07381 Abstracts Collection
Cryptography
— Dagstuhl Seminar —

Johannes Blömer[1], Dan Boneh[2], Ronald Cramer[3] and Ueli Maurer[4]

[1] Univ. Paderborn, DE
[2] Stanford University, US
dabo@cs.stanford.edu
[3] CWI - Amsterdam, NL
cramer@cwi.nl
[4] ETH Zürich, CH
maurer@inf.ethz.ch

Abstract. From 16.09.2007 to 21.09.2007 the Dagstuhl Seminar 07381 "Cryptography" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Cryptography, information security, public-key cryptography, cryptographic protocols, security proofs

07381 Executive Summary – Cryptography

0.1 Introduction and Motivation

Cryptography is of paramount importance for information security. Cryptographic primitives are the core building blocks for constructing secure systems. The last three decades have seen tremendous progress in cryptography and the field has substantially matured. Major achievements include the proposal of adequate security definitions, of new cryptographic schemes, and of security proofs for these schemes, relative to the security definition. As a consequence, cryptography has shifted from an ad-hoc discipline with many interesting tricks and ideas to a mathematically rigorous science. Despite this progress many essential problems in cryptography still remain open and new areas and topics arise constantly. The field is more lively than ever before.

While the number of scientific conferences focusing on cryptography is increasing, most of these meetings have a broad focus, and due to a growing interest by practitioners, the number of non-expert attendees has increased. As

Dagstuhl Seminar Proceedings 07381
Cryptography
http://drops.dagstuhl.de/opus/volltexte/2008/1293

a result, it becomes more difficult to discuss the details of the advancement of the field, as well as to identify promising innovative trends. Therefore, the aim of the seminar was to provide an opportunity for key cryptographers to meet, to interact, to focus on the scientific foundation of cryptography, to spot the emerging new areas, and to work on them. Applications were also covered but the emphasis was on the conceptual framework that allows the use of appropriate models, amenable to mathematical reasoning.

0.2 Participation, Organization, and Atmosphere

The seminar brought together about 40 leading cryptographers from all over the world. Almost all participants gave a presentation about their recent research and also about future research plans they have, encouraging others to join in. In many cases the choice of the subject for the talk was targeted to the unique list of participants. The presentations were highly interactive and led to lively discussions, well into the evenings and nights. A number of new collaborations were initiated at the seminar. Overall, the seminar was a great success, as is also documented by the feedback given by the participants on the questionnaires.

0.3 Summary of Topics

The topics covered in the seminar spanned most areas of cryptography, in one way or another, both in terms of the types of schemes (public-key cryptography, symmetric cryptography, hash functions and other cryptographic functions, multi-party protocols, etc.) and in terms of the mathematical methods and techniques used (algebra, number theory, elliptic curves, probability theory, information theory, combinatorics, quantum theory, etc.). The range of applications addressed in the various talks was broad, ranging from secure communication, key management, authentication, digital signatures and payment systems to e-voting and Internet security.

While the initial plan had been to focus more exclusively on public-key cryptography, it turned out that this sub-topic branches out into many other areas of cryptography and therefore the organizers decided to expand the scope, emphasizing quality rather than close adherence to public-key cryptography. This decision turned out to be a wise one.

What was common to almost all the talks is that rigorous mathematical proofs for the security of the presented schemes were given. In fact, a central topic of many of the talks were proof methodologies for various contexts.

Keywords: Cryptography, information security, public-key cryptography, cryptographic protocols, security proofs

Joint work of: Blömer, Johannes; Boneh, Dan; Cramer, Ronald; Maurer, Ueli

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1292

New Techniques for Cryptanalysis of Hash Functions and Improved Attacks on Snefru

Eli Biham (Technion - Haifa, IL)

In this talk we present new techniques for the cryptanalysis of hash functions that allow the implementation of prior attacks with additional properties, and to reach previously impossible results. The first technique shows how to use generic attacks within the scope of differential cryptanalysis, and in particular the Floyd and Nivasch cycle detection and collision finding algorithms in order to find collisions. We use this technique to show the first found collision of 3-pass Snefru. The second technique uses virtual messages (that do not exist in practice) with a second preimage attack in order to find a preimage of the compression function. We also observe how the padding scheme of the hash function affects the ability to find preimages of the full hash function, and present a very long preimage of Snefru.

Keywords: Hash functions, Snefru, differential cryptanalysis, collisions, preimages

Space-Efficient Identity Based Encryption Without Pairings

Dan Boneh (Stanford University, USA)

Identity Based Encryption (IBE) systems are often constructed using bilinear maps (a.k.a. pairings) on elliptic curves. One exception is an elegant system due to Cocks which builds an IBE based on the quadratic residuosity problem modulo an RSA composite N. The Cocks system, however, produces long ciphertexts. Since the introduction of the Cocks system in 2001 it has been an open problem to construct a space efficient IBE system without pairings. In this paper we present an IBE system in which ciphertext size is short: an encryption of an ℓ-bit message consists of a single element in $\mathbb{Z}_N$ plus $\ell+1$ additional bits. Security, as in the Cocks system, relies on the quadratic residuosity problem. The system is based on the theory of ternary quadratic forms and as a result, encryption and decryption are slower than in the Cocks system.

Keywords: Identity Based Encryption, Quadratic Residousity, Public-key cryptography

Joint work of: Boneh, Dan; Gentry, Craig; Hamburg, Michael

Full Paper:
http://crypto.stanford.edu/∼dabo/abstracts/bgh.html

A tour of set-up assumptions for obtaining UC security

Ran Canetti (IBM TJ Watson Research Center - Hawthorne, USA)

A desirable goal for cryptographic protocols is to guarantee security when the protocol is composed with other protocol instances.

Universally Composable (UC) security provides this guarantee in a strong sense: A UC-secure protocol maintains its security properties even when composed concurrently with an unbounded number of instances of arbitrary protocols. However, many interesting cryptographic tasks are provably impossible to realize with UC security, unless some trusted set-up is assumed. Impossibility holds even if ideally authenticated communication channels are provided.

The talk will examine and compare a number of set-up assumptions (models) that were recently demonstrated to suffice for constructing UC-secure protocols that realize practically any cryptographic task. We start with the common reference string (CRS) and key registration (KR) models. We then proceed to the "sunspot" models, which allow for some adversarial control over the set-up, a number of models which better captures set-up that is globally available in the system, and a timing assumption.

Finally, we briefly touch upon set-up models for obtaining authenticated communication.

Keywords: Security analysis, composable security, set-up assumptions

Simulatable Verifiable Random Functions

Melissa Chase (Brown Univ. - Providence, USA)

We introduce simulatable verifiable random functions (sVRF). VRFs are similar to pseudorandom functions, except that they are also verifiable: corresponding to each seed sk, there is a public key pk, and for $y = F_{pk}(x)$, it is possible to prove that y is indeed the value of the function seeded by sk. A simulatable VRF is a VRF for which this proof can be simulated, so a simulator can pretend that the value of $F_{pk}(x)$ is any y. We begin by introducing the notion and formal definitions of sVRFs. (joint work with Anna Lysyanskaya.)

We then present a new construction of sVRFs. This construction uses an asymmetric bilinear map $e : G_1 \times G_2 \to G_T$. It is based on the SDHI assumption in G_1 and uses the Groth Sahai bilinear map commitment and proof system (which can be based on either the SXDH or the decisional linear assumption). The input domain must be polynomial size, and the output is pseudorandom over G_1. (joint work with Mira Belenkiy, Markulf Kohlweiss, and Anna Lysyanskaya).

Keywords: Verifiable Random Functions, Pseudorandom Functions

Joint work of: Belenkiy, Mira; Chase, Melissa; Kohlweiss, Markulf; Lysyanskaya, Anna

Combinatorial authentication codes secure against related-key attacks and their applications

Ronald Cramer (CWI - Amsterdam, NL)

We introduce a class of combinatorial authentication codes that withstand certain related-key attacks. Consider the standard notion of security for combinatorial authentication codes, i.e., security against impersonation and substitution attacks. Our notion requires that security is guaranteed even if the attacker can algebraically modify the secret key of the receiver.

We show that these codes have interesting applications to fuzzy randomness extractors (which in turn are applicable in certain settings of biometric identification), secure message transmission and robust secret sharing.

Finally, we show how to construct nearly optimal combinatorial authentication codes secure against related-key attacks from certain classes of cyclic error correcting codes.

Keywords: Cryptography, authentication codes, error correcting codes, randomness extractors, secret sharing, secure message transmission, biometric identification

Joint work of: Cramer, Ronald; Dodis, Yevgeniy; Fehr, Serge; Padro', Carles; Wichs, Daniel

Applying Recreational Mathematics to Secure Multiparty Computation

Yvo Desmedt (Univ. College London, GB)

The problem of a mouse traveling through a maze is well known. The maze can be represented using a planar graph. We present a variant of the maze. We consider a grid vertex colored planar graph in which an adversary can choose up to t colors and remove all vertices that have these colors and their adjacent edges. We call the grid in which these vertices and adjacent edges are removed a reduced grid. The problem is that a mouse must be able to move in the reduced grid from the first row to the last row, and from the first column to the last column, and this for all possible reductions. We present three types of solutions to construct such grids. The efficiency of these solutions is discussed.

The problem finds its origin in the problem of secure multiparty computation. We consider the problem of parties each having a secret belonging to a non-abelian group. The parties want to compute the product of these secrets without leaking anything that does not follow trivially from the product. Our solution is black box, i.e., independent of the non-abelian group. This has applications to threshold block ciphers and post-quantum cryptography.

Keywords: Multi-party computation, private and reliable computation, non-abelian groups

Does Privacy Require True Randomness?

Yevgeniy Dodis (Courant Institute - New York, USA)

All known techniques for achieving privacy seem to fundamentally require (nearly) perfect randomness. We ask the question whether this is just a coincidence, or, perhaps, privacy inherently requires true randomness?

We resolve this question for the case of (information-theoretic) private-key encryption, where parties wish to encrypt a b-bit value using an n-bit shared secret key sampled from some imperfect source of randomness S. Our main result shows that if such n-bit source S allows for a secure encryption of b bits, where b > log n, then one can deterministically extract nearly b almost perfect random bits from S.

Moreover, the restriction that b > log n is nearly tight.

Hence, to a large extent, true randomness is inherent for encryption: either the key length must be exponential in the message length b, or one can deterministically extract nearly b almost unbiased random bits from the key. In particular, ** the one-time pad scheme is essentially "universal" **

Our technique also extends to related *computational* primitives which are "perfectly-binding", such as perfectly-binding commitment and computationally secure private- or public-key encryption, showing the necessity to *efficiently* extract almost b *pseudorandom* bits.

Keywords: Randomness, extraction, privacy, encryption

Joint work of: Dodis, Yevgeniy; Bosley, Carl

Full Paper:
http://people.csail.mit.edu/dodis/ps/enc-ext.ps

Randomness Extraction via Delta-Biased Masking in the Presence of a Quantum Attacker

Serge Fehr (CWI - Amsterdam, NL)

Randomness extraction is of fundamental importance for information-theoretic cryptography.

It allows to transform a raw key about which an attacker has some limited knowledge into a fully secure random key, on which the attacker has essentially no information.

We show that randomness extraction by means of xor'ing a so-called delta-biased mask to the raw key is secure also in case where the attacker has quantum information on the raw key. Up to date, only very few techniques are known to work against a quantum attacker, much in contrast to the classical (non-quantum) setting, which is much better understood and for which a vast amount of different techniques for randomness extraction are known. We show how the new randomness-extraction technique allows to do error-correction without leaking partial information to a quantum attacker. Such a technique is useful in settings where the raw key may contain errors, since standard error-correction techniques may provide the attacker with information on, say, a secret key that was used to obtain the raw key.

An additional application, which I will not talk about, is to entropically secure encryption.

Keywords: Quantum cryptography, randomness extraction, small-biased sets

Joint work of: Fehr, Serge; Schaffner, Christian

On the Impossibility of Three-Move Blind Signature Schemes

Marc Fischlin (TU Darmstadt, D)

We investigate the possibility to build blind signature schemes in which the interactive signature issuing between the signer and the user can be achieved in three (or less) moves. While such protocols are known to exist in the random oracle model and the common reference string model, currently the best protocol in the standard model by Okamoto requires four moves. Here we give indications that schemes with three moves in the standard model are hard to achieve. This also sheds some light on the hardness of instantiating the random oracles in the schemes by Chaum and by Pointcheval and Stern.

Keywords: Blind signature scheme, black-box reduction

Joint work of: Fischlin, Marc; Schröder, Dominique

How to Share a Key

Matthias Fitzi (ETH Zürich, CH)

The problem of asynchronous perfectly secure communication via one-time pads (OTP) has been recently introduced by Di Crescenzo and Kiayias.

There, several players share the same OTP to be used in parallel but it is not known in advance which players will consume how many bits of the pad. Based on the common OTP and only partial local knowledge of how many key bits have already been used by each other player, the goal is to commonly consume as many key bits as possible without any overlap.

In this paper, we consider a related problem with immediate implications to the previous model. We consider n players to share the same k keys of length bits. The goal is to assign a key sequence to each player such that, for as many keys as possible and independently of which player uses how many of them, it is guaranteed that all used keys are independent. Such an assignment is called

loss-free if k keys can always be consumed independently. Note that, in contrast to the previous model, the players are ignorant of each other's key consumptions. We first observe a simple loss-free solution for the case that the key is of certain (small) minimal length . Furthermore, for the case of key length $= 1$ (the most general case), we show that loss-free assignments are possible if and only if the number of players is at most three. Our solutions directly apply to the model of Di Crescenzo and Kiayias. For the case $n = 3$, we strictly improve over their solution.

For $n > 3$, we still partially improve over their solution despite the fact that our construction is simple and oblivious.

Keywords: How, loss-free, one-time pad, parallel use, perfect security

Joint work of: Fitzi, Matthias; Nielsen, Jesper Buus; Wolf, Stefan

Security Under Key-Dependent Inputs

Shai Halevi (IBM TJ Watson Research Center - Yorktown Heights, USA)

In this work we re-visit the question of building cryptographic primitives that remain secure even when queried on inputs that depend on the secret key.

This was investigated by Black, Rogaway, and Shrimpton in the context of randomized encryption schemes and in the random oracle model. We extend the investigation to deterministic symmetric schemes (such as PRFs and block ciphers) and to the standard model. We term this notion "security against key-dependent-input attack", or KDI-security for short. Our motivation for studying KDI security is the existence of significant real-world implementations of deterministic encryption (in the context of storage encryption) that actually rely on their building blocks to be KDI secure.

We consider many natural constructions for PRFs, ciphers, tweakable ciphers and randomized encryption, and examine them with respect to their KDI security. We exhibit inherent limitations of this notion and show many natural constructions that fail to be KDI secure in the standard model, including some schemes that have been proven in the random oracle model. On the positive side, we demonstrate examples where some measure of KDI security can be provably achieved (in particular, we show such examples in the standard model).

Keywords: Circular encryption, Key-dependent input, Self encryption

Joint work of: Halevi, Shai; Krawczyk, Hugo

Full Paper:
http://eprint.iacr.org/2007/315

See also: ACM-CCS 2007

Towards Key-Dependent Message Security in the Standard Model

Dennis Hofheinz (CWI - Amsterdam, NL)

Standard security notions for encryption schemes do not guarantee any security if the encrypted messages depend on the secret key. Yet it is exactly the stronger notion of security in the presence of *key-dependent* messages (KDM security) that is required in a number of applications: most prominently, KDM security plays an important role in analyzing cryptographic multi-party protocols in a formal calculus. But although often assumed, the mere existence of KDM secure schemes is an open problem. The only previously known construction was proven secure in the random oracle model.

We present symmetric encryption schemes that are KDM secure in the standard model (i.e., without random oracles). The price we pay is that we achieve only a relaxed (but still useful) notion of key-dependent message security. Our work answers (at least partially) an open problem posed by Black, Rogaway, and Shrimpton. More concretely, our contributions are as follows: - We present a (stateless) symmetric encryption scheme that is information-theoretically secure in face of a *bounded* number and length of encryptions for which the messages depend in an arbitrary way on the secret key. - We present a stateful symmetric encryption scheme that is computationally secure in face of an arbitrary number of encryptions for which the messages depend only on the respective *current* secret state/key of the scheme. The underlying computational assumption is minimal: we assume the existence of one-way functions. - We give evidence that the only previously known KDM secure encryption scheme cannot be proven secure in the standard model (i.e., without random oracles).

Keywords: Key-dependent message security, security

Joint work of: Hofheinz, Dennis; Unruh, Dominique

MPC in the Head

Yuval Ishai (Technion - Haifa, IL)

I will survey a recent approach for designing secure two-party protocols via the use of secure multi-party computation (MPC) protocols.

The first part of the talk (joint work with Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai) will describe a way to obtain a zero-knowledge proof for a given NP language by making a black-box use of any MPC protocol for a related n-party functionality. The latter protocol only needs to be secure against a small number of "honest-but-curious" parties. This new connection allows us to draw on a large body of techniques for MPC with honest majority in order to improve the efficiency of zero-knowledge proofs.

The second part of the talk (ongoing joint work with Danny Harnik, Eyal Kushilevitz, and Jesper Nielsen) will describe a new general connection between MPC and OT combiners that has applications to the efficiency of secure two-party computation.

Keywords: Secure multiparty computation, zero-knowledge proofs, oblivious transfer

Twinning Diffie and Hellman

Eike Kiltz (CWI - Amsterdam, NL)

We propose the strong twin Diffie-Hellman assumption, a new interactive assumption that we prove weaker than the standard Diffie-Hellman (DH) assumption. We use it to construct the first redudancy-free public-key encryption scheme based on the DH assumption. We find several other applications for these ideas, including non-interactive authenticated key exchange, securing password authenticated key exchange against server compromise, and redundancy-free identity-based encryption.

Keywords: Diffie-Hellman problem, Twin Diffie-Hellman problem, redundancy-free public-key encryption

Joint work of: Cash, David; Kiltz, Eike; Shoup, Victor

Cryptography in Constant Parallel Time

Eyal Kushilevitz (Technion - Haifa, IL)

The talk gives a survey of the recent line of work on the subject.

In particular, we are interested in implementing cryptographic primitives in the complexity class NC^0, that consists of all functions where each output bit depends on a constant number of input bits. We are also interested in implementations where each input bit depends on a constant number of output bits and implementations that simultaneously achieve both properties. Such implementations are of interest both from the theoretical point of view and for obtaining parallel cryptography.

Among other things, we prove that any implementation of basic cryptographic primitives (such as one-way function, pseudorandom generators, encryption and more) in the complexity class NC^1 (such implementations exist under most common cryptographic assumptions, like the intractability of factoring) implies an NC^0 implementation for those primitives.

Keywords: Parallel cryptography, one-way functions, pseudorandom generators

Joint work of: Kushilevitz, Eyal; AppleBaum, Benny; Ishai, Yuval

Random systems

Ueli Maurer (ETH Zürich, CH)

Most cryptographic systems can be modeled as a discrete system which interacts with its environment by taking a sequence of inputs and producing, for each new input, an output. The number of interactions can be fixed (e.g. one) or unbounded. In most contexts, only the *observable* input-output behavior of a system, but not the internal state representation, is of interest. For example, if one considers the distinguishing advantage of a certain distinguisher D for two systems F and G, then all that matters is the input-output behavior of the systems D, F and G. The abstraction capturing the input-output behavior of a system is called a random system and is, mathematically, a sequence of conditional probability distributions. This is in the same spirit as a communication channel in communication theory is abstracted as a conditional probability distribution $P_{Y|X}$ of the output Y, given the input X, independently of the physical description of the channel.

One purpose of an abstraction is to make statements and proofs at the same time simpler, more general, and more elegant. In this talk we explore the power of the abstraction of random systems in cryptography.

Keywords: Cryptography, indistinguishability, random systems, security amplification

An Optimal RSA Broadcast Attack

Alexander May (TU Darmstadt, D)

We address the problem of polynomial time solving univariate modular equations with mutually co-prime moduli. For a given system of equations we determine up to which size the common roots can be calculated efficiently. We further determine the minimum number of equations which suffices for a recovery of all common roots. The result that we obtain is superior to Hastad's original RSA broadcast attack, even when Hastad's method is combined with the best known lattice technique due to Coppersmith. Namely, our reduction uses a slightly different transformation from polynomial systems to a single polynomial. Thus, our improvement is achieved by optimal polynomial modelling rather than improved lattice techniques. Moreover, we show by a counting argument that our results cannot be improved in general. A typical application for our algorithm is an improved attack on RSA with a smaller number of polynomially related messages.

Keywords: Univariate modular polynomial equations, RSA

Joint work of: May, Alexander; Ritzenhofen, Maike

Precise Cryptography

Rafael Pass (Cornell University - Ithaca, USA)

The seminal work of Goldwasser, Micali and Rackoff put forward a computational approach to knowledge in interactive systems, providing the foundation of modern Cryptography. Their notion, and its refinement by Goldriech, Micali and Wigderson, bounds the knowledge of a player in terms of his *potential* computational power, technically defined as its worst-case running-time. We put forward a stronger notion that precisely bounds the knowledge gained by a player in an interaction in terms of the *actual* computation it has performed in that *particular* interaction.

Our approach—which is exemplified in the contexts of zero-knowledge proofs, proofs of knowledge, encryption and secure computation—-not only remains valid even if P= NP, but is most meaningful when modeling knowledge of computationally easy properties.

Keywords: Zero Knowledge, Precision, Proofs of Knowledge, Encryption

Joint work of: Pass, Rafael; Micali, Silvio

Generic Attacks and Proofs of Security for the Xor of Random Permutations

Jacques Patarin (University of Versailles, F)

Xoring the output of k permutations, $k >= 2$, is a very simple way to construct pseudo-random functions from pseudo-random permutations.

In this talk we will be present the best known attacks on this construction, and the best known security results.

When $k = 2$ we will present a proof of security in $O(2^n)$ based on the "coefficients H technique".

Moreover, when $k >= 3$ we will see that if a few points are changed in the output, we obtain a construction that seems to be even much more secure, and that is still very simple to implement.

Keywords: Pseudorandom functions, pseudorandom permutations, security beyond the birthday bound, Luby-Rackoff backwards, generic attacks

Black-Box Combiners for Collision Resistance Really don't Exist

Krzysztof Pietrzak (CWI - Amsterdam, NL)

A black-box combiner for collision resistant hash functions (CRHF) is a construction which given black-box access to two hash functions is collision resistant if at least one of the components is collision resistant.

In this paper we prove a lower bound on the output length of black-box combiners for CRHFs.

The bound we prove is tight as it is achieved by a recent construction of Canetti et al [crypto'07]. Previously known lower bounds only applied to restricted constructions which either were deterministic (Boneh, Boyen [crypto'06], Pietrzak [eurocrypt'07]), or for constructions whose security proof required that the underlying hash-functions can be broken given a single collision for the combiner (Canetti et al [crypto'07]). Our proof uses a lemma similar to the elegant "reconstruction lemma" of Gennaro and Trevisan [focs'00], which states that any function which is not one-way is compressible (and thus uniformly random function must be one-way). In a similar vein we show that a function which is not collision resistant is compressible.

We also borrow ideas from recent work by Haitner et al. [FOCS'07], who show how to prove the reconstruction lemma even relative to a powerful "collision-finding" oracle.

Keywords: CRHF, combiner

Universal Hash Functions are Not So Universal

Bart Preneel (Katholieke Universiteit Leuven, B)

In this talk we demonstrate some very simple key recovery attacks on several universal hash function based MAC algorithms. The attacks use a substantial number of verification queries and in some cases require nonce reuse; this is realistic in settings in which the receiver is stateless or the nonce is a random number. Some of these attacks exploit weak keys, while others can make use of partial information on a secret key, for example, due to a side channel attack. These results show that while universal hash functions offer provable security, high speeds and parallelism, their simple combinatorial properties make them less robust than conventional message authentication primitives.

Keywords: Universal hash functions, message authentication codes, key recovery, cryptanalysis, side channel attacks

Joint work of: Preneel, Bart; Handschuh, Helena

Formalizing Human Ignorance + Permutation-Based Cryptographic Hashing

Phillip Rogaway (Univ. of California - Davis, USA)

The talk is of two unrelated parts. PART 1: There is a rarely mentioned foundational problem involving collision-resistant hash-functions: common constructions are keyless, while formal definitions are keyed.

The discrepancy stems from the fact that a function $H : \{0,1\}^* \rightarrow \{0,1\}^n$ always admits an efficient collision-finding adversary, it just that us humans are too dumb to find it. I explain that there's a simple and "almost known" way to sidestep this difficulty that avoids having to key the hash function: just state theorems in a way that prescribes an explicitly given reduction, normally a black-box one. PART 2: I discussed very recent work on how to construct a cryptographic hash function producing n or more output bits from a random permutation from n bits to n bits. The main construction, PHASH, can, for example, map $2n$ bits to n bits using three permutation calls, getting security close to the $2^{n/2}$. We also show that this number of permutation calls, three, is necessary as well as sufficient for $2 \rightarrow 1$ compression. More generally, we provide a matrix-parameterized construction, PHASH, for compressing mn bits to rn bits for any $m > r \geq 1$; and we look at lower bounds (attacks) on what is possible for permutation-based hashing with k calls.

Keywords: Cryptographic hash functions, cryptography, collision-resistant hash functions

Full Paper:
http://www.cs.ucdavis.edu/∼rogaway/papers

Applying Cryptography–lottery, anonymous authentication and voting

Kazue Sako (NEC - Kawasaki, J)

We discuss several trials of applying cryptography to the real world, on a belief that it would benefit people. The examples include fair digital lootery, anonymous authentication such as group signatures to enhance user privacy, and voting over network. We further present a new privacy requirement that we faced on designing a network voting for nominating best paper award at a symposium, which deals with privacy of not voters but of candidates in the voting.

Keywords: Privacy, fairness, voting, anonymity

A Tight High-Order Entropic Quantum Uncertainty Relation with Applications

Christian Schaffner (CWI - Amsterdam, NL)

We derive a new entropic quantum uncertainty relation involving min-entropy. The relation is tight and can be applied in various quantum-cryptographic settings.

Protocols for quantum 1-out-of-2 Oblivious Transfer and quantum Bit Commitment are presented and the uncertainty relation is used to prove the security of these protocols in the bounded-quantum-storage model according to new strong security definitions.

As another application, we consider the realistic setting of Quantum Key Distribution (QKD) against quantum-memory-bounded eavesdroppers.

The uncertainty relation allows to prove the security of QKD protocols in this setting while tolerating considerably higher error rates compared to the standard model with unbounded adversaries. For instance, for the six-state protocol with one-way communication, a bit-flip error rate of up to 17% can be tolerated (compared to 13% in the standard model).

Our uncertainty relation also yields a lower bound on the min-entropy key uncertainty against known-plaintext attacks when quantum ciphers are composed. Previously, the key uncertainty of these ciphers was only known with respect to Shannon entropy.

Keywords: Quantum cryptgraphy, quantum uncertainty relations, information theory, bounded-quantum-storage model

Joint work of: Damgård, Ivan; Fehr, Serge; Renner, Renato; Salvail, Louis; Schaffner, Christian

Full Paper:
http://arxiv.org/abs/quant-ph/0612014

See also: Advances in Cryptology - CRYPTO 2007, Springer LNCS 4622, pages 360-378, 2007

Identification and Signatures Based on NP-hard Problems of Quadratic Forms

Claus Peter Schnorr (Universität Frankfurt, D)

A symmetric matrix $A = A^t \in \mathbb{Z}^{n\times n}$ defines the quadratic form $\boldsymbol{x}^t A\boldsymbol{x}$. The forms $A_0, A_1 \in \mathbb{Z}^{n\times n}$ are *equivalent* if $T^t A_0 T = A_1$ holds for some $T \in \mathrm{GL}_n(\mathbb{Z})$. We present public key identification and digital signatures that provide proofs of knowledge of an equivalence transform $T \in \mathrm{GL}_n(\mathbb{Z})$.

Importantly, solving $T^t A_1 T = A_0$ for a "small" T is NP-hard for indefinite forms $A_1, A_0 \in \mathbb{Z}^{n\times n}$ for every fixed $n \geq 3$. This is a non trivial consequence of the NP-hardness of binary quadratic equations over the integers of [MA78]. Small dimension n yields short private and public keys and efficient protocols.

The NP-hardness holds for isotropic and for anisotropic forms.

While the computational equivalence problem has many easy instances for isotropic forms no easy instances are known for anisotropic forms.

Proof of knowledge. Prover $\mathcal{P}$ proves to verifier $\mathcal{V}$ knowledge of S such that $S^t A_1 S = A_0$ by iterating:

1. $\mathcal{P}$ computes and sends an LLL-reduced form $A' := T^t A_0 T$ for a randomized $T \in \mathrm{GL}_n(\mathbb{Z})$, see [HS07].
2. $\mathcal{V}$ sends a random one-bit challenge $b \in_R \{0,1\}$,
3. $\mathcal{P}$ sends the reply $R_b := S^b T \in \mathrm{GL}_n(\mathbb{Z})$, and $\mathcal{V}$ checks that $R_b^t A_b R_b = A'$.

If a fraudulent $\widetilde{\mathcal{P}}$ succeeds with $\widetilde{A}'$ and replies $\widetilde{R}_b$ for both $\widetilde{R}_0, \widetilde{R}_1$ he gets an equivalent private key $S' := \widetilde{R}_1 \widetilde{R}_0^{-1}$ satisfying $S'^t A_1 S' = A_0$. This protocol is statistical zeroknowledge under reasonable heuristics.

Another proof of knowledge uses, long challenges and can be transformed into an efficient public key signature scheme by replacing $\mathcal{V}$ through a cryptographic hash function. This proof represents some $c \in \mathbb{Z}$ as $\mathbf{x}^t A_b \mathbf{x} = c = \mathbf{y}^t A' \mathbf{y}$. As the knowledge of such $\mathbf{x}, \mathbf{y}$ reduce the dimension n of the unknown part of the equivalence transform T by 1 we require that $n \geq 4$.

References. [Ca78] presents the classical theory of rational quadratic forms, for LLL-reduction of quadratic forms see [S07, Si05].

Keywords: Identification, signature, quadratic form, proof of knowledge, zero-knowledge, NP-hardness

Efficient Implementation of Pairing Based Cryptosystems

Tsuyoshi Takagi (Future University - Hakodate, J)

Pairing based cryptosystems can accomplish novel security applications such as ID-based cryptosystems, efficient broadcast encryptions and so on, which have not been constructed efficiently without the pairing.

Recently some efficient algorithms for computing the pairing have been proposed, namely Duursma-Lee algorithm and its variant η_T pairing.

In this talk, we present some implementation of the η_T pairing over different computation platforms. Our processing speeds of the η_T pairing over $GF(3^{97})$ are as follows: 479 microseconds on AMD Opteron at 2.2GHz, 215 milliseconds on NTT FOMA SH903iS (JAVA mobilephone), 38 milliseconds on ARM9 at 225MHz using BREW, 27 microseconds on FPGA Altera Cyclone II EP2C35 at 147 MHz, and 5.8 seconds on ATmega128L at 7.37 MHz using TinyOS, respectively.

Keywords: Pairing, implementation

Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from any One-Way Function

Salil Vadhan (Harvard University, USA)

We give a construction of statistically hiding commitment schemes (ones where the hiding property holds against even computationally unbounded adversaries) under the minimal complexity assumption that one-way functions exist.

Consequently, one-way functions suffice to give statistical zero-knowledge arguments for any NP statement (whereby even a computationally unbounded adversarial verifier learns nothing other than the fact the assertion being proven is true, and a polynomial-time adversarial prover cannot convince the verifier of a false statement). These results resolve an open question posed by Naor, Ostrovsky, Venkatesan, and Yung (CRYPTO ‘92, J. Cryptology ‘98).

Keywords: Cryptography, statistically hiding commitments, statistical zero-knowledge argument systems, one-way functions, interactive hashing

Joint work of: Haitner, Iftach; Nguyen, Minh; Ong, Shien Jin; Reingold, Omer; Vadhan, Salil

See also: FOCS 06 paper by Nguyen, Ong, and Vadhan, and STOC 07 paper by Haitner and Reingold.

E-passports

Serge Vaudenay (EPFL - Lausanne, CH)

Passports are documents that help immigration officers to identify people. In order to strongly authenticate their data and to automatically identify people, they are now equipped with RFID chips. These contain private information, biometrics, and a digital signature by issuing authorities. Although they substantially increase security at the border controls, they also come with new security and privacy issues.

It is a well established fact that the basic access control (which is also used for symmetric key agreement) is pretty weak. It resists neither passive avesdropping nor online bruteforce attack. The European extension is better (based on Diffie-Hellman with authenticated keys) but not quite enough since the hash of files leaks.

One of the main privacy threat comes from the so-called passive authentication process which discloses digital evidence for private data authentication. Indeed, by accessing to the e-passport, anyone can get a digital signature from government authorities of a facial picture together with a name, a date of birth, and a citizenship. Future extensions will include extra private data. We suggest to fix passive authentication by using Zero-Knowledge proof of signature knowledge based on the Guillou-Quisquater protocol. This makes it possible to authenticate data while leaking no transferable evidence.

Keywords: RFID, travel documents, security, privacy

Joint work of: Monnerat, Jean; Vaudenay, Serge; Vuagnoux, Martin;

Full Paper:
http://lasecwww.epfl.ch/php_code/publications/search.php?ref=MVV07

Group message authentication

Douglas Wikström (KTH Stockholm, S)

Group signatures is a powerful primitive with many practical applications, allowing a group of parties to share a signature functionality, while protecting the anonymity of the signer.

However, despite intensive research in the past years, there is still no fully satisfactory implementation of group signatures. The schemes proposed so far are either too inefficient to be used in practice, or their security is based on rather strong, non-standard assumptions.

We observe that for some applications the full power of group signatures is not necessary. For example, a group signature can be verified by any third party, while in many applications such an universal verifiability is not needed or even not desired.

Motivated by this observation, we propose a notion of *group message authentication*, which can be viewed as a relaxation of group signatures. Group message authentication enjoys the group-oriented features of group signatures, while dropping some of the features which are not needed in many real-life scenarios. An example application of group message authentication is an implementation of an *anonymous* credit card.

We present a generic implementation of group message authentication, and also propose an efficient concrete implementation based on standard assumptions, namely strong RSA and DDH.

Keywords: Group signatures, anonymous credit cards, weaker assumptions

Joint work of: Wikström, Douglas; Przydatek, Bartosz

Relativistic Cryptography

Stefan Wolf (ETH Zürich, CH)

It has been observed that protocols for quantum key agreement can exist the security of which is provable under the assumption that quantum OR relativity theory is correct. More precisely, such schemes rely on the phenomenon of non-locality and on the non-signaling principle of relativity. A practical aspect is that the security is device-independent and holds whatever quantum systems are operated on. In the quest of finding efficient protocols of this kind, we discuss two new, pessimistic, results: First, binary quantum non-locality cannot be distilled, and second, there is no amplification of non-signaling privacy.

Keywords: (Post-) Quantum cryptography, device-independent security, relativity.

Joint work of: Wolf, Stefan; Dukaric, Dejan; Haenggi, Esther

Secure Multi-Party Multiplication with Low Communication

Robbert de Haan (CWI - Amsterdam, NL)

Multi-party computation based on Shamir's secret sharing scheme has two important drawbacks; the communication required is rather high and the field-size is dictated by the number of participants, which in turn increases the communication complexity as the field size grows with the number of participants. In this talk we give a survey of the recent advances towards alleviating these issues, mainly focusing on the non-amortized solutions.

The first construction that tackles the communication problem is due to Franklin and Yung, who present a variant of Shamir's scheme that allows to perform many multiplications in parallel at the cost of a single multiplication.

At Eurocrypt'07, Cramer, Damgaard and de Haan present another variant that allows to perform multiplications in a finite field requiring only operations and communication over a subfield, thus reducing the communication cost of a single multiplication, as opposed to the Franklin and Yung approach where only the communication cost of many multiplications performed in parallel can be reduced.

At Crypto'06 Chen and Cramer introduced a generalization of Shamir's scheme based on algebraic geometric coding theory. This approach has the advantage that it allows a number of participants much larger than the field size, and in fact multi-party computation can be performed over constant-sized fields for infinitely many settings of parameters.

At Eurocrypt'07, Chen et al. demonstrate an alternative solution that replaces Shamir's scheme with a scheme based on error correcting codes, where the general parameters of the code determine the parameters of the secret sharing scheme. This approach has the advantage that it can be applied for arbitrary field sizes, i.e., constructions over binary fields are possible, but only schemes with a regular multiplication property can be achieved in this way.

We also discuss our latest results, which include a very clean and basic replacement of the scheme due to Cramer, Damgaard and de Haan and its generalization over algebraic geometric curves.

Keywords: Secure multiplication, multi-party computation, ramp sharing schemes

Joint work of: de Haan, Robbert; Cascudo, Ignacio; Chen, Hao; Cramer, Ronald; Damgaard, Ivan; Goldwasser, Shafi; Vaikuntanathan, Vinod