

Tutorial on Composability

Related Literature

Dominique Unruh

April 13, 2010

- The UC framework was first defined in [Can01]. The model was later extended and revised in [Can05]. There is a tutorial on the topic by Canetti [Can06] (I did not read that tutorial). A very compact summary of most of the important technical definitions of UC can be found in the section reviewing the UC framework in the full version of [MQU07]. Independently, Pfitzmann and Waidner (later joined by Backes) presented the Reactive Simulatability framework [PW00, BPW07] which essentially shares the same ideas.
- The impossibility of constructing UC commitments from scratch was shown in [CF01]. More general characterizations of functionalities that cannot be UC realized are given in [CKL03].
- [CF01] give protocols for implementing UC commitments from a CRS. [CLOS02] show how to do general multi-party computation based on a CRS. [BCNP04] shows how to use other setup assumptions than a CRS.
- [Lin03] shows that (a slight variant of) UC is actually the weakest notion that allows for universal composition.
- Examples of non-composability (in the special case of zero-knowledge protocols) are given in [GK96], [Fei90, Chapter 4], and, recently, [BV10].
- The idea of extractability to model the knowledge of some secure appears, as far as I know, first in the context of proofs of knowledge. The notion was sketched in [GMR85] and formally defined in [BG93].
- A symbolic variant of the UC model in the applied π -calculus has been presented in [DKP09].
- Finally, some of my own papers on the topic: [MQU07] shows how to extend the UC model to capture the notion of long-term security, i.e., security against adversaries that may break all crypto after the protocol's end. It also gives protocols for commitments and zero-knowledge proofs in that setting. [Unr10b] shows how to extend UC to the quantum case and gives protocols for two-party computation from commitments. [UMQ09] shows how to extend the idea of UC to model the possibility of coercions. [Unr10a] applies UC to the bounded quantum storage model. In [HUMQ07] (see also [CDPW07] for similar independent work) a variant of UC is discussed that allows to share a functionality between different protocols.

References

- [BCNP04] Boaz Barak, Ran Canetti, Jesper Buus Nielsen, and Rafael Pass. Universally composable protocols with relaxed set-up assumptions. In *45th Symposium on Foundations of Computer Science, Proceedings of FOCS 2004, 17-19 October 2004, Rome, Italy*, pages 186–195. IEEE Computer Society, October 2004.
- [BG93] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Ernest F. Brickell, editor, *Advances in Cryptology, Proceedings of CRYPTO '92*, number 740 in Lecture Notes in Computer Science, pages 390–420. Springer-Verlag, 1993. Extended version online available at <http://www-cse.ucsd.edu/users/mihir/papers/pok.ps>.
- [BPW07] Michael Backes, Birgit Pfizmann, and Michael Waidner. The reactive simulatability (RSIM) framework for asynchronous systems. *Information and Computation*, 2007. Preliminary version available at <http://eprint.iacr.org/2004/082>.
- [BV10] Eleanor Birrell and Salil P. Vadhan. Composition of zero-knowledge proofs with efficient provers. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *Lecture Notes in Computer Science*, pages 572–587. Springer, 2010.
- [Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42th Annual Symposium on Foundations of Computer Science, Proceedings of FOCS 2001*, pages 136–145. IEEE Computer Society, 2001.
- [Can05] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. IACR ePrint Archive, January 2005. Full and revised version of [Can01], online available at <http://eprint.iacr.org/2000/067.ps>.
- [Can06] Ran Canetti. Security and composition of cryptographic protocols: a tutorial (part I). *SIGACT News*, 37(3):67–92, 2006. Updated version on <http://eprint.iacr.org/2006/465>.
- [CDPW07] Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish. Universally composable security with global setup. In *Theory of Cryptography, Proceedings of TCC 2007*, volume 4392 of *LNCS*, pages 61–85. Springer, March 2007.
- [CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In *Crypto 2001*, volume 2139 of *LNCS*, pages 19–40. Springer, 2001. Full version is IACR ePrint 2001/055.
- [CKL03] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. In Eli Biham, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2003*, number 2656 in Lecture Notes in Computer Science, pages 68–86. Springer-Verlag, 2003. Full version online available at <http://eprint.iacr.org/2004/116.ps>.
- [CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *34th Annual ACM Symposium on Theory of Computing, Proceedings of STOC 2002*, pages 494–503. ACM Press, 2002. Extended abstract, full version online available at <http://eprint.iacr.org/2002/140.ps>.

- [DKP09] Stéphanie Delaune, Steve Kremer, and Olivier Pereira. Simulation based security in the applied pi calculus. In Ravi Kannan and K Narayan Kumar, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2009)*, volume 4 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 169–180, Dagstuhl, Germany, 2009. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [Fei90] Uriel Feige. *Alternative Models for Zero Knowledge Interactive Proofs*. PhD thesis, Weizmann Institute of Science, 1990. Online available at <http://www.wisdom.weizmann.ac.il/~feige/thesis.ps>.
- [GK96] Oded Goldreich and Hugo Krawczyk. On the composition of zero-knowledge proof systems. *SIAM J. Comput.*, 25(1):169–192, 1996. Extended version online available at <http://www.wisdom.weizmann.ac.il/~oded/PS/zk-comp.ps>.
- [GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304. ACM Press, 1985.
- [HUMQ07] Dennis Hofheinz, Dominique Unruh, and Jörn Müller-Quade. Universally composable zero-knowledge arguments and commitments from signature cards. *Tatra Mt. Math. Publ.*, 37:93–103, 2007. Online available at <http://crypto.m2ci.org/unruh/publications/hofheinz07universally.html>.
- [Lin03] Yehuda Lindell. General composition and universal composability in secure multi-party computation. In *44th Annual Symposium on Foundations of Computer Science, Proceedings of FOCS 2003*, pages 394–403. IEEE Computer Society, 2003. Online available at <http://eprint.iacr.org/2003/141>.
- [MQU07] Jörn Müller-Quade and Dominique Unruh. Long-term security and universal composability. In *Theory of Cryptography, Proceedings of TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 41–60. Springer-Verlag, March 2007. Full version on <http://eprint.iacr.org/2006/422>.
- [PW00] Birgit Pfitzmann and Michael Waidner. Composition and integrity preservation of secure reactive systems. In *Proc. 7th ACM Conference on Computer and Communications Security*, pages 245–254, 2000. Extended version (with Matthias Schunter) IBM Research Report RZ 3206, May 2000, <http://www.semper.org/sirene/publ/PfSW1::00ReactSimulIBM.ps.gz>.
- [UMQ09] Dominique Unruh and Jörn Müller-Quade. Universally composable incoercibility, October 2009. Preprint on IACR ePrint 2009/520.
- [Unr10a] Dominique Unruh. Concurrent composition in the bounded quantum storage model. Note yet available online. If you wish to get a preliminary copy, please send me an email., 2010.
- [Unr10b] Dominique Unruh. Universally composable quantum multi-party computation. In *EUROCRYPT 2010*, LNCS. Springer, 2010. To appear, preprint on arXiv:0910.2912 [quant-ph].