Secure Protocols for Complex Tasks in Complex Environments

Amit Sahai

University of California, Los Angeles
sahai@cs.ucla.edu

Over the last two decades, there has been tremendous success in placing cryptography on a sound theoretical foundation, and building an amazingly successful theory out of it. The key elements in this Modern Cryptographic Theory are the definitions capturing the intuitive, yet elusive notions of security in various cryptographic settings. The definitions of the early 80's proved to be extremely successful in this regard. But with time, as the theory started addressing more and more complex concerns, further notions of security had to be introduced. One of the most important concerns theory ventured into is of complex environments where different parties are communicating with each other concurrently in many different protocols. A series of efforts in extending security definitions led to the paradigm of Universally Composable (UC) Security [1], which along with modeling a general complex network of parties and providing definitions of security in that framework, provided powerful tools for building protocols satisfying such definitions.[1]

The basic underlying notion of security in the UC framework and its many predecessors is based on *simulation*. An "ideal" world is described, where all requisite tasks get accomplished securely, as if by magic. The goal of the protocol designer is to find a way to accomplish these tasks in the "real" world, so that no malicious adversary can take advantage of this substitution of ideal magic by real protocols. To formalize this, we say that for every malicious adversary $\mathcal{A}$ that tries to take advantage of the real world, there is an adversary $\mathcal{S}$ that can achieve *essentially the same results* in the ideal world. The "results" are reflected in the behavior of an *environment*. In this survey we shall refer to this notion of security as *"Environmental Security."* If a real-life protocol "Environmentally Securely realizes" a task, it ensures us that replacing the magic by reality does not open up new unforeseen threats to the system. (There may already be threats to the system even in the ideal world. But employing cryptographic primitives cannot offer a solution if the ideal system itself is badly conceived.) The ideal-world adversary $\mathcal{S}$ is called a *simulator* as it simulates the real-world behavior of $\mathcal{A}$, in the ideal world.

A major advantage of Environmentally Secure (ES) protocols, as shown in [1], is that they are "Universally Composable," i.e., roughly, if multiple copies

[1] A similar framework to UC Security was independently proposed by Pfitzmann and Waidner [5, 6]. These two frameworks are conceptually very similar, although there are a number of technical differences. We choose to concentrate on the UC framework in this survey.

A. Canteaut and K. Viswanathan (Eds.): INDOCRYPT 2004, LNCS 3348, pp. 14–16, 2004.

of an ES-protocol are present in the system (in fact they could be copies of different protocols), then they collectively ES-realize the collection of the tasks they individually ES-realize. Hence we shall often refer to the framework in [1] as the ES/UC framework, or simply ES-framework or UC-framework.

Unfortunately, this notion of security turns out to be too strong to be achievable in standard settings. It has been shown that much of the interesting cryptographic tasks (including *e.g.* commitment, zero knowledge and secure multi-party computation) *cannot* be ES-realized when the adversary can control at least half the parties [1, 2, 3]. On the other hand, under a trusted set-up assumption – that there is a public reference string chosen by a completely trusted party – it is known how to build protocols for the most ambitious of cryptographic tasks (general secure multiparty computation with dishonest majority) satisfying the Environmental Security definition [4]. However, if no trusted party is assumed, then we are left with the strong impossibility results mentioned above.

We recently overcame these impossibility results in [7]. In that work, we develop secure protocols in the plain model (without any trusted set-up assumptions), by modifying the notion of security, while still retaining the composability. The new direction taken by this work opens up many interesting new questions and directions for the field of cryptographic protocols.

In this survey talk, we will outline the fundamental ideas and results leading up to the recent work mentioned above, and the many open questions that remain.

Acknowledgements. The author's research in this area has been supported by generous grants from the NSF ITR and Cybertrust programs, as well as an Alfred P. Sloan Foundation Research Fellowship.

References

1. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Electronic Colloquium on Computational Complexity (ECCC) (016): (2001) (Preliminary version in *IEEE Symposium on Foundations of Computer Science*, pages 136–145, 2001.)
2. Ran Canetti and Marc Fischlin. Universally composable commitments. In *CRYPTO*, pages 19–40, 2001.
3. R. Canetti, E. Kushilevitz, and Y. Lindell. On the limitations of universally composable two-party computation without set-up assumptions. In *EUROCRYPT*, pages 68–86, 2003.
4. R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party and multi-party secure computation. In *ACM Symposium on Theory of Computing*, pages 494–503, 2002.
5. B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In ACM Conference on Computer and Communications Security (CCS 2000), pp. 245–254, 2000.

6. B. Pfitzmann and M. Waidner. A Model for Asynchronous Reactive Systems and its Application to Secure Message Transmission. In IEEE Symposium on Security and Privacy, 2001.
7. Manoj Prabhakaran and Amit Sahai. New Notions of Security: Achieving Universal Composability without Trusted Setup. In *ACM Symposium on Theory of Computing*, 2004. Full version to appear in *SIAM Journal of Computing*, Special Issue for STOC 2004. Preliminary full version available at the Cryptology ePrint Archive `http://eprint.iacr.org/`.