.g. $S = T \approx N^{1/2}$). For random functions a weaker attack $N^2 \approx S^2 \cdot T$ (e.g. $S = T \approx N^{2/3}$) exists.

We construct functions where for any constant k we can prove a lower bound of the form $S^k \cdot T \in \Omega(N^k)$ (in particular, $S = T \approx N^{k/(k+1)}$). Our construction does not contradict Hellman's attacks, which require that the function can be efficiently computed in forward direction. Our function cannot be efficiently evaluated, but its entire function table can still be computed in time quasilinear in N, which turns out to be sufficient to be used for PoS.

Our simplest construction is build from a random function $g : [N] \times [N] \to [N]$ and a random permutation $f : [N] \to [N]$ and is defined as $h(x) = g(x, x')$ where $f(x') = \pi(f(x))$, where π can be any permutation on $[N]$ without fixpoints. For this function we prove that any adversary, who gets S bits of auxiliary information, makes at most T oracle queries, and inverts h on an ϵ fraction of outputs must satisfy $S^2 \cdot T \in \Omega(\epsilon^2 N^2)$.

References

[DFKP15] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 585–605. Springer, Heidelberg, August 2015.

[Hel80] Martin E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Trans. Information Theory*, 26(4):401–406, 1980.

[RD16] Ling Ren and Srinivas Devadas. Proof of space from stacked expanders. In *TCC 2016-B, Part I*, LNCS, pages 262–285. Springer, Heidelberg, November 2016.

Spooky Encryption and its Applications

Ron D. Rothblum
(joint work with Yevgeniy Dodis, Shai Halevi, Daniel Wichs)

Consider encrypting n inputs under n independent public keys. Given the ciphertexts $\{c_i = \mathsf{Enc}_{\mathsf{pk}_i}(x_i)\}_i$, Alice outputs ciphertexts $c'_1, \dots, c'_n$ that decrypt to $y_1, \dots, y_n$ respectively. What relationships between the x_i's and y_i's can Alice induce?

Motivated by applications to delegating computations, Dwork, Langberg, Naor, Nissim and Reingold [DLN$^+$04] showed that a semantically secure scheme disallows *signaling* in this setting, meaning that y_i cannot depend on x_j for $j \neq i$. On the other hand if the scheme is homomorphic then any *local* (component-wise) relationship is achievable, meaning that each y_i can be an arbitrary function of x_i. However, there are also relationships which are neither signaling nor local. Dwork et al. asked if it is possible to have encryption schemes that support such "spooky" relationships. Answering this question is the focus of our work.

Our first result shows that, under the *learning with errors* (LWE) assumption, there exist encryption schemes supporting a large class of "spooky" relationships, which we call *additive function sharing* (AFS) spooky. In particular, for any polynomial-time function f, Alice can ensure that $y_1, \dots, y_n$ are random subject to $\sum_{i=1}^{n} y_i = f(x_1, \dots, x_n)$. For this result, the public keys all depend on common public randomness. This scheme is based on a recent multi-key fully homomorphic encryption scheme proposed by Clear and McGoldrick [CM15], later simplified by Mukherjee and Wichs [MW16].

Our second result shows that, assuming sub-exponentially hard indistinguishability obfuscation (iO) (and additional more standard assumptions), we can remove the common randomness and choose the public keys completely independently. Furthermore, in the case of $n = 2$ inputs, we get a scheme that supports an even larger class of spooky relationships.

We discuss several implications of AFS-spooky encryption. Firstly, it gives a strong counter-example to a method proposed by Aiello et al. [ABOR00] for building arguments for NP from homomorphic encryption. Secondly, it gives a simple

2-round multi-party computation protocol where, at the end of the first round, the parties can locally compute an additive secret sharing of the output. Lastly, it immediately yields a function secret sharing (FSS) scheme for all functions. Thus, in particular, we obtain a function secret sharing scheme for all functions based on LWE (prior to our work such a result was only known based on sub-exponential indistinguishability obfuscation [BGI15]).

We also define a notion of *spooky-free* encryption, which ensures that no spooky relationship is achievable. We show that any non-malleable encryption scheme is spooky-free. Furthermore, we can construct spooky-free *homomorphic* encryption schemes from SNARKs (i.e., succinct non-interactive arguments of knowledge).

We mention some open problems:

(1) Construct a *spooky free* and yet *homomorphic* encryption scheme from standard assumptions (e.g., LWE) or even from indistinguishability obfuscation. This would imply, in particular, succinct non-interactive arguments for NP (c.f. [GW11]).
(2) Remove the common random string from LWE based construction.
(3) Construct an encryption scheme that supports *all* spooky operations (our first construction supports only additive function sharing operations, whereas our second construction supports general operations but only for 2 keys).

References

[ABOR00] William Aiello, Sandeep Bhatt, Rafail Ostrovsky, and S. Raj. Rajagopalan. Fast verification of any remote procedure call: Short witness-indistinguishable one-round proofs for NP. In *ICALP: Annual International Colloquium on Automata, Languages and Programming*, 2000.

[BGI15] Elette Boyle, Niv Gilboa, and Yuval Ishai. Function secret sharing. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, volume 9057 of *Lecture Notes in Computer Science*, 337–367. Springer, 2015.

[CM15] Michael Clear and Ciaran McGoldrick. Multi-identity and multi-key leveled FHE from learning with errors. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, 630–656. Springer, 2015.

[DLN$^+$04] Cynthia Dwork, Michael Langberg, Moni Naor, Kobbi Nissim, and Omer Reingold. Succinct proofs for NP and spooky interactions. Unpublished manuscript, available at `http://www.cs.bgu.ac.il/~kobbi/papers/spooky_sub_crypto.pdf`, 2004.

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In *STOC*, 99–108, 2011.

[MW16] Pratyay Mukherjee and Daniel Wichs. Two round mutliparty computation via multi-key FHE. In *Eurocrypt 2016, to appear*, 2016. `http://eprint.iacr.org/2015/345`, accessed Jan 2016.

Average-Case Fine-Grained Hardness

Alon Rosen
(joint work with Marshall Ball, Manuel Sabin, Prashant Nalini Vasudevan)

We present functions that are hard to compute on average for algorithms running in some fixed polynomial time, assuming widely-conjectured worst-case hardness of certain problems from the study of fine-grained complexity.

We discuss the relevance of such average-case hardness to cryptography and present, as an illustration, an outline of a proof-of-work protocol constructed based on the hardness and certain structural properties of our functions.

Witness-Indistinguishable Verifiable Mix-nets

Saleet Klein
(joint work with Elette Boyle, Alon Rosen, and Gil Segev)

The goal of this work is to explore the possibility of constructing a simple mix-net that is secure against malicious verifiers and in addition is unconditionally sound. This would in particular mean that when applying the Fiat-Shamir transform to the proofs in the mix-net, anonymity would provably be guaranteed for *any choice* of a hash function. While soundness would still be heuristic, unconditional soundness of the protocols makes them less susceptible to theoretical doubts cast on the Fiat-Shamir transform in the case of certain computationally sound protocols [1].

Towards this end, we aim for a relaxed indistinguishability-based notion of anonymity, which is weaker than zero-knowledge and yet guarantees the privacy of voters in the system. We demonstrate how indistinguishability-based anonymity of an entire mix-net system can be attained, even if most of the underlying sub-protocols are merely WI. At the core of our analysis are new techniques for guaranteeing the existence of multiple witnesses in NP-verification relations upon which the soundness of mixnets is based.

We instantiate our ideas with a very simple and appealing Beneš-network based construction due to Abe [2, 3]. While this construction does not match the sub-linear verification efficiency of later mix-nets in the literature (verification time is quasi-linear in the number of voters), it does enjoy a number of desirable features, most notably high parallelizability. In addition, proving and verifying consists of invoking standard and widely used proofs of knowledge, making the mix-net easy to understand and implement.

Abe's mixnet was originally shown to be anonymous assuming honest verifiers, and specifically based on the honest verifier ZK property of the underlying proofs of knowledge. In the case of a *malicious* verifier, these sub-protocols are known only to be witness indistinguishable, alas this guarantees nothing in cases where there is a single witness. Moreover, in Abe's mixnet cases in which only one witness exists *cannot be ruled out*, and if indeed leakage on the single witness occurs in these situations we demonstrate that the system is *not anonymous*.

Our Results. We propose two different methods for modifying Abe's original proposal so that it results in a verifiable mix-net anonymous against malicious verifiers and sound against computationally unbounded provers. Both methods require only minor changes to Abe's original protocol:

Lossy Abe mix-net: This method is identical to Abe's original proposal, with the only difference being that plain ElGamal encryption is replaced with an alternative, yet equally efficient, encrpytion scheme with the property that public-keys can be sampled using a "lossy" mode (this mode is only invoked in the analysis). When sampled with lossy public-keys encrypted ciphertexts do not carry any information about the plaintext.

Injected Abe mix-net: This method consists of running the original Abe mix-net with some additional dummy ciphertexts that are injected to the system for the purpose of proving D-WI without having to modify and/or assume anything about the encryption scheme in use (beyond it being rerandomizable). The analysis of this construction relies on combinatorial properties of the Beneš-network, and may turn out to be relevant elsewhere.

In both cases, we show that the entire transcript of the mixnet system satisfies the following natural anonymity property:*for any choice of votes and any two permutations on the votes, the corresponding views of an adversary are computationally indistinguishable.*

References

[1] S. Goldwasser and Y. T. Kalai, On the (In)security of the Fiat-Shamir Paradigm, In *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings* , 102–113, 2003

[2] M. Abe, Mix-Networks on Permutation Networks, In *Advances in Cryptology - ASIACRYPT '99, International Conference on the Theory and Applications of Cryptology and Information Security, Singapore, November 14-18, 1999, Proceedings*, 258–273, 1999

[3] M. Abe and F. Hoshino, Remarks on Mix-Network Based on Permutation Networks, In *Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, Cheju Island, Korea, February 13-15, 2001, Proceedings*, 317–324, 2001

NTRU Prime

Tanja Lange

(joint work with Daniel J. Bernstein, Chitchanok Chuengsatiansup, Christine van Vredendaal)

Several ideal-lattice-based cryptosystems have been broken by recent attacks that exploit special structures of the rings used in those cryptosystems. The same structures are also used in the leading proposals for post-quantum lattice-based cryptography, including the classic NTRU cryptosystem and typical Ring-LWE-based cryptosystems.

This talk (1) proposes NTRU Prime, which tweaks NTRU to use rings without these structures; (2) proposes Streamlined NTRU Prime, a public-key cryptosystem optimized from an implementation perspective, subject to the standard design goal of IND-CCA2 security; (3) finds high-security post-quantum parameters for Streamlined NTRU Prime; and (4) optimizes a constant-time implementation of those parameters. The performance results are surprisingly competitive with the best previous speeds for lattice-based cryptography.

For more details see [1].

References

[1] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Christine van Vredendaal. *NTRU Prime*, `https://eprint.iacr.org/2016/461`.

A kilobit hidden SNFS discrete logarithm computation

Nadia Heninger
(joint work with Joshua Fried, Pierrick Gaudry, and Emmanuel Thomé)

We demonstrate that constructing and exploiting trapdoored primes for Diffie-Hellman and DSA is feasible for 1024-bit keys with modern academic computing resources.

The Number Field Sieve (NFS) was originally proposed as an integer factoring algorithm [3]. Gordon adapted the algorithm to compute discrete logarithms in prime fields [2]. For the past twenty years, the NFS has been routinely used in record computations. The NFS can handle an arbitrary prime p and compute discrete logarithms in $\mathbb{F}_p^*$ in asymptotic time $L_p(1/3, (64/9)^{1/3})^{1+o(1)}$, using the usual L-notation, defined as $L_p(e, c) = \exp(c(\log p)^e(\log\log p)^{1-e})$.

Very early on in the development of NFS, it was observed that the algorithm was particularly efficient for inputs of a special form. Some composite integers are particularly amenable to being factored by NFS, and primes of a special form allow easier computation of discrete logarithms. This relatively rare set of inputs defines the Special Number Field Sieve (SNFS). It is straightforward to start with parameters that give a good running time for the NFS—more precisely, a pair of irreducible integer polynomials f and g, sharing a common root m modulo p and satisfying certain size and degree requirements—and derive an integer to be factored, or a prime modulus for a discrete logarithm. The complexity of SNFS is $L_p(1/3, (32/9)^{1/3})^{1+o(1)}$, much less than its general counterpart.

Gordon [1] suggested that one could craft primes so that SNFS polynomials exist, but may not be apparent to the casual observer. Heidi, a mischievous designer for a crypto standard, would select a pair of SNFS polynomials to her liking *first*, and publish only their resultant p (if it is prime) *afterwards*. The hidden trapdoor then consists in the pair of polynomials which Heidi used to generate p, and that she can use to considerably ease the computation of discrete logarithms in $\mathbb{F}_p$.

Let $\mathbb{F}_p$ be a prime field, let $\gamma \in \mathbb{F}_p^*$ be an element of prime order $q \mid p-1$. We wish to solve discrete logarithms in $\langle\gamma\rangle$.

In Algorithm 1, we recall the method of Gordon to construct hidden SNFS parameters in a DSA setting, in which the subgroup order q is much smaller than p. The general idea is to start from the polynomial f and the prime q, then derive a polynomial g such that q divides the resultant of f and g minus 1, and only at the end check if this resultant is a prime p. This avoids the costly factoring of $p-1$ that would be needed to check whether there is a factor of appropriate size to play the role of q.

```
Input  : The bit-sizes $s_p$ and $s_q$ for $p$ and $q$; the degree $d$ of $f$.
Output: HSNFS parameters $f$, $g$, $p$, $q$.
Pick a random irreducible polynomial $f$, with $\|f\| \approx 2^{s_q/2(d+1)}$;
Pick a random prime $q$ of $s_q$ bits;
Pick a random integer $g_0 \approx 2^{s_p/d}/\|f\|$;
Consider the polynomial $G_1(g_1) = \mathrm{Res}_x(f(x), g_1x + g_0) - 1$ of degree $d$ in $g_1$;
Pick a root $r$ of $G_1$ modulo $q$; if none exists go back to Step 1;
Add a random multiple of $q$ to $r$ to get an integer $g_1$ of size $\approx 2^{s_p/d}/\|f\|$;
Let $p = |\,\mathrm{Res}_x(f(x), g_1x + g_0)|$;
If $p$ has not exactly $s_p$ bits or if $p$ is not prime or if $q$ does not divide $p-1$,
  then go back to Step 1;
Return $f$, $g$, $p$, $q$.
```

Algorithm 1: Gordon's hidden SNFS construction algorithm

Twenty-five years later, we reconsider the best-case scenario for Heidi: given a target size, what type of polynomial pair will give the fastest running time for a discrete logarithm computation? Back in 1992, when Gordon studied the question, the complexity analysis of the Number Field Sieve was not as well understood, and the available computing power was far less than today. At that time, the proposed parameter sizes for DSA were to generate a 160-bit prime subgroup modulo a 512-bit prime p, leading to difficulties satisfying the condition of Algorithm 1 unless a suboptimal degree d for polynomial f was chosen. Nowadays, popular DSA parameters are 1024-bit primes p with 160-bit subgroup order, leaving much room for the condition to hold, and it is possible to choose $d = 6$, which is optimal for our NFS implementation. Therefore, Gordon's algorithm can be run with optimal parameters, and detecting that p has this trapdoor seems out of reach.

We generated such a trapdoored 1024-bit prime. Our chosen prime p looks random, and $p-1$ has a 160-bit prime factor, in line with recommended parameters for the Digital Signature Algorithm. We then performed a special number field sieve discrete logarithm computation for this prime. To our knowledge, this is the first kilobit-sized discrete logarithm computation ever reported for prime fields. This computation took a little over two months of calendar time on an academic cluster using the open-source CADO-NFS software.

Twenty-five years ago, there was considerable controversy around the possibility of backdoored parameters for DSA. Our computations show that trapdoored primes are entirely feasible with current computing technology.

As can be expected from a trapdoor mechanism which we say is hard to detect, our research did not reveal any trapdoored prime in wide use. The only way for a user to defend against a hypothetical trapdoor of this kind is to require verifiably random primes.

Cryptosystems based on the hardness of discrete logarithms should have ceased to use 1024-bit primes entirely already a while ago. NIST recommended transitioning away from 1024-bit key sizes for DSA, RSA, and Diffie-Hellman in 2010 [4]. Unfortunately, such key sizes remain in wide use in practice. Our results are yet another reminder of the risk, and we show this dramatically in the case of primes which lack verifiable randomness.

References

[1] D. M. Gordon. Designing and detecting trapdoors for discrete log cryptosystems. In E. F. Brickell, editor, *CRYPTO'92*, volume 740 of *Lecture Notes in Comput. Sci.*, 66–75. Springer, Heidelberg, Aug. 16–20, 1993.

[2] D. M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discrete Math.*, 6(1):124–138, Feb. 1993.

[3] A. K. Lenstra and H. W. Lenstra, Jr., editors. *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.* Springer–Verlag, 1993.

[4] E. Barker and A. Roginsky. Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths. Technical report, National Institute of Standards and Technology, 2011.

Reporter: Lucas Schabhueser

Participants

Dr. Benny Applebaum
Department of Electrical
Engineering Systems
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL

Prof. Dr. Daniel J. Bernstein
Department of Computer Science
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street
Chicago IL 60607-7045
UNITED STATES

Dr. Elette Boyle
Department of Computer Science
and Applied Mathematics, Technion
The Institute of Technology
Haifa 32000
ISRAEL

Dr. Zvika Brakerski
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O.Box 26
Rehovot 76100
ISRAEL

Prof. Dr. Johannes Buchmann
Fachbereich Informatik
Technische Universität Darmstadt
64283 Darmstadt
GERMANY

Prof. Dr. Ran Canetti
Department of Computer Science
Boston University
Boston, MA 02215
UNITED STATES

Aloni Cohen
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Dr. Denise Demirel
Fachbereich Informatik
Technische Universität Darmstadt
64283 Darmstadt
GERMANY

Prof. Dr. Jintai Ding
McMicken College of Arts and Sciences
University of Cincinnati
7148 Edwards One
Cincinnati, Ohio 45221-0025
UNITED STATES

Dr. Craig B. Gentry
IBM Research
T.J. Watson Research Center
1101 Kitchawan Road, Route 134
Yorktown Heights NY 10598
UNITED STATES

Prof. Dr. Shafi Goldwasser
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Dr. Shai Halevi
IBM Research
T.J. Watson Research Center
1101 Kitchawan Road, Route 134
Yorktown Heights NY 10598
UNITED STATES

Prof. Dr. Nadia Heninger
Department of Computer
and Information Science
University of Pennsylvania
3330 Walnut Street
Philadelphia, PA 19104-6389
UNITED STATES

Prof. Dr. Dennis Hofheinz
Karlsruher Institut f. Technologie (KIT)
Arbeitsgruppe Kryptograhie und
Sicherheit
Am Fasanengarten 5
76131 Karlsruhe
GERMANY

Justin Holmgren
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Dr. Andreas Hülsing
Department of Mathematics
Eindhoven University of Technology
P.O.Box 513
5600 MB Eindhoven
NETHERLANDS

Dr. Yuval Ishai
Department of Computer Science
University of California
Boelter Hall, Room 3731 M
Los Angeles CA 90095
UNITED STATES

Prof. Dr. Antoine Joux
Laboratoire d'informatique de Paris 6
UPMC - Paris VI
4, Place Jussieu
75252 Paris Cedex 05
FRANCE

Dr. Yael Kalai
Microsoft Research
Office 14063
One Memorial Drive
Cambridge MA 02142
UNITED STATES

Prof. Dr. Eike Kiltz
Lehrstuhl für Kryptologie und
IT-Sicherheit
Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum
Universitätsstraße 150
44780 Bochum
GERMANY

Saleet Klein
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Dr. Ilan Komargodski
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O.Box 26
Rehovot 76100
ISRAEL

Dr. Juliane Krämer
Fachbereich Informatik
Technische Universität Darmstadt
64283 Darmstadt
GERMANY

Prof. Dr. Tanja Lange
Department of Mathematics
and Computer Science
Eindhoven University of Technology
P.O. Box 513
5600 MB Eindhoven
NETHERLANDS

Prof. Dr. Hendrik W. Lenstra
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Prof. Dr. Huijia (Rachel) Lin
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
UNITED STATES

Prof. Dr. Vadim Lyubashevsky
IBM Research
Säumerstrasse 4
8803 Rüschlikon
SWITZERLAND

Prof. Dr. Jörn Müller-Quade
Karlsruher Institut für Technologie
(KIT)
Institut für Kryptograhie und Sicherheit
Am Fasanengarten 5
76131 Karlsruhe
GERMANY

Prof. Dr. Moni Naor
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O.Box 26
Rehovot 76100
ISRAEL

Prof. Dr. Kobbi Nissim
Department of Computer Science
Harvard University
MD 243
33 Oxford Street
Cambridge, MA 02138
UNITED STATES

Prof. Dr. Rafail Ostrovsky
Department of Mathematics
University of California, Los Angeles
Math. Sciences Building 6363
P.O. Box 951555
Los Angeles, CA 90095-1555
UNITED STATES

Omer Paneth
Department of Computer Science
Boston University
808 Commonwealth Avenue
Boston MA 02215
UNITED STATES

Prof. Dr. Rafael Pass
Computer Science Department
Cornell University
White Hall
Ithaca, NY 14853
UNITED STATES

Prof. Dr. Krzysztof Pietrzak
Institute of Science and Technology
(IST Austria)
Am Campus 1
3400 Klosterneuburg
AUSTRIA

Prof. Dr. Tal Rabin
IBM Research
Thomas J. Watson Research Center
Yorktown Heights, NY 10598
UNITED STATES

Dr. Silas Richelson
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. Alon Rosen
The Interdisciplinary Center
Kanfei Nesharim St.
P.O. Box 167
Herzliya 46150
ISRAEL

Dr. Guy Rothblum
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O.Box 26
Rehovot 76100
ISRAEL

Dr. Ron Rothblum
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Dr. Alessandra Scafuro
Department of Mathematics
Boston University
111 Cummington Street
Boston, MA 02215-2411
UNITED STATES

Lucas Schabhueser
Fachbereich Informatik
Technische Universität Darmstadt
64283 Darmstadt
GERMANY

Prof. Dr. Gil Segev
School of Computer Science
and Engineering
The Hebrew University
Givat-Ram
Jerusalem 91904
ISRAEL

Prof. Dr. Nicolas Sendrier
INRIA
Équipe-projet SECRET
2, Rue Simone Iff
75589 Paris Cedex
FRANCE

Giulia Traverso
Fachbereich Informatik
Technische Universität Darmstadt
64283 Darmstadt
GERMANY

Prof. Dr. Vinod Vaikuntanathan
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Christine van Vredendaal
Department of Mathematics
and Computer Science
Eindhoven University of Technology
5600 MB Eindhoven
NETHERLANDS

Prashant Vasudevan
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge MA 02139
UNITED STATES

Prof. Dr. Muthuramakrishnan Venkitasubramaniam
Department of Computer Science
University of Rochester
Rochester, NY 14627
UNITED STATES

Prof. Dr. Hoeteck Wee
Département d'informatique
École Normale Superieure
45, rue d'Ulm
75005 Paris Cedex
FRANCE

Prof. Dr. Daniel Wichs
College of Computer Science
Northeastern University
215 Cullinane Hall
Boston, MA 02115
UNITED STATES

Thomas Wunderer
Fachbereich Informatik
Technische Universität Darmstadt
64283 Darmstadt
GERMANY