Report from Dagstuhl Seminar 11391

Public-Key Cryptography

Edited by

Marc Fischlin[1], Anna Lysyanskaya[2], Ueli Maurer[3], and Alexander May[4]

1 **TU Darmstadt, DE,** marc.fischlin@gmail.com
2 **Brown University – Providence, US**
3 **ETH Zürich, CH,** maurer@inf.ethz.ch
4 **Ruhr-Universität Bochum, DE,** alex.may@ruhr-uni-bochum.de

Abstract

From September 25th till September 30th, 2011, the Dagstuhl Seminar 11391 about "Public-Key Cryptography" took place at Schloss Dagstuhl. The meeting hosted 33 international researchers and incited active discussions about recent developments in this area.

Seminar 25.–30. September, 2011 – www.dagstuhl.de/11391
1998 ACM Subject Classification D.4.6 Security and Protection
Keywords and phrases Fully-Homomorphic Encryption, Leakage-Resilience, Constructive Cryptography
Digital Object Identifier 10.4230/DagRep.1.9.76
Edited in cooperation with Alexander Meurer

1 Executive Summary

Marc Fischlin
Anna Lysyanskaya
Ueli Maurer
Alexander May

Cryptography is the science of protecting data in presence of malicious parties. Without cryptography e-commerce, e-banking and e-government would not be possible. Indeed, the most prominent application of cryptography today is the SSL/TLS protocol to secure e-mail and web communication. But soon citizens will also use cryptography on large scales on identity cards, passports and health cards.

Cryptography is a relatively new area in computer science, with the first modern and scientific approaches dating back to the mid 70's, and the first large-scale scientific conferences in this area in the early 80's. Since then, cryptography has evolved as its own sub area in computer science, with intersections with many areas like number-theory or complexity theory.

Cryptography has a good tradition within the Dagstuhl Seminar series, with the first meeting about cryptography held in 1993, and subsequent seminars on this topic about every 5 years. In 2007 and 2012 a seminar for the sub area of "Symmetric Cryptography" is added, inciting us to coin the seminar here "Public-Key Cryptography" for sake of distinction.

The seminar brought together 33 of the leading scientists in the area of public-key cryptography. The participants came from all over the world, including countries like the US, Great Britain, Israel, France, or Italy. Among the affiliations Germany lead the number with 10 participants, followed by the US with 7, and Switzerland with 6.

Public-Key Cryptography, *Dagstuhl Reports*, Vol. 1, Issue 9, pp. 76–94
Editors: Marc Fischlin, Anna Lysyanskaya, Ueli Maurer, and Alexander May
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The program contained 28 talks, each of 25-30 minutes, and a panel discussion about the field's future, with a free afternoon on Wednesday for social activities and half a day on Friday for traveling. Before the seminar we asked the participants to present very recent and ongoing work which, ideally, should not have been published or accepted to publication yet. Most of the participants followed our suggestion and to a large extend the presentations covered topics which have not even been submitted at the time.

The topics of the talk represented the diversity of public-key cryptography. As expected and envisioned, there was quite a number of talks about encryption schemes (such as homomorphic encryption) and their use for the cloud scenario. To further this area has been stated as one of the goals of the seminar. Presentations about this topic included improvements for such encryption schemes, e.g., the even more general functional encryption was covered comprehensively, as well as their applicability. Another well-represented area of the seminar touched the intended question of looking into more leakage-resilient alternatives like learning with errors (LWE) or lattice-based constructions. Discussions during and after the talks were lively.

The goal of the seminar was to incite new research in the area of public-key cryptography, with the explicit goal to enhance the areas of computing on encrypted data, leakage-resilience, and hash functions. We —and seemingly also the participants— enjoyed the possibility to further discuss fresh topics like constructive cryptography. Overall, the personal feedback of the participants to us was very positive, with the wish to repeat such a seminar.

The organizers would like to thank Alexander Meurer for collecting all abstracts of this seminar report. Finally, the organizers, also on behalf of the participants, would like to thank the staff and the management of Schloss Dagstuhl for providing the surrounding for a very pleasant and fruitful seminar.

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Generic Algorithms for Hard Subset Sums and its Application to Linear Codes

Anja Becker (University of Versailles, FR)

Joint work of Becker, Anja; Coron, Jean-Sébastien; Joux, Antoine;
Main reference A. Becker, J.S. Coron, A. Joux, "Improved Generic Algorithms for Hard Knapsacks," in Advances in Cryptology – EUROCRYPT 2011, pp. 364–385, LNCS Vol. 6632.
URL http://dx.doi.org/10.1007/978-3-642-20465-4_21

At Eurocrypt 2010, Howgrave-Graham and Joux described an algorithm for solving hard knapsacks of density close to 1 in time $\mathcal{O}(2^{0.337n})$ and memory $\mathcal{O}(2^{0.256n})$, thereby improving a 30-year old algorithm by Shamir and Schroeppel. In this talk we will present the following:

Using the simple observation that a binary vector can be represented by two overlapping vectors with coefficients in $\{-1, 0, 1\}$, we can obtain a better algorithm of running time $\mathcal{O}(2^{0.291n})$.

Furthermore, this technique can be directly applied to improve information set decoding attacking linear codes such as used in McEliece public key encryption.

3.2 Functional Re-encryption and Collusion-Resistant Obfuscation

Melissa Chase (Microsoft Research – Redmond, US)

Joint work of Chandran, Nishanth; Chase, Melissa; Vaikuntanathan, Vinod;
Main reference N. Chandran, M. Chase, V. Vaikuntanathan, "Collusion Resistant Obfuscation and Functional Re-encryption," IACR eprint archive, 2011/337, 2011.
URL http://eprint.iacr.org/2011/337

We introduce a natural cryptographic functionality called functional re-encryption.

Informally, functional re-encryption allows an untrusted server to transform a ciphertext encrypted for Alice into a ciphertext encrypted for one of n recipients, depending on the message. In particular, a functional re-encryption function for a function F will transform an encryption of message m intended for Alice into an encryption of m intended for recipient $F(m)$.

In many settings, one might require that the program implementing the functional re-encryption functionality should reveal as little as possible about the input secret key SK and the function F. Furthermore, ideally we would obtain an even stronger guarantee: that this information remains hidden even when some of the n recipients may be corrupted.

To formalize these issues, we introduce the notion of collusion-resistant obfuscation and define this notion with respect to average-case secure obfuscation (Hohenberger et al. – TCC 2007). We show that this notion of functional re- encryption can be achieved for any function F with polynomial-size domain, by providing a direct construction from bilinear pairings.

This is joint work with Nishanth Chandran and Vinod Vaikuntanathan.

3.3 Active Security in General Secure Multi-Party Computation via Black-Box Groups

Yvo Desmedt (University College London, GB)

At CRYPTO 2007, Desmedt et al introduced a construction for a multi-party multiplication protocol for black-box non-Abelian groups. The security achieved was against a passive adversary controlling t parties using the unconditionally secure model. This left as an open problem how to achieve security against active attacks. The construction was based on a reduction to a new planar graph coloring problem.

In this presentation, we extended above to the case of general adversary structure. Our focus was on, for such an adversary, to achieve security against an active adversary. Our solution is the first n-party protocol that achieves multiparty computation using as building block a black-box non-Abelian group solution, which is secure against an active attacker, tolerating any adversary structure satisfying the property that no union of three subsets from the adversary structure covers the whole player's set.

Our protocol uses Maurer's Verifiable Secret Sharing (VSS) but preserves roughly the essential simplicity of the graph-based approach of Desmedt et al. This implies that each shareholder can avoid having to rerun the full VSS protocol after each local computation. The reduction of the need to use VSS may have consequences to secure multiparty computation beyond the fact we use non-Abelian groups.

3.4 Leftover Hash Lemma, Revisited

Yevgeniy Dodis (New York University, US)

Joint work of Barak, Boaz; Dodis, Yevgeniy; Krawczyk, Hugo; Pereira, Olivier; Pietrzak, Krzysztof; Standaert, Francois-Xavier; Yu, Yu
Main reference B. Barak,Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, Y. Yu, "Leftover Hash Lemma, Revisited", Published at CRYPTO'2011.
URL http://eprint.iacr.org/2011/088

Randomness extractors are procedures used to extract nearly perfect randomness from any "imperfect" source of randomness, such as physical sources, biometrics, etc. Such extractor have found numerous applications in many areas of computer science.

A very simple and elegant randomness extractor is given by the famous Leftover Hash Lemma (LHL), which states that a random universal hash function is a good extractor.

Unfortunately, despite their numerous applications, LHL-based extractors suffer from the following two drawbacks. First, the maximum number of extracted bits is at least 2*log(1/e) less than the amount of entropy in the source, where e is the desired statistical distance from uniform, which could be large for low-entropy sources.

Second, the description length of a random universal hash function (called the "seed") is linear in the length of the imperfect source, which could be very large.

Quite surprisingly, we show that both limitations of the LHL — large entropy loss and large seed — can often be overcome (or, at least, mitigated) in various quite general scenarios. First, we show that "entropy loss" could be halved from 2log(1/e) to log(1/e) for the setting of deriving secret keys for most cryptographic applications. Second, we study the soundness of the natural *expand-then-extract* approach, where one uses a pseudorandom generator (PRG) to compress the description length of the extractor seed. We show that, although the expand than extract-approach is *not* sound in general, any counter-example implies an efficient construction of public-key encryption from a PRG.

This suggests that the sample-then-extract approach is likely secure when used with 'practical' PRGs, despite lacking a reductionist proof of security!

The paper can be found at http://eprint.iacr.org/2011/088, and is also mentioned in the New Yorker magazine (October 2011).

3.5 Functional Encryption: Extensions and Implications

Pooya Farshim (TU Darmstadt, DE)

We propose extensions of functional encryption (FE) to more complex application scenarios and, in doing so, shed additional light on the properties of simulation-based and indistinguishability-based security notions for FE schemes.

We first study chosen-ciphertext security in the functional setting. We find (somewhat surprisingly) that a CCA-secure FE scheme can be generically built from a CPA-secure one. This transformation, in contrast to the usual CHK transformation (which we also show to hold in the functional setting) does not rely on a delegation mechanism. We then propose an extension of functional encryption to probabilistic functionalities. We call this primitive probabilistic-functional encryption (PFE), and discuss the correct security notions for it. We present constructions of PFE schemes, both generic and concrete, from standard FE schemes. Finally we consider two homomorphic extensions for functional encryption: one notion allows arbitrary computations over a restricted portion of encrypted data, while the other allows restricted computation over the entire encrypted data (i.e., allows functional re-encryption). We identify a class of functionalities for which a meaningful definition of security for the first primitive can be formulated, and show that a large and practically relevant subclass can be securely realized via the KEM/DEM paradigm. We also describe two generic constructions of the second primitive. As a corollary, we show that a homomorphic encryption scheme supporting a large class of circuits can be generically built from a semantically secure FE scheme.

3.6 Resource-based Corruptions and the Combinatorics of Anonymity

Juan A. Garay (AT&T Research – Florham Park, US)

Main reference Submitted for publication.

In the setting of cryptographic protocols, the corruption of a party has been viewed as a simple, uniform and atomic operation, where the adversary decides to get control over a party and this party immediately gets corrupted. In this paper, motivated by the fact that different players may require different resources to get corrupted, we put forth the notion of *resource-based corruptions*, where the adversary must invest some resources in order to do so.

If the adversary has full information about the system configuration then resource-based corruptions would provide no fundamental difference from the standard corruption model. However, in a *resource anonymous* setting, in the sense that such configuration is hidden from the adversary, much is to be gained in terms of efficiency and security.

We showcase the power of anonymity in the setting of secure multiparty computation (MPC) with resource-based corruptions and prove that anonymity can effectively be used to circumvent known impossibility results. Specifically, if OPT is the corruption budget that violates the completeness of MPC (the case when half or more of the players are corrupted), we show that by using anonymity, the completeness of MPC can be made to hold against an adversary with as much as a $B \cdot OPT$ budget, for any constant $B > 1$. This result requires a suitable choice of parameters (in terms of number of players and their hardness to corrupt), which we provide and further prove other tight variants of the result when the said choice is not available. Regarding efficiency gains, we show that anonymity can be used to force the corruption threshold to drop from 1/2 to 1/3, in turn allowing the use of much more efficient (information-theoretic) MPC protocols.

We achieve the above through a series of technical contributions:

- The formulation of the notion of *inversion effort preserving* (IEP) functions which is a type of direct-sum property, and the property of *hardness indistinguishability.* While hardness indistinguishability enables the dissociation of parties' identities and the resources needed to corrupt them, IEP enables the discretization of adversarial work into corruption tokens;
- the modeling of the corruption process in the setting of MPC through *corruption oracles* as well as the introduction of a notion of reduction to relate such oracles;
- the abstraction of the corruption game as a combinatorial problem and its analysis,

all of which may be of independent interest.

3.7 All-But-Many Lossy Trapdoor Functions

Dennis Hofheinz (KIT – Karlsruhe Institute of Technology, DE)

Main reference D. Hofheinz, "All-But-Many Lossy Trapdoor Functions,
IACR Cryptology ePrint Archive, 2011/230, 2011.
URL http://eprint.iacr.org/2011/230

We put forward a generalization of lossy trapdoor functions (LTFs). Namely, all-but-many lossy trapdoor functions (ABM-LTFs) are LTFs that are parametrized with tags. Each tag can either be injective or lossy, which leads to an invertible or a lossy function. The interesting property of ABM-LTFs is that it is possible to generate an arbitrary number of lossy tags by means of a special trapdoor, while it is not feasible to produce lossy tags without this trapdoor.

Our definition and construction can be seen as generalizations of all-but-one LTFs (due to Peikert and Waters) and all-but-N LTFs (due to Hemenway et al.).

However, to achieve ABM-LTFs (and thus a number of lossy tags which is not bounded by any polynomial), we have to employ some new tricks. Concretely, we give two constructions that employ "'disguised"' variants of the Waters, resp. Boneh-Boyen signature schemes to make the generation of lossy tags hard without trapdoor. In a nutshell, lossy tags simply correspond to valid signatures. At the same time, tags are disguised (i.e., suitably blinded) to keep lossy tags indistinguishable from injective tags.

ABM-LTFs are useful in settings in which there are a polynomial number of adversarial challenges (e.g., challenge ciphertexts). Specifically, building on work by Hemenway et al., we show that ABM-LTFs can be used to achieve selective opening security against chosen-ciphertext attacks. One of our ABM-LTF constructions thus yields the first SO-CCA secure encryption scheme with compact ciphertexts (O(1) group elements) whose efficiency does not depend on the number of challenges. Our second ABM-LTF construction yields an IND-CCA (and in fact SO-CCA) secure encryption scheme whose security reduction is independent of the number of challenges and decryption queries.

3.8 Constructing a Pseudorandom Generator Requires an Almost Linear Number of Calls

Thomas Holenstein (ETH Zürich, CH)

Joint work of Holenstein, Thomas; Sinha, Makrand

We show that a black-box construction of a pseudorandom generator from a one-way function needs to make $\Omega(\frac{n}{\log(n)})$ calls to the underlying one-way function. The bound even holds if the one-way function is guaranteed to be regular. In this case it matches the best known construction due to Goldreich, Krawczyk, and Luby (SIAM J. Comp. 22, 1993), which uses $O(\frac{n}{\log(n)})$ calls.

3.9 How to Garble Arithmetic Circuits

Yuval Ishai (Technion – Haifa, IL)

Joint work of Applebaum, Benny; Ishai, Yuval; Kushilevitz, Eyal;
Main reference B. Applebaum, Y. Ishai, E. Kushilevitz, "How to Garble Arithmetic Circuits," Proceedings of FOCS 2011.

Yao's garbled circuit construction transforms a boolean circuit $C : \{0,1\}^n \to \{0,1\}^m$ into a "garbled circuit" $\hat{C}$ along with n pairs of k-bit keys, one for each input bit, such that $\hat{C}$ together with the n keys corresponding to an input x reveal $C(x)$ and no additional information about x. The garbled circuit construction is a central tool for constant-round secure computation and has several other applications.

Motivated by these applications, we suggest an efficient arithmetic variant of Yao's original construction. Our construction transforms an arithmetic circuit $C : \mathbb{Z}^n \to \mathbb{Z}^m$ over integers from a bounded (but possibly exponential) range into a garbled circuit $\hat{C}$ along with n affine functions $L_i : \mathbb{Z} \to \mathbb{Z}^k$ such that $\hat{C}$ together with the n integer vectors $L_i(x_i)$ reveal $C(x)$ and no additional information about x. The security of our construction relies on the intractability of the learning with errors (LWE) problem.

3.10 Cover and Decomposition on Elliptic Curves

Antoine Joux (University of Versailles, FR)

Joint work of Joux, Antoine; Vitse, Vanessa
Main reference A. Joux, V. Vitse, "Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a seemingly secure curve over F_{p^6}," IACR Cryptology ePrint Archive, 2011/020, 2011.
URL http://eprint.iacr.org/2011/020

We present a new "cover and decomposition" attack on the elliptic curve discrete logarithm problem, that combines Weil descent and decomposition-based index calculus into a single discrete logarithm algorithm. This attack applies, at least theoretically, to all composite degree extension fields, and is particularly well-suited for curves defined over $\mathbb{F}_{p^6}$. We give a real-size example of discrete logarithm computations on a curve over a 151-bit degree 6 extension field, which would not have been practically attackable using previously known algorihtms.

3.11 LWE is Lossy

Eike Kiltz (Ruhr-Universität Bochum, DE)

Joint work of Bellare, Mihir; Kiltz, Eike; Peikert, Chris; Waters, Brent
Main reference M. Bellare, E. Kiltz, C. Peikert, B. Waters, "Identity-Based (Lossy) Trapdoor Functions and Applications," IACR Cryptology ePrint Archive, 2011/479, 2011.
URL http://eprint.iacr.org/2011/479

We show that, under an appropriate choice of parameters, the Learning With Errors (LWE) function is a lossy trapdoor function.

3.12 Constructive Cryptography – A New Paradigm for Security Definitions and Proofs

Ueli Maurer (ETH Zürich, CH)

Joint work of Maurer, Ueli; Renner, Renato
Main reference U. Maurer, R. Renner, "Abstract Cryptography," in Proceedings of Innovations in Computer Science – ICS 2010.

Constructive cryptography, an application of abstract cryptography proposed by Maurer and Renner, is a new paradigm for defining the security of cryptographic schemes such as symmetric encryption, message authentication codes, public-key encryption, key-agreement protocols, and digital signature schemes, and for proving the security of protocols making use of such schemes. Such a cryptographic scheme can be seen (and defined) as constructing a certain resource (e.g. a channel or key) with certain security properties from another (weaker) such resource. For example, a secure encryption scheme constructs a secure channel from an authenticated channel and a secret key.

The term "construct", which is defined by the use of a simulator, is composable in the sense that a protocol obtained by the composition of several secure constructive steps is itself secure. This is in contrast to both the traditional, game-based security definitions for cryptographic schemes and the attack-based security definitions used in formal-methods based security research, which are generally not composable.

Constructive cryptography allows to take a new look at cryptography and the design of cryptographic protocols. One can give explicit meaning to various types of game-based security notions of confidentiality, integrity, and malleability, one can design key agreement, secure communication, certification, and other protocols in a modular and composable manner, and one can separate the understanding of what cryptography achieves from the technical security definitions and proofs, which is useful for didactic purposes and protocol design.

3.13 A New Information Set Decoding Algorithm

Alexander Meurer (Ruhr-Universität Bochum, DE)

Joint work of May, Alexander; Meurer, Alexander; Thomae, Enrico
Main reference A. May, A. Meurer, E. Thomae, "Decoding Random Linear Codes in $O(2^{0.054n})$," Advances in Cryptology – ASIACRYPT 2011, pp. 107–124, LNCS Vol. 7073.
URL http://dx.doi.org/10.1007/978-3-642-25385-0_6

Decoding random linear codes is a fundamental problem in complexity theory and lies at the heart of almost all code-based cryptography. The best attacks on the most prominent code-based cryptosystems such as McEliece directly use decoding algorithms for linear codes. The asymptotically best decoding algorithm for random linear codes of length n was for a long time Sterns variant of information-set decoding running in time $\mathcal{O}(2^{0.05563n})$.

Recently, Bernstein, Lange and Peters proposed a new technique called Ball-collision decoding which offers a speed-up over Sterns algorithm by improving the running time to $\mathcal{O}(2^{0.05558n})$. In this talk, we present a new algorithm for decoding linear codes that is inspired by a representation technique due to Howgrave-Graham and Joux in the context of subset sum algorithms. Our decoding algorithm offers a rigorous complexity analysis for random linear codes and brings the time complexity down to $\mathcal{O}(2^{0.05363n})$.

3.14 Code Obfuscation with a Stateless Hardware Token

Joern Mueller-Quade (KIT – Karlsruhe Institute of Technology, DE)

Code obfuscation is one of the most powerful concepts in cryptography. It could yield functional encryption, digital rights management, and maybe even secure cloud computing. However, general code obfuscation has been proven impossible and the research then focused on obfuscating very specific functions, studying weaker security definitions for obfuscation, and using tamper-proof hardware tokens to achieve general code obfuscation. Following this last line this work presents the first scheme which bases general code obfuscation of multiple programs on one single stateless hardware token.

Our construction is proven secure in the UC-framework and proceeds in three steps:

1. We construct an obfuscation scheme based on fully homomorphic encryption (FHE) and a hybrid functionality conditional decrypt, which decrypts the result of a homomorphic computation given a proof that the computation was performed as intended. One difficulty of the first step are possible decryptions errors in the FHE. These decryption errors can occur whenever the randomness for the encryption is chosen maliciously by the receiver of the obfuscated code. Such decryption errors then could make a real obfuscated computation distinguishable from a black box use of the non-obfuscated program.

2. Given two common reference strings (CRS) we construct a UC-protocol realizing the functionality conditional decrypt with a stateless hardware token.

As the token is stateless it is resettable by a dishonest receiver and the proofs given to the token must be resettably sound. One additional difficulty occurs when the issuer of the token can be corrupted. A malicious token can be stateful and it cannot be prevented that it aborts after a hardwired number of invocations. To prevent adaptive behavior of a malicious token the data of the receiver has to be hidden from the token and the proofs given to the token must even hide the size of the program and the length of the computation.

3. Last we construct a protocol constructing a CRS with a stateless hardware token. Care has to be taken here to not let the token learn anything about the resulting CRS which could not be simulated, because the very same token will later be used in a protocol based on the security of this CRS.

3.15 Oblivious Transfer with Anonymous Access Control and Pricing

Gregory Neven (IBM Research – Zürich, CH)

This talk unifies several schemes in a line of work that combines oblivious transfer (OT) protocols with anonymous credentials. It shows how to enhance a basic OT protocol (presented at Eurocrypt 2007) to support priced records (Financial Cryptography 2010) and anonymous access control with known (ACM CCS 2009) and hidden policies (PKC 2011).

3.16 On the Joint Security of Encryption and Signature, Revisited

Kenny Paterson (Royal Holloway University – London, GB)

Joint work of Paterson, Kenneth G.; Schuldt, Jacob C.N.; Stam, Martijn; Thomson, Susan
Main reference K.G. Paterson, J.C.N. Schuldt, M. Stam, S. Thomson, "On the Joint Security of Encryption and Signature, Revisited," Advances in Cryptology – ASIACRYPT 2011, pp. 161–178, LNCS Vol. 7073.
URL http://dx.doi.org/10.1007/978-3-642-25385-0_9

We revisit the topic of joint security for combined public key schemes, wherein a single keypair is used for both encryption and signature primitives in a secure manner. While breaking the principle of key separation, such schemes have attractive properties and are sometimes used in practice. We give a general construction for a combined public key scheme having joint security that uses IBE as a component and that works in the standard model. We provide a more efficient direct construction, also in the standard model. We then consider the problem of how to build signcryption schemes from jointly secure combined public key schemes. We provide a construction that uses any scheme to produce a triple of schemes signature, encryption and signcryption that are jointly secure in an appropriate and strong security model.

3.17 Hidden Vector Encryption Fully Secure Against Unrestricted Queries – No Query Left Unanswered

Giuseppe Persiano (University of Salerno, IT)

Joint work of De Caro, Angelo; Iovino, Vincenzo; Persiano, Giuseppe;
Main reference A. De Caro, V. Iovino, G. Persiano, "Hidden Vector Encryption Fully Secure Against Unrestricted Queries," IACR Cryptology ePrint Archive, 2011/546, 2011.
URL http://eprint.iacr.org/2011/546

Predicate encryption is an important cryptographic primitive that enables fine-grained control on the decryption keys. Roughly speaking, in a predicate encryption scheme the owner of the master secret key can derive secret key sk_P, for any predicate P from a specified class of predicates. In encrypting a message, the sender can specify an attribute vector and the resulting ciphertext $\tilde{X}$ can be decrypted only by using keys sk_P such that $P(\vec{x}) = 1$.

Our main contribution is the *first* construction of a predicate encryption scheme that can be proved *fully* secure against *unrestricted* queries by probabilistic polynomial-time adversaries under non-interactive constant sized (that is, independent of the length ℓ of the attribute vectors) hardness assumptions on bilinear groups of composite order.

Specifically, we consider *hidden vector encryption* (HVE in short), a notable case of predicate encryption introduced by Boneh and Waters. In a HVE scheme, the ciphertext attributes are vectors $\vec{x} = \langle x_1, \ldots, x_\ell \rangle$ of length ℓ over alphabet Σ, keys are associated with vectors $\vec{y} = \langle y_1, \ldots, y_\ell \rangle$ of length ℓ over alphabet $\Sigma \cup \{\star\}$ and we consider the $\mathsf{Match}(\vec{x}, \vec{y})$ predicate which is true if and only if, for all i, $y_i \neq \star$ implies $x_i = y_i$. Previous constructions restricted the proof of security to adversaries that could ask only *non-matching* queries; that is, for challenge attribute vectors $\vec{x}_0$ and $\vec{x}_1$, the adversary could ask only for keys of vectors $\vec{y}$ for which $\mathsf{Match}(\vec{x}_0, \vec{y}) = \mathsf{Match}(\vec{x}_1, \vec{y}) =$ false.

Our proof employs the dual system methodology of Waters, that gave one of the first fully secure construction in this area, blended with a careful design of intermediate security games that keep into account the relationship between challenge ciphertexts and key queries.

3.18 Commitments and Efficient Zero- Knowledge from Hard Learning Problems

Krzysztof Pietrzak (IST Austria – Klosterneuburg, AT)

Joint work of Jain, Abhishek; Pietrzak, Krzysztof; Tentes, Aris

I'll first show a simple (non-interactive) perfectly binding string commitments scheme whose security (i.e. hiding property) relies on the learning parity with noise (LPN) problem.

Next, I'll give an efficient zero-knowledge proof of knowledge (a Σ-protocol) for any linear function of the secret used to generate LPN instances.

Combining these results, we get a very simple string commitment scheme which allows to efficiently (but interactively) open any linear function (e.g. a subset) of the committed string, while revealing no other information. We borrow ideas from Stern [CRYPTO'93], and for the special case where one opens an "empty" commitment, our protocol can be seen as a "dual" version of Stern's public-key identification protocol.

3.19 Careful with Composition: Limitations of Indifferentiability and Universal Composability

Thomas Ristenpart (University of Wisconsin – Madison, US)

URL http://eprint.iacr.org/2011/339

We exhibit a hash-based storage auditing scheme which is provably secure in the random-oracle model (ROM), but easily broken when one instead uses typical indifferentiable hash constructions. This contradicts the widely accepted belief that the indifferentiability composition theorem applies to any cryptosystem. We characterize the uncovered limitation of the indifferentiability framework by showing that the formalizations used thus far implicitly exclude security notions captured by experiments that have multiple, disjoint adversarial stages. Examples include deterministic public-key encryption (PKE), password- based cryptography, hash function nonmalleability, key-dependent message security, and more. We formalize a stronger notion, reset indifferentiability, that enables an indifferentiability-style composition theorem covering such multi-stage security notions, but then show that practical hash constructions cannot be reset indifferentiable. We discuss how these limitations also affect the universal composability framework. We finish by showing the chosen-distribution attack security (which requires a multi-stage game) of some important public-key encryption schemes built using a hash construction paradigm introduced by Dodis, Ristenpart, and Shrimpton.

3.20 Pseudo Random Functions and Lattices

Alon Rosen (The Interdisciplinary Center – Herzliya, IL)

Joint work of Banerjee, Abhishek; Peikert, Chris; Rosen, Alon
Main reference A. Banerjee, C. Peikert, A. Rosen, "Pseudorandom Functions and Lattices," IACR Cryptology ePrint Archive, 2011/401, 2011.
URL http://eprint.iacr.org/2011/401

We give direct constructions of pseudorandom function (PRF) families based on conjectured hard lattice problems and learning problems. Our constructions are asymptotically efficient and highly parallelizable in a practical sense, i.e., they can be computed by simple, relatively *small* low-depth arithmetic or boolean circuits (e.g., in NC^1 or even TC^0). In addition, they are the first low-depth PRFs that have no known attack by efficient quantum algorithms.

Central to our results is a new "derandomization" technique for the learning with errors (LWE) problem which, in effect, generates the error terms deterministically.

3.21 Identification and Signatures Based on NP-Hard Problems of Indefinite Quadratic Forms

Claus Peter Schnorr (Goethe-Universität Frankfurt am Main, DE)

Joint work of Hartung, Rupert J.; Schnorr, Claus Peter;
Main reference R.J. Hartung, C.P. Schnorr, "Identification and signatures based on NP-hard problems of indefinite quadratic forms," in J. Math. Crypt., 2(4), pp. 327–341.

Quadratic form cryptography covers both lattice cryptography and factoring cryptography. While the lattice problems **SVP** and **CVP** of finding shortest and closest lattice vectors are only **NP**-hard for large, non constant dimension n representation and equivalence problems for quadratic forms are already **NP**-hard for dimension $n = 3$. While integers N can be factored in subexponential time solving **NP**-hard problems, with a reduction from **3SAT** that merely linearly increases the bit length, require exponential time as **3SAT** requires exponential time for all known algorithms.

The following problems **CBR** of finding small representations of integers and **CBE** of finding small equivalence transforms are **NP**-hard for indefinite, quadratic forms of arbitrary dimension $n \geq 3$.

CBR: Given an n-ary quadratic form f and an integer $m \in \mathbb{Z}$
Find a representation $x \in \mathbb{Z}^n$ with a given bound, i.e., $f(x) = m$.
CBE: Given two equivalent n-ary quadratic forms f_0, f_1
Find an equivalence transform $T \in GL_n(\mathbb{Z})$ with a given bound.

We present a practical identification scheme and a corresponding signature scheme on quaternary quadratic forms ($n = 4$) for which the best known attacks require to solve **NP**-hard problems and require exponential time. We use **CBE** of anisotropic forms.

3.22 Security of Blind Signatures Revisited

Dominique Schroeder (University of Maryland – College Park, US)

Joint work of Schroeder, Dominique; Unruh, Dominique
Main reference U. Schroeder, D. Unruh, "Security of Blind Signatures Revisited," IACR Cryptology ePrint Archive, 2011/316, 2011.
URL http://eprint.iacr.org/2011/316

We revisit the definition of unforgeability of blind signatures as proposed by Pointcheval and Stern (Journal of Cryptology 2000). Surprisingly, we show that this established definition falls short in two ways of what one would intuitively expect from a secure blind signature scheme: It is not excluded that an adversary submits the same message m twice for signing, and then produces a signature for $m' \neq m$. The reason is that the forger only succeeds if *all* messages are distinct. Moreover, it is not excluded that an adversary performs k signing queries and produces signatures on $k + 1$ messages as long as *each* of these signatures does not pass verification with probability 1.

Finally, we proposed a new definition, honest-user unforgeability, that covers these attacks. We give a simple and efficient transformation that transforms any unforgeable blind signature scheme (with deterministic verification) into an honest-user unforgeable one.

3.23 Integrity Notions for Encryption Schemes

Bjoern Tackmann (ETH Zürich, CH)

Joint work of Maurer, Ueli; Rueedlinger, Andreas; Tackmann, Bjoern;

The fundamental goal of encryption schemes is to protect the confidentiality of the encrypted plaintext messages. Some applications, however, require the encryption scheme to additionally guarantee some type of integrity: A prime example is the Authenticate-then-Encrypt transformation used, e.g., in TLS.

The security definitions for such confidentiality or integrity guarantees that appear in the literature are mostly game-based and do not provide any composability guarantees. Moreover, their exact semantics often remain unclear.

In this work, we use the approach of constructive cryptography for a systematic treatment of confidentiality and integrity, questioning the justification for the existing game-based security properties. We translate previous game-based notions into integrity guarantees of channels, and find that some of the considered notions are too weak, such as INT-PTXT, some are appropriate, and others are too strong, such as INT-CTXT. Some notions have semantics that appear inappropriate for symmetric encryption, such as IND-CCA.

3.24 The equivalence of the random oracle model and the ideal cipher model, revisited.

Stefano Tessaro (University of California – San Diego, US)

Joint work of Holenstein, Thomas; Künzler, Robin; Tessaro, Stefano;
Main reference T. Holenstein, R. Künzler, S. Tessaro, "The equivalence of the random oracle model and the ideal cipher model, revisited," in Proc. 43rd ACM Symp. on Theory of Computing (STOC'11), pp. 89–98, 2011.
URL http://dx.doi.org/10.1145/1993636.1993650

We consider the cryptographic problem of constructing an invertible random permutation from a public random function (i.e., which can be accessed by the adversary). This goal is formalized by the notion of indifferentiability of Maurer et al. (TCC 2004). This is the natural extension to the public setting of the well-studied problem of building random permutations from random functions, which was first solved by Luby and Rackoff (Siam J. Comput., '88) using the so-called Feistel construction.

The most important implication of such a construction is the equivalence of the random oracle model (Bellare and Rogaway, CCS '93) and the ideal cipher model, which is typically used in the analysis of several constructions in symmetric cryptography.

Coron et al. (CRYPTO 2008) gave a rather involved proof that the six-round Feistel construction with independent random round functions is indifferentiable from an invertible random permutation. Also, it is known that fewer than six rounds do not suffice for indifferentiability. The first contribution (and starting point) of our paper is a concrete distinguishing attack which shows that the indifferentiability proof of Coron et al. is not correct. In addition, we provide supporting evidence that an indifferentiability proof for the six-round Feistel construction may be very hard to find.

To overcome this gap, our main contribution is a proof that the Feistel construction with eigthteen rounds is indifferentiable from an invertible random permutation. The approach of our proof relies on assigning to each of the rounds in the construction a unique and specific role needed in the proof. This avoids many of the problems that appear in the six-round case.

3.25 Secure Computation with Corruptible Setups

Vassilis Zikas (University of Maryland – College Park, US)

Joint work of Katz, Jonathan; Kiayias, Aggelos; Zikas, Vassilis; Zhou, Hong-Sheng

Universally composable (UC) protocols satisfy strong and desirable security properties. Unfortunately, soon after the introduction of the UC framework it was shown that in the "plain" model most cryptographic tasks cannot be realized without an honest majority. Researchers since then have therefore proposed various forms of "trusted setup", and have shown many setups that are *complete* and can thus be leveraged to securely carry out any desired task.

With only a few notable exceptions, past work has viewed these setup assumptions as being implemented by some ideal, incorruptible entity. In reality, however, setups would likely be carried out by some mechanism that could be subverted, or by some party that could be compromised. Most prior work provides no guarantees in such cases.

We propose here a clean, general, and generic approach for modeling potential corruption of setups within the UC framework, where such corruption might be fail-stop, passive, or arbitrary and is in addition to possible corruption of the parties. We also show several results regarding feasibility in this model for these corruption types (and their combinations) for different specifications of the corruptible sets. For example, we show that given m complete setups, any t of which might be actively corrupted, general secure computation is possible iff $t < m/2$ even when arbitrarily many parties are actively corrupted.

4 Working Groups

Because one of the most renowned conferences in our area, Eurocrypt, had the submission deadline on Sept 30th, some researchers took the opportunity to prepare their submission with attending colleagues and submit from Dagstuhl. Our feedback was that, being able to work with one's co-authors face to face, was in fact one of the nice side effects of this seminar. We currently know of more than half a dozen submissions to Eurocrypt which have been worked out to the final state during the seminar.

5 Open Problems

The interest in hash functions, one of the three main areas of interest of the seminar, was decent but smaller than expected, with only a few talks covering this topic. Here, the participants mainly discussed model-related issues with "idealized" hash functions (so-called random oracles), which are not know to yield the desired impact on the standardization process. Instead, the general idea of "constructive cryptography", presented by one of the organizers, Ueli Maurer, as a new view on cryptography incited many discussions. We found the occasion at Dagstuhl a perfect setting to put such a topic to scrutiny.

6 Panel Discussions

The panel discussion on the "Future of Public-Key Cryptography" revealed that the area of (public-key) cryptography is by no means a closed area, despite the fact that basic primitives for digital signatures and encryption are known for decades now. Instead, new challenges arise permanently through the changing environment in which crypto is used. Some participants expressed their wish to work more towards bridging applied security and cryptography but the general consensus was that the current seminar is —and should be— the platform for public-key cryptography as a whole.

7 Scientific Output

As for now, we know of at least the following four publications that, to some extent, originated from joint collaborations at the Dagstuhl seminar.

- Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs, "Message Authentication, Revisited", accepted at Eurocrypt 2012.
- Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer,"Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding", accepted at Eurocrypt 2012.
- Dennis Hofheinz, "All-But-Many Lossy Trapdoor Functions", accepted at Eurocrypt 2012.

Participants

- Anja Becker
University of Versailles, FR
- Johannes Blömer
Universität Paderborn, DE
- Jan Camenisch
IBM Research – Zürich, CH
- Melissa Chase
Microsoft Res. – Redmond, US
- Yvo Desmedt
University College London, GB
- Yevgeniy Dodis
New York University, US
- Pooya Farshim
TU Darmstadt, DE
- Marc Fischlin
TU Darmstadt, DE
- Juan A. Garay
AT&T Res. – Florham Park, US
- Dennis Hofheinz
KIT – Karlsruhe Institute of Technology, DE
- Thomas Holenstein
ETH Zürich, CH
- Yuval Ishai
Technion – Haifa, IL
- Antoine Joux
University of Versailles, FR
- Eike Kiltz
Ruhr-Universität Bochum, DE
- Anja Lehmann
IBM Research – Zürich, CH
- Stefan Lucks
Bauhaus-Universität Weimar, DE
- Ueli Maurer
ETH Zürich, CH
- Alexander May
Ruhr-Universität Bochum, DE
- Alexander Meurer
Ruhr-Universität Bochum, DE
- Jörn Müller-Quade
KIT – Karlsruhe Institute of Technology, DE
- Gregory Neven
IBM Research – Zürich, CH
- Tatsuaki Okamoto
NTT Labs. – Tokyo, JP
- Kenneth G. Paterson
RHUL – London, GB
- Giuseppe Persiano
University of Salerno, IT
- Krzysztof Pietrzak
IST Austria – Klosterneuburg, AT
- Thomas Ristenpart
University of Wisconsin – Madison, US
- Alon Rosen
The Interdisciplinary Center – Herzliya, IL
- Claus Peter Schnorr
Goethe-Universität Frankfurt am Main, DE
- Dominique Schroeder
University of Maryland – College Park, US
- Björn Tackmann
ETH Zürich, CH
- Stefano Tessaro
University of California – San Diego, US
- Bogdan Warinschi
University of Bristol, GB
- Vassilis Zikas
University of Maryland – College Park, US