Notes on Ten TCC'10 Talks

Oded Goldreich
Department of Computer Science
Weizmann Institute of Science
Rehovot, ISRAEL.
oded.goldreich@weizmann.ac.il

February 14, 2010

Preface: These notes refer to ten of the talks that I heard at the last TCC (see the conference's proceedings published as LNCS 5978). While one may definitely infer from the fact that a certain work is reviewed in these notes that I liked it, the converse may not be true. That is, the fact that some works are not reviewed here does not mean that I did not like them, since there may be other reasons for such omissions (e.g., failing to attend the talk, failing to understand it sufficiently well, etc.)

1 Parallel Repetition Theorems for Interactive Arguments

By Kai-Min Chung and Feng-Hao Liu

It has been known for more than a decade that, in general, parallel repetition may fail to reduce the soundness error (or rather the computational soundness error) of interactive arguments. Recent results have shown that (1) parallel repetition does reduce the soundness error in *any public-coin protocol* [see work by Hastad *et al.*, these proceedings][1], and (2) parallel repetition reduces the soundness error in a "random termination" modification of *any protocol* [see work by Haitner, FOCS'09], The current work provides an optimal (quantitative) version of the first result.

The quantitative improvement is achieved by directly analyzing the parallel execution, using Hölder's Inequality, rather than considering a *single* related stand-alone execution (and using a sampling lemma of Ran Raz). In other words, rather than analyzing the success probability of the stand-alone execution derived in a single randomly selected copy, the current work analyzes the evolution of the produce of the corresponding probabilities associated with all copies. This leads to an extremely clean and elegant analysis, which (as stated above) yields the optimal quantitative bound.

2 On Symmetric Encryption and Point Obfuscation

By Ran Canetti, Yael Tauman Kalai, Mayank Varia, and Daniel Wichs

This paper demonstrates a tight connection between the notion of obfuscation, when applied to point functions, and strong notions of secure (private-key) encryption.

[1]Early version of their work date to April 2008.

Specifically, a multi-bit point function, is a function $f_{K,M} : \{0,1\}^* \to \{0,1\}^* \cup \{\perp\}$, which is indexed by (K, M) and is defined such that $f_{K,M}(x) = M$ if $x = K$ and $f_{K,M}(x) = \perp$ otherwise. Having an obfuscator, $\mathcal{O}$, for such a class, yields a private-key encryption scheme in which the message M is encrypted under key K as the ciphertext $C \leftarrow \mathcal{O}(f_{K,M})$ and the ciphertext C (viewed as a circuit) is decrypted (under key K) to $C(K)$. This private-key encryption scheme is secure in a strong sense; that is, it is secure also under a linear amount of information leakage from the key (i.e., "key leakage"), and it is secure also under key-dependent attacks (i.e., "key-dependent messages"). It is also shown that strongly secure encryption schemes , yield point obfuscator.

3 From Passive to Covert Security at Low Cost

By Ivan Damgard, Martin Geisler, and Jesper Buus Nielsen

This work refers to the appealing notion of covert security, introduced by Aumann and Lindell [TCC'07]. Intuitively, covert security refers to protocols in which security breaches are detected with fair probability (e.g., probability at least 1/2), while incriminating some party that behaved improperly, which in turn deters improper behavior (assuming some external mechanisms). Clearly, covert security extends security against semi-honest behavior, and the hope is that it can be achieved at about the same cost, while providing a level of security that in many settings is almost as good as the standard notion of security (i.e., security against arbitrary malicious behavior).

The latter hope is fully satisfied by the current work, which shows a generic and simple transformation of a wide range of protocols that are secure in the semi-honest model into related protocols for the covert model. Essentially, the covert protocol invokes the semi-honest protocol twice, running it once with the real inputs and once with dummy inputs, while relying on a secure (against malicious behavior) implementation of a simple "oblivious selection" functionality. The transcript of the dummy execution is used for detecting deviation from the protocol, by having it be fully revealed.

4 A Hardcore Lemma for Computational Indistinguishability: Security Amplification for Arbitrarily Weak PRGs with Optimal Stretch

By Ueli Maurer and Stefano Tessaro

This work presents a "computational indistinguishability" analogue of the notion of a hardcore region/set of a computationally hard decision problem. Recall that the latter notion, introduced by Impagliazzo [FOCS'95], refers to predicates that are moderately hard to approximate and defines their hardcores as regions on which these predicates are infeasible to approximate significantly better than by a coin toss. Impagliazzo showed that any such predicate has a hardcore of size that is linearly related to the level of inapproxability (i.e., the probability with which any efficient predictor fails, when given a random instance).

The current work may be viewed as generalizing Impagliazzo's notion from "one bit indistinguishability" to general indistinguishability. Specifically, it is shown that if two distributions are moderately indistinguishable (i.e., the best distinguishability gap is ϵ), then there exists a proportional region (of measure $1 - \epsilon$) on which the corresponding conditional distributions are strongly indistinguishable. In particular, if a distribution is moderately indistinguishable from the uniform one, then with proportional probability the former has high min-entropy.

5 Delayed-Key Message Authentication for Streams

By Marc Fischlin and Anja Lehmann

In many settings of message authentication, it is desirable to start processing (e.g., authenticating) the message before obtaining the authentication key. This feature was provided in the past by patches of known MACs, but it is unclear whether these patches preserve the security of the original schemes. The current work initiates a systematic study of this problem, while providing a methodology for deriving such schemes from ordinary MACs. This methodology is actually universal, in the sense that under a proper formulation of the goal (not provided in the paper...) any solution can be cast in its terms.

The paper distinguishes between "one sided" versions, in which the key is delivered late only to one of the two parties (i.e., authenticator and verifier), and schemes that support the "delayed key" feature for both parties. The results for the "one sided" versions preserves the efficiency (and security) of the original MACs, whereas in the "two sided" case only a feasibility result is presented.

6 Founding Cryptography on Tamper-Proof Hardware Tokens

By Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, and Akshay Wadia

This work initiates a comprehensive study of the type of cryptographic applications that can be achieved by relying on tamper-proof hardware. Needless to say, the focus is on applications that cannot be achieved in the "plain model" (i.e., without such hardware). The tamper-proof hardware considered is typically "light weight" and is thus referred to as "(hardware) tokens", while a distinction is drawn between stateful tokens and stateless tokens. A typical type of *stateful tokens* are ones that can be activated (or invoked) only once (i.e., on one input), and seize to respond after they provide the corresponding output.

In particular, it is shown that stateful tokens can be used to provide non-interactive perfectly-secure two-party computation (without relying on any computational assumptions). The tokens uses here are of the "1-out-of-2 OT" type. When using stateless tokens, it is shown how to achieve (interactive) UC-secure two-party computation based on one-way functions (rather than various forms of trapdoor permutations). Additional results regarding one-time programs [cf. Goldwasser *et al.*, Crypto'08] and program obfuscation [cf. Barak *et al.*, Crypto'01] are also presented.

7 Public-Key Cryptographic Primitives Provably as Secure as Subset Sum

By Vadim Lyubashevsky, Adriana Palacio, and Gil Segev

Building upon and being inspired by the work of Impagliazzo and Naor (JofC'96), this work presents a public-key encryption scheme based on the conjecture hardness of subset sum. Unlike the knapsack schemes suggested in the 1970's (cf. the Merkle Hellman scheme), the current scheme uses a random sequence rather than a structured one. Furthermore, the density (as in Impagliazzo and Naor) is in the seemingly hard region, and thus seems invulnerable to the lattice-based attacks. (While the resulting scheme is related to schemes that may be derived based on lattices, the assumptions here seem weaker, the parameters are better, and the proof of security is much simpler.)

The scheme itself uses a public-key that is a set of n vectors over $GF(q)$, augmented by n vectors that are each obtained by taking a random linear combination of the n vecotors, but viewing them a integers in base q and adding them accrdingly (as integers) modulo $M = q^n$. (The n random combinations serves as the secret key, and encryption is done by an analogous process that uses the transposed matrix that represents the public-key.) This looks like using subset sum of vectors with added noise, except that the noise here is determined by the vectors being added (rather than being random). Interestingly, this "deterministic noise" allows the proof proof of security to sail through, and it is not clear whether the "intuitively more secure" addition of random noise results in a secure scheme. Indeed, the (elegant and relatively simple) proof of security is based on the relationship between the arithmetics of n-dimensional vector spaces over $GF(q)$ and the modular arithmetic (i.e., mod $M = q^n$), when q is polynomially related to n. Specifically, we may view the addition of n numbers modulo M, as addition of the corresponding vectors, except for the carry values, which in this case are small.

8 Bounds on the Sample Complexity for Private Learning and Private Data Release

By Amos Beimel, Shiva Kasiviswanathan, and Kobbi Nissim

Private learning refers to the task of learning (in the PAC sense) such that the output hypothesis preserves the privacy of the examples (or rather the privacy of the underlying individuals) used in the learning process, where privacy means differential privacy as in Dwork *et al.* [TCC'06]. It is known that anything that is PAC learnable can be learned privately [cf. Kasiviswanathan *et al.*, FOCS'08], but the currently known sample complexity bound for learning a concept class $\mathcal{C}$ is $O(\log|\mathcal{C}|)$ rather than $O(\text{VC-dim}(\mathcal{C}))$ as in case of (non-private) learning. The question addressed in this work is whether this gap is inherent.

The main result of this paper is that the aforementioned gap is inherent *as far as proper learning is concerned*, where in proper learning the output hypothesis is required to be in the concept class being learned. In particular, there exists a concept class $\mathcal{C}$ that can be properly learned based on a constant number of samples, but privately learning it in the proper sense requires $\Omega(\log|\mathcal{C}|)$ samples. (Note that the aforementioned upper bounds on private and non-private learning are achieved using proper learning, as is always the case when the Occam Razor approach is used.)

9 Secure Computation and Its Diverse Applications (survey)

By Yuval Ishai

The focus of this survey talk was on unexpected relations between different forms of secure MPC (multi-party computation) as well as between MPC and other problems in cryptography, and even outside of cryptography.

One such connection is the construction of zero-knowledge proofs based on perfectly secure MPC, specifically, a MPC that is 2-private in the semi-honest model [cf. Ishai *et al.*, STOC'07]. Here when seeking to prove that the common input x has an NP-witness (w.r.t R), the prover runs, as a mental experiment, a MPC for the function for f, where $f((x,w_1),...,(x,w_n)) = 1$ if $(x, \oplus_{i\in[n]} w_i) \in R$ and $f((x_1,w_1),...,(x_n,w_n)) = 0$ otherwise. Then the prover sends the verifier a commitment to each of the n individual local views (in that execution). Next, the verifier selects at random $i,j \in [n]$ and sends (i,j) to the prover, which should respond with the proper decommitment. The verifier accepts if and only if the two revealed views are consistent with the protocol. Intuitively, the zero-knowledge feature follows from the 2-privacy of the protocol, whereas soundness (with error $1 - (2/n^2)$) follows from its correctness. Interestingly, this approach yields various advantages over the standard zero-knowledge proofs for R.

Yuval advocated abstracting the standard GMW-protocol as well as the above protocol as a two-step process in which one first provides a zero-knowledge PCP [cf. Kilian *et al.*, STOC'99], and then implements the PCP oracle by a commitment scheme. He also mentioned other unexpected connections between MPC and non-MPC issues including

- The connection between communication efficient MPC (where efficiency is measured in terms of the input length, independent of the function being computed) and PIR/LDC (Private Information Retrieval schemes and Locally Decodable Codes).
- The connection between computational PIR schemes and collision resistant hashing.
- The work in MPC leading to "cryptography in NC0" [cf. Applebaum *et al.*, FOCS'04].

Yuval recommended a survey by Maurer titled "Abstraction in Cryptography" (Crypto'09).

10 Eye for an Eye: Efficient Concurrent Zero-Knowledge in the Timing Model

By Rafael Pass, Wei-Lung Dustin Tseng, and Muthuramakrishnan Venkitasubramaniam

This paper provides a flexible methodology for the construction of concurrent zero-knowledge proofs in the timing model, allowing trade offs between the maximum message delivery time bound, the round complexity of the protocol, and the security level (captured by the simulation time). The most appealing suggestion is to "shift the delays to adversarial parties" in the sense that the protocol applies a delay that is proportional to the one observed in the actual execution (rather than applying a delay that is set to the maximum message delivery time bound).

The quantitative results allow, for example, to reduce the execution time from $t + O(\Delta)$ to $c \cdot t + \Delta/c^3$, for any constant c, where t is the actual execution time (without the artificial delays) and Δ is the maximum message delivery time bound. An alternative trade off yields execution time of $t^c + (2\Delta)^{1/c^3}$. That is, while prior protocols had steps that delayed some communication by Δ regardless of how fast messages were delivered in the actual execution, the current protocol uses much smaller fixed delays (in addition to execution-adaptive delays).