6.897: Selected Topics In Cryptography Canetti and Rivest

Handout 2: Planned lecture schedule until spring break

5 Thursday 2004

Lecture 1 (2/5/4): Overview of the course. The "classic" definitional framework of multiparty function evaluation (along the lines of [C00]): Motivation for the ideal-model paradigm. The basic definition.

Lecture 2 (2/6/4): Variants of the basic definition. Non-concurrent composition.

Lecture 3 (2/12/4): Example: Casting Zero-Knowledge within the basic definitional framework. The Blum protocol for Graph Hamiltonicity. Composability of Zero-Knowledge.

Lecture 4 (2/13/4): The universally composable (UC) security framework: Motivation and the basic definition (based on [C01]).

Lecture 5 (2/19/4): No lecture (TCC)

Lecture 6 (2/20/4): No lecture (TCC)

Lecture 7 (2/26/4): Alternative formulations of UC security. The universal composition theorem. Survey of feasibility results in the UC framework.

Lecture 8 (2/27/4): UC commitments: Motivation. The ideal commitment functionality. Impossibility of realizations in the plain model. A protocol in the Common Reference String (CRS) model (based on [CF01]).

Lecture 9 (3/4/4): The multi-commitment functionality and realization. UC Zero Knowledge from UC commitments. Universal composition with joint state.

Lecture 10 (3/5/4): Secure realization of any multi-party functionality with any number of faults (based on [GMW87, G98, CLOS02]): The semi-honest case. (Static, adaptive, two-party, multi-party.)

Lecture 11 (3/11/4): Secure realization of any multi-party functionality with any number of faults: The Byzantine case. (Static, adaptive, two-party, multi-party.) The case of honest majority.

Lecture 12 (3/12/4): UC signatures. Equivalence with existential unforgeability against chosen message attacks (as in [GMRi88]). Usage for certification and authentication.

Lecture 13 (3/18/4): UC key-exchange and secure channels. (Based on [CK02]).

Lecture 14 (3/19/4): UC encryption and equivalence with security against adaptive chosen ciphertext attacks (CCA). Replayable CCA encryption. (Based on [CKN03].)

References

[C00] R. Canetti, "Security and composition of multi-party cryptographic protocols", *Journal of Cryptology,* Vol. 13, No. 1, winter 2000.

[C01] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *Proc. 42st FOCS*, pages 136–145. IEEE, 2001. http://eprint.iacr.org/2000/067.

[CF01] R. Canetti and M. Fischlin, "Universally Composable Commitments", Crypto '01, 2001.

[CK02] R. Canetti and H. Krawczyk. Universally Composable Key Exchange and Secure Channels . In *Eurocrypt '02*, pages 337–351, 2002. LNCS No. 2332.

[CKN03] R. Canetti, H. Krawczyk, and J. Nielsen, "Relaxing Chosen Ciphertext Security of Encryption Schemes," *Crypto '03,* 2003.

[CLOS02] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally Composable Two-Party and Multi-Party Secure Computation. In *Proc.* 34*th STOC*, pages 494–503.

[CR03] R. Canetti and T. Rabin, Universal Composition with Joint State, *Crypto'03,* 2003.

[G98] O. Goldreich. *"Secure Multi-Party Computation"*, 1998. (Available at http://philby.ucsd.edu)

[GMW87] O. Goldreich, S. Micali and A. Wigderson, "How to Play any Mental Game", *19th Symposium on Theory of Computing (STOC),* ACM, 1987, pp. 218-229.

[GMRi88] S. Goldwasser, S. Micali, and R.L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM J. Comput.*, April 1988, pages 281–308.