Chapter 7

Conclusion

In this brief chapter we present a personal view of our work and try to point out its merits. We also outline some directions for further research.

Merit of this work. An important contribution of this work is, in our opinion, the precise and workable definitions of secure multiparty computation (presented in Chapter 2 and Section 4.1). These definitions allow us, for the first time, to have a clear and precise notion of a secure multiparty protocol, and to prove security of our protocols.

We believe that without these definitions we would not have been able to come up with protocols that solve the adaptive security problem and the problem of secure computation in asynchronous networks. Hopefully, the framework and tools developed for these definitions will prove helpful in formulating precise definitions of primitives encountered in the future.

The long-sought solution for the adaptive security problem (Chapter 3) allows us to present secure solutions for an abundance of known protocol problems in the presence of adaptive adversaries (which seem to be a better model of reality than non-adaptive ones). Our solution stems from a better understanding of the nature of secure multiparty computation. This understanding resulted in a better modeling of the degree of trust the party have in each other, namely in the notion of a semi-honest party.

Our solution works only for non-erasing parties. Investigating this notion of semi-honesty only slightly further, one finds out that in a very natural (arguably, even the most natural) trust-model, namely that of honest-looking parties, we are unable to prove adaptive security of practically *any* non-trivial protocol (unless a trusted dealer is available in an initial preprocessing phase). This holds even in the presence of absolutely secure channels. This surprising phenomenon should be taken into account whenever adaptive adversaries are considered.

The main tool used in solving the adaptive security problem is non-committing encryption. The essence of these encryptions is separating *encryption* from *commitment.* Until this work, encryption was thought of as an inevitably committing primitive (in the sense that the ciphertext could serve as a *commitment* of the sender - and of the receiver - to the plaintext). We showed that encryption can be done without commitment, and demonstrated the benefits of this separation. We believe that non-committing encryption is of independent interest. In particular, non-committing encryption may prove to be a 'more secure' way to encrypt data than standard encryption in many other scenarios.

In the chapter on asynchronous secure computation (Chapter 4) we define what it means to securely compute (or, rather, approximate) a function in an asynchronous setting with faults. We also show, in a detailed way, how known techniques for constructing protocols for securely computing any function can be adapted to the asynchronous setting. Finally, to the best of our knowledge this is the first (and so far only) place where a *full proof of security* of a construction for securely computing any function appears, in *any* model of computation. In particular, a security proof of the [BGW] construction can be extracted from the proof presented here.

The chapter on asynchronous Byzantine agreement (Chapter 5) applies ideas and techniques from secure multiparty computation to constructing the first asynchronous Byzantine agreement (BA) protocol with optimal resilience and polynomial complexity. The construction is quite involved, using many layers and techniques. The main technical contributions are, in our opinion, two: First, we adapt techniques from [RB, TRa] to construct the first Asynchronous Verifiable Secret Sharing (AVSS) scheme with optimal resilience. Next, we slightly modify the [F] scheme (which was never published and unaccessible) for reaching BA given an AVSS scheme, and present it in a (hopefully) readable way. Indeed, this work is the first accessible source to any asynchronous BA protocol with linear resilience and polynomial complexity.

The chapter on proactive security (Chapter 6) introduces a new approach to maintaining the security of computer systems in the presence of transient and repeated break-ins (or failures). We hope and believe that this approach will become a standard in the effort to protect computer systems. In fact, a number of works have already followed this approach (e.g., [ChH, HJKY, CHH, HJJKY]).

Subsequent and future work. We mention two directions for subsequent research. The first deals with an additional security requirements from multiparty protocols. Namely, we require that the computation will not leave a 'trace' that can be later used against the parties. An example is a 'mafia' that records the transcript and later uses it to 'coerce' parties to reveal their inputs. Some research in this direction has been done ([BT, SK, CDNO, CG]); however many questions remain open.

Another issue, not addressed in this work at all, is how to deal with *unauthenticated* communication channels, that can be actively controlled by the adversary. In fact how, again, to precisely define the problem? (Here additional definitional problems are encountered. For instance, the adversary may always prevent the parties from completing the computation, by simply not delivering messages.) A somewhat restricted definition, as well as a solution for a certain (quite powerful) adversary model is presented in [CHH]. Still, many questions remain open.

Bibliography

[AFL] E. Arjomandi, M. Fischer and N. Lynch, "Efficiency of Synchronous Versus Asynchronous Distributed Systems", *Journal of the ACM*, No. 3, Vol. 30, 1983, pp. 449-456.

[Aw] B. Awerbuch, "The complexity of Network Synchronization", *JACM, Vol. 32, no. 4,* pp. 804-823, 1985.

[Ba] E. Bach, "How to generate factored random numbers", *SIAM J. on Comput.,* Vol. 17, No. 2, 1988, pp. 179-193.

[Be] D. Beaver, "Foundations of Secure Interactive Computing", *CRYPTO,* 1991.

[BH] D. Beaver and S. Haber, "Cryptographic Protocols Provably secure Against Dynamic Adversaries", *Eurocrypt,* 1992.

[BR1] M. Bellare and P. Rogaway, "Entity authentication and key distribution", *Advances in Cryptology: Proc. of Crypto 93*, August 1993, pp. 232-249.

[BR2] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", *First ACM conf. on Computer and Comm. Security,* November 1993, pp. 62-73.

[BT] Josh Benaloh and Dwight Tunistra, "Receipt-Free Secret-Ballot Elections", *26th STOC,* 1994, pp. 544-552.

[BCG] M. Ben-Or, R. Canetti and O. Goldreich, "Asynchronous Secure Computations", *25th STOC,* 1993, pp. 52-61.

[BE] M. Ben-Or and R. El-Yaniv, "Interactive Consistency in Constant Time", submitted for publication, 1991.

[BGW] M. Ben-Or, S. Goldwasser and A. Wigderson, " Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation", *20th STOC,* 1988, pp. 1-10.

[BKR] M. Ben-Or, B. Kelmer and T. Rabin, "Asynchronous Secure Computation with Optimal Resilience", *13th PODC,* 1994 pp. 183-192.

[BGH+1] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, "A family of light-weight protocols for authentication and key distribution", Submitted to IEEE T. Networking, 1993.

[BGH+2] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, "Systematic design of a family of attack-resistant authentication protocols", *IEEE Journal on Selected Areas in Communications*, 11(5) (Special issue on Secure Communications), June 1993, pp.679–693. See also a different version in *Crypto 91.*

[BM] M. Blum, and S. Micali, "How to generate Cryptographically strong sequences of pseudo-random bits", em SIAM J. on Computing, Vol. 13, 1984, pp. 850-864.

[Br] G. Bracha, "An Asynchronous $\lfloor (n-1)/3 \rfloor$-resilient Consensus Protocol", *3rd PODC,* 1984, pp. 154-162.

[BCC] G. Brassard, D. Chaum and C. Crepeau, "Minimum Disclosure Proofs of Knowledge", *Journal of Computing and System Sciences,* Vol. 37, No. 2, 1988, pp. 156-189.

[C] R. Canetti, "Asynchronous Secure Computation", *Technical Report no. 755,* CS department, Technion, 1992.

[CDNO] R. Canetti, C. Dwork, M. Naor and R. Ostrovsky, "Deniable Encryptions", manuscript.

[CFGN] R. Canetti, U. Feige, O. Goldreich and M. Naor, "Adaptively Secure Computation", *28th STOC,* 1996.

[CG] R. Canetti and R. Genaro, "Deniable Multiparty Computation", manuscript.

[CHH] R. Canetti, S. Halevi and A. Herzberg, "How to Maintain Authenticated Communication in the Presence of Break-ins", manuscript.

[CaH] R. Canetti and A. Herzberg, "Maintaining security in the presence of transient faults", *Crypto' 94*, 1994, pp. 425-439.

[CR] R. Canetti and T. Rabin, "Optimal Asynchronous Byzantine Agreement", *25th STOC,* 1993, pp. 42-51.

[CCD] D. Chaum, C. Crepeau and I Damgard, "Multiparty unconditionally secure protocols", *20th STOC,* 1988, pp. 11-19.

[CD] B. Chor and C. Dwork, "Randomization in Byzantine Agreement", *Advances in Computing Research, Vol. 5*, 1989, pp. 443-497.

[CGMA] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults", *26th FOCS,* 1985, pp. 383-395.

[CK] B. Chor and E. Kushilevitz, "A Zero-One Law for Boolean Privacy", *SIAM J. on Disc. Math., Vol. 4, no. 1,* 1991, pp.36-47.

[CM] B. Chor and L. Moscovici, "Solvability in Asynchronous Environments", *30th FOCS,* 1989.

[ChH] C. Chow and A. Herzberg, "A reconstructible proactive pseudo-randomness protocol", Work in progress, June 1994.

[DP] A. De-Santis and G. Persiano, "Zero-Knowledge proofs of knowledge without interaction", *33rd FOCS,* pp. 427-436, 1992.

[DH] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Trans. on Info. Theory*, IT-22(6), 1976, pp. 644-654.

[Ed] J. Edmonds, 'Paths, Trees, and Flowers", *Canadian J. of Math., Vol.17,* 1965, pp. 449-467.

[DDN] D. Dolev, C. Dwork and M. Naor, "Non-malleable Cryptography", *23rd STOC,* 1991.

[ER] M. Elchin and J. Rochlis, "With microscope and tweezers: An analysis of the internet virus of november 1988", *IEEE Symp. on Security and Privacy*, 1989, pp. 326–343.

[EGL] S. Even, O. Goldreich and A. Lempel, "A randomized protocol for signing contracts", *CACM,* vol. 28, No. 6,1985, pp. 637-647.

[Fe] P. Feldman, "Asynchronous Byzantine Agreement in Constant Expected Time", unpublished manuscript, 1989.

[FM] P. Feldman and S. Micali, "An Optimal Algorithm For Synchronous Byzantine Agreement", *20th STOC,* 1988, pp. 148-161.

[F] M. Fischer, "The Consensus Problem in Unreliable Distributed System", *Technical Report, Yale University*, 1983.

[FLP] M. Fischer, N. Lynch and M. Paterson, "Impossibility of Distributed Consensus with One Faulty Process", *JACM, Vol. 32, no. 2,* 1985, pp. 374-382.

[GJ] M. R. Garey and D. S. Johnson, *"Computers and Intractability : a guide to NP-Completeness",* W.H. Freeman ed., N.Y., 1979.

[G] O. Goldreich, "Foundations of Cryptography (Fragments of a Book)", ed. Dept. of Computer Science and Applied Mathemetics, Weizmann Institute, 1995.

[GGL] O. Goldreich, S. Goldwasser, and N. Linial, "Fault-Tolerant Computation in the Full Information Model", *32nd FOCS,* 1991, pp. 447-457.

[GGM1] O. Goldreich, S. Goldwasser, and S. Micali, "On the cryptographic applications of random functions", *Advances in Cryptology: Proc. of Crypto 84*, 1984, pp. 276-288.

[GGM2] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions" *J. ACM*, 33(4), 1986, pp. 792-807. Extended abstract in FOCS84.

[GILVZ] O. Goldreich, R. Impagliazzo, L. Levin, R. Venkatesan and D. Zuckerman, "Security Preserving Amplification of Hardness", FOCS 1990, pp. 318–326.

[GrL] O. Goldreich and L. Levin, "A Hard-Core Predicate to any One-Way Function", *21st STOC,* 1989, pp. 25-32.

[GMW] O. Goldreich, S. Micali and A. Wigderson, "How to Play any Mental Game", *19th STOC,* 1987,pp. 218-229.

[GwL] S. Goldwasser, and L. Levin, "Fair Computation of General Functions in Presence of Immoral Majority", *CRYPTO,* 1990.

[HILL] J. Hästad, R. Impagliazzo, L. Levin, and M. Luby, "Construction of pseudo-random generator from any one-way functions", Manuscript, see preliminary versions by Impagliazzo et al. in *21st STOC* and Hästad in *22nd STOC*, 1993.

[HJJKY] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk and M. Yung, "Proactive Public-Key and Signature Systems", manusript.

[HJKY] A. Herzberg, S. Jarecki, H. Krawczyk and M. Yung, "Proactive Secret Sharing or: How to Cope with Perpetual Leakage", *CRYPTO* 1995.

[IR] R. Impagliiazzo and S. Rudich, "Limits on the provable consequences of one-way permutations", *21th STOC,* 1989, pp. 44-58.

[KY] A. Karlin and A. Yao, "Probabilistic Lower Bounds for Byzantine Agreement", unpublished manuscript, 1986.

[LE] T. A. Longstaff and S. E. Eugene, "Beyond preliminary analysis of the wank and oilz worms: A case of study of malicious code", *Computers and Security*, 12(1), 1993, pp. 61-77.

[MS] F. J. Macwiliams and N. J. A. Sloane, *"The Theory of Error Correcting Codes",* North-Holland, 1977.

[MR] S. Micali and P. Rogaway, "Secure Computation", in preparation. Preliminary version in *CRYPTO 91.*

[MV] S. Micali and V. Vazirani, "An $O(\sqrt{|V|} \cdot |E|)$ Algorithm for Finding Maximum Matching in General Graphs", *21st FOCS,* 1980.

[MNSS] S. P. Miller, C. Neuman, J. I. Schiller, and J. H. Saltzer, "Kerberos authentication and authorization system", *Project Athena Technical Plan.* Massachusetts Institute of Technology, July 1987.

[MT] R. H. Morris and K. Thompson, "Unix password security", *Comm. ACM*, 22(11), November 1979, pp. 594-597.

[OY] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks", *Proceedings of the* 10^{th} *Annual ACM Symposium on Principles of Distributed Computing,* 1991, pp 51–59.

[PSL] R. Pease, Shostak and L. Lamport, "Reaching Agreement in the Presence of Faults", *JACM, Vol. 27 No. 2,* 1980, pp. 228-234.

[MRa1] M. Rabin, "How to exchange secrets by oblivious transfer", Tech. Memo TR-81, Aiken Computation Laboratory, Harvard U., 1981.

[MRa2] M. Rabin, "Randomized Byzantine Generals", *24th FOCS,* 1983, pp. 403-409.

[RB] T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority", *21st STOC,* 1989, pp. 73-85.

[TRa] T. Rabin , "Robust Sharing of Secrets When The Dealer is Honest or Faulty", *Journal of the ACM*, No. 6, Vol. 41, 1994, pp. 1089-1109.

[Re] R. Reischuk, "A new solution to the byzantine generals problem", *Information and Control*, 1985, pp. 23-42.

[SK] K. Sako and J. Kilian, "Receipt-Free Mix-Type Voting Scheme", *Eurocrypt* 1995, pp. 393-403.

[Sh] A. Shamir, "How to share a secret", *CACM, Vol. 22, No. 11,* 1979, pp. 612-613.

[St] C. Stoll, "How secure are computers in the u.s.a.?", *Computers and Security*, 7(6), 1988, pp. 543-547.

[Y1] A. Yao, "Protocols for Secure Computation", *23th FOCS,* 1982, pp. 160-164.

[Y2] A. Yao, "Theory and applications of trapdoor functions", *23rd FOCS,* 1982, pp. 80-91.