Share Conversion and Private Information Retrieval (Abstract)*

Amos Beimel[1], Yuval Ishai[2], Eyal Kushilevitz[2], and Ilan Orlov[1]

[1] Dept. of Computer Science, Ben Gurion University of the Negev, Beer Sheva, Israel
[2] Dept. of Computer Science, Technion, Haifa, Israel

Abstract. An information-theoretic *private information retrieval* (PIR) protocol allows a client to retrieve the i-th bit of a database, held by two or more servers, without revealing information about i to any individual server. Information-theoretic PIR protocols are closely related to *locally decodable codes* (LDCs), which are error correcting codes that can simultaneously offer a high level of robustness and sublinear-time decoding of each bit of the encoded message. Recent breakthrough results of Yekhanin (STOC 2007) and Efremenko (STOC 2009) have led to a dramatic improvement in the asymptotic complexity of PIR and LDC. We suggest a new "cryptographic" perspective on these recent constructions, which is based on a general notion of *share conversion* in secret-sharing schemes that may be of independent interest.

Our new perspective gives rise to a clean framework which unifies previous constructions and generalizes them in several directions. In a nutshell, we use the following two-step approach: (1) apply *share conversion* to get a low-communication secure multiparty computation protocol $\mathcal{P}$ for a nontrivial class $\mathcal{F}$ of low-depth circuits; (2) use a lower bound on the *VC dimension* of $\mathcal{F}$ to get a good PIR protocol from $\mathcal{P}$. Our framework reduces the task of designing good PIR protocols to that of finding powerful forms of share conversion which support circuit classes of a high VC dimension.

Motivated by this framework, we study the general power of share conversion and obtain both positive and negative results. Our positive results improve the concrete complexity of PIR even for very feasible real-life parameters. They also lead to some improvements in the asymptotic complexity of the best previous PIR and LDC constructions. For 3-server PIR, we improve the asymptotic communication complexity from $O(2^{146\sqrt{\log n \log\log n}})$ to $O(2^{6\sqrt{\log n \log\log n}})$ bits, where n is the database size. Our negative results on share conversion establish some limitations on the power of our approach.

* The paper was presented in the 27th IEEE Conference on Computational Complexity, 2012 at Porto, Portugal. This research was supported by ERC Starting Grant 259426. The first and fourth authors are additionally supported by ISF grant 938/09 and by the Frankel Center for Computer Science. The second and third authors are additionally supported by ISF grant 1361/10 and BSF grant 2008411.

Almost-Everywhere Secure Computation with Edge Corruptions (Abstract)[⋆]

Nishanth Chandran[1,⋆⋆], Juan Garay[2,⋆⋆⋆], and Rafail Ostrovsky[3,†]

[1] Microsoft Research, Redmond
[2] AT&T Labs – Research
[3] Departments of Computer Science and Mathematics, UCLA

Abstract. We consider secure multi-party computation (MPC) in a setting where the adversary can separately corrupt not only the parties (nodes) but also the communication channels (edges) in the network. We consider this question in the information-theoretic setting, and require security against a computationally unbounded adversary.

In a fully connected network the above question is simple (and we also provide an answer that is optimal up to a constant factor). What makes the problem more challenging is to consider the case of sparse networks. Partially connected networks are far more realistic than fully connected networks, which led Garay and Ostrovsky [Eurocrypt'08] to formulate the notion of (unconditional) *almost-everywhere (a.e.) secure computation* in the node-corruption model, i.e., a model in which not all pairs of nodes are connected by secure channels and the adversary can corrupt some of the nodes (but not the edges).

In this work we introduce the notion of *almost-everywhere secure computation with edge corruptions*, which is exactly the same problem as described above, except that we additionally allow the adversary to completely control some of the communication channels between two correct nodes—i.e., to "corrupt" edges in the network. While it is easy to see that an a.e. secure computation protocol for the original node-corruption model is also an a.e. secure computation protocol tolerating edge corruptions (albeit for a reduced fraction of edge corruptions with respect to the bound for node corruptions), no polynomial-time protocol is known in the case where a **constant fraction** of the edges can be corrupted (i.e., the maximum that can be tolerated) and the degree of the network is sub-linear.

We make progress on this front, by constructing graphs of degree $O(n^\epsilon)$ (for arbitrary constant $0 < \epsilon < 1$) on which we can run a.e. secure computation protocols tolerating a constant fraction of adversarial edges.

[⋆] A version of this paper entitled "Edge Fault Tolerance on Sparse Networks" appears in the Proceedings of the 39th *International Colloquium on Automata, Languages and Programming* (ICALP 2012). The full version of this paper is available at `http://eprint.iacr.org/2012/221`.

[⋆⋆] Email: `nish@microsoft.com`. Part of this work was done at UCLA.

[⋆⋆⋆] Email: `garay@research.att.com`.

[†] Email: `rafail@cs.ucla.edu`.

Improving the Quality of Santha-Vazirani Sources (Abstract)

Roger Colbeck and Renato Renner

Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland

Abstract. Is it possible to generate perfectly random bits, using only a source of weakly random bits? A well-known result by Santha and Vazirani [1] shows that this is impossible if the only guarantee one has about the initial randomness is that the bias of each bit (that is, the difference between the probability of the most likely bit value and $\frac{1}{2}$), conditioned on all previous ones, is upper bounded by a (known) constant ε. However, this impossibility result only applies to classical methods. Here we show that it is in fact possible to improve the quality of a Santha-Vazirani source using a quantum protocol provided the randomness source has a sufficiently low ε. Furthermore, the randomness of the resulting bits can be certified without relying on the correctness or completeness of quantum theory; the result holds in any non-signalling theory.

This has implications for cryptography, where honest users are often assumed to have trusted sources of perfect randomness. Our result implies that this assumption can be weakened: using our protocol, any task that can be securely performed using perfect randomness can in principle be securely performed using imperfect randomness (provided it is not too weak).

Although the present technique only works for a source with a sufficiently small bound on ε, we conjecture that with an alternative method this bound can be increased. More precisely, we conjecture that, given a source with any non-trivial bound on ε (i.e. with ε strictly smaller than $\frac{1}{2}$), there exists a protocol that uses only this source to generate bits with an arbitrarily small bias.

The full version of this work can be found in [2].

References

1. Santha, M., Vazirani, U.V.: Generating quasi-random sequences from slightly random sources. In: Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS 1984), pp. 434–440 (1984)
2. Colbeck, R., Renner, R.: Free randomness can be amplified. Nature Physics 8, 450–453 (2012); also available as arXiv:1105.3195

David & Goliath Oblivious Affine Function Evaluation (Abstract)

Asymptotically Optimal Building Blocks for Universally Composable Two-Party Computation from a Single Untrusted Stateful Tamper-Proof Hardware Token

Nico Döttling[⋆], Daniel Kraschewski, and Jörn Müller-Quade

Institute of Cryptography and Security, Department of Informatics,
Karlsruhe Institute of Technology, Germany
{doettling,kraschewski,mueller-quade}@kit.edu

Abstract. Cryptographic assumptions regarding tamper-proof hardware tokens have gained increasing attention. Even if the tamper-proof hardware is issued by a party that is not trusted by the other(s), many tasks become possible: Tamper proof hardware is sufficient for universally composable protocols, for information-theoretically secure protocols, and even allows to create software that can only be used once (one-time programs).

In a two-party setting, where only *one single* tamper-proof token is issued, we present secure constructions for multiple one-time memories (OTMs), and reusable and bidirectional commitment and oblivious transfer (OT) primitives. Our approach in its primary variant comes along without any computational assumptions, but allows only for limited, yet arbitrary token reuse. However, unlimited token reusability can be achieved straightforwardly by using a pseudorandom number generator. All our constructions have only linear communication complexity (i.e. per implemented instance of k-bit OTM/commitment/OT only $O(k)$ bits are transferred) and are thus asymptotically optimal. Moreover, the computation complexity of our protocols for k-bit OTMs/commitments/OT is dominated by $O(1)$ finite field multiplications with field size 2^k, what is considerably more efficient than any other known construction based on untrusted tamper-proof hardware alone.

The central part of our contribution is a construction for oblivious affine function evaluation (OAFE), which can be seen as a generalization of the well known oblivious transfer primitive: Parametrized by a finite vector space $\mathbb{F}_q^k$, the OAFE primitive allows a designated sender party to choose an arbitrary affine function $f : \mathbb{F}_q \to \mathbb{F}_q^k$, such that hidden from the sender party a designated receiver party may learn $f(x)$ for exactly *one* function argument $x \in \mathbb{F}_q$ of its choice. All our abovementioned results build on this primitive and it may also be of particular interest for the construction of garbled arithmetic circuits.

See http://eprint.iacr.org/2012/135 for a public version of the full paper.

[⋆] Supported by IBM Research & Development Germany within the HomER project.

A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy (Abstract)

Benjamin Fuller[1], Adam O'Neill[2], and Leonid Reyzin[2]

[1] Boston University and MIT Lincoln Laboratory
[2] Boston University

Abstract. We propose a general construction of deterministic encryption schemes that unifies prior work and gives novel schemes. Specifically, its instantiations provide:

- A construction from any trapdoor function that has sufficiently many hardcore bits.
- A construction that provides "bounded" multi-message security from lossy trapdoor functions.

The security proofs for these schemes are enabled by three tools that are of broader interest:

- A weaker and more precise sufficient condition for semantic security on a high-entropy message distribution. Namely, we show that to establish semantic security on a distribution M of messages, it suffices to establish indistinguishability for all conditional distribution $M|\mathsf{E}$, where E is an event of probability at least $1/4$. (Prior work required indistinguishability on *all* distributions of a given entropy.)
- A result about computational entropy of conditional distributions. Namely, we show that conditioning on an event E of probability p reduces the quality of computational entropy by a factor of p and its quantity by $\log_2 1/p$.
- A generalization of leftover hash lemma to correlated distributions.

We also extend our result about computational entropy to the average case, which is useful in reasoning about leakage-resilient cryptography: leaking λ bits of information reduces the quality of computational entropy by a factor of 2^λ and its quantity by λ.

A conference version of this work appeared in Theory of Cryptography 2012 [2] and a full version is available online at [1].

References

1. Fuller, B., O'Neill, A., Reyzin, L.: A unified approach to deterministic encryption: New constructions and a connection to computational entropy. Cryptology ePrint Archive, Report 2012/005, http://eprint.iacr.org/2012/005
2. Fuller, B., O'Neill, A., Reyzin, L.: A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 582–599. Springer, Heidelberg (2012)

Bounds for Secure Two-Party Sampling from a Generalization of Common Information (Abstract)*

Vinod M. Prabhakaran[1] and Manoj M. Prabhakaran[2]

[1] Tata Institute of Fundamental Research, India
[2] University of Illinois at Urbana-Champaign, USA

Abstract. Secure multi-party computation is a central problem in modern cryptography. An important sub-class of this are problems of the following form: Alice and Bob desire to produce sample(s) of a pair of jointly distributed random variables. Each party must learn nothing more about the other party's output than what its own output reveals. To aid in this, they have available a *set up* — correlated random variables whose distribution is different from the desired distribution — as well as unlimited noiseless communication. We upper-bound how efficiently a given set up can be used to produce samples from a desired distribution.

The key tool we develop is called *tension* – or more precisely, the *region of tension* – which measures how well the correlation between a pair of random variables can be (or rather, cannot be) resolved as a piece of common information and other independent pieces of information. We show various properties of this region, including a crucial monotonicity property: *a protocol between two parties can only lower the tension between their views.* Then we derive state-of-the-art bounds on the rate at which samples from one distribution can be produced per sample of a set up, by comparing the regions of tension of the two distributions.

Another important contribution of this work is to generalize the notion of common information of two dependent variables introduced by [Gács-Körner, 1973]. They defined common information of (X, Y) as the largest entropy rate of a common random variable that two parties observing X^n and Y^n respectively, can agree upon. It is well-known that this captures only a limited form of dependence between X and Y, and is zero in most cases of interest. Our generalization, which we call *Assisted Common Information*, lets us take into account "almost common" information ignored by Gács-Körner common information. In the assisted common information system, a genie assists the parties in agreeing on a more substantial common random variable; we characterize the trade-off between the amount of communication from the genie and the quality of the common random variable produced. We show that the optimal trade-off is essentially given by the region of tension. Connections to the Gray-Wyner system and Wyner's common information are also studied.

* Based partly on papers at IEEE International Symposia on Information Theory (ISIT) 2010 and 2011. Full version available at http://arxiv.org/abs/1206.1282. Supported in part by a Ramanujan Fellowship of the Department of Science and Technology, Government of India, and NSF CAREER award 07-47027.

An Information-Theoretic Approach to Privacy (Abstract)*

Lalitha Sankar[1], S. Raj Rajagopalan[2], and H. Vincent Poor[1]

[1] Dept. of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
[2] HP Labs, Princeton, NJ 08540, USA

Abstract. Ensuring the usefulness of electronic data sources while providing necessary privacy guarantees is an important unsolved problem. This problem drives the need for an analytical framework that can quantify the safety of personally identifiable information (privacy) while still providing a quantifiable benefit (utility) to multiple legitimate information consumers. State of the art approaches have predominantly focused on privacy. Utility of a data source is potentially (but not necessarily) degraded when it is restricted or modified to uphold privacy requirements. The central problem of this paper is a precise quantification, using information theoretic tools, of the tradeoff between the privacy needs of the *respondents* (individuals represented by the data) and the utility of the *sanitized* (published) data for any data source. The central contribution of this work is a precise quantification of the tradeoff between the privacy needs of the individuals represented by the data and the utility of the *sanitized* (published) data for any data source using the theory of rate distortion with additional privacy constraints. Utility is quantified (inversely) via *distortion* (accuracy), and privacy via *equivocation* (entropy). We expose an essential dimension of information disclosure for the first time via an additional constraint on the disclosure rate which is a measure of the precision of the sanitized data. We translate the rate-distortion-equivocation formalism of information theory to the utility-privacy problem and develop a framework that allows us to model data sources, including multi-dimensional databases and data streams, develop application independent utility and privacy metrics, quantify the fundamental bounds on the utility-privacy tradeoffs, and develop a side-information model for dealing with questions of external knowledge. We demonstrate the application of this framework for both numerical and categorical examples [1]. We have also applied this framework to privacy applications with time-series sources and organizational data disclosure.

References

1. Sankar, L., Rajagopalan, S.R., Poor, H.V.: An information-theoretic approach to privacy. In: Proc. 48th Allerton Conference on Communication, Control, and Computing, Monticello, IL, pp. 1220–1227 (September 2010)

* This research is supported in part by the U. S. NSF under Grant CCF-1016671 and the Air Force Office of Scientific Research under Grant FA9550-09-1-0643. This research described here first appeared as [1].

Author Index