UNIVERSITY OF CALIFORNIA
Los Angeles

Stronger Notions of Secure Computation

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Computer Science

by

Vipul Goyal

2009

The dissertation of Vipul Goyal is approved.

Professor Paul Balmer

Professor Adam Meyerson

Professor Yuval Ishai

Professor Rafail Ostrovsky, Committee Co-chair

Professor Amit Sahai, Committee Co-chair

University of California, Los Angeles

2009

ACKNOWLEDGMENTS

First of all, I would like to thank my advisors Rafail Ostrovsky and Amit Sahai for their constant support and inspiration. Rafi is an unending source of excellent research problems. I have always been amazed at his ability to draw connections between seemingly unrelated concepts. I have learnt a lot from him about identifying the right problems and solving them. Amit is an amazing listener and can understand my unorganized and half baked ideas really well. His clarity of thought is striking. Amit puts more faith in me than I do myself. My maturing as a researcher has a lot to do with my interactions with Amit. I will always be grateful to Amit and Rafi for taking me as a student and giving me the direction I needed early on in my research career.

I was very lucky that Yuval Ishai was at UCLA during the second half of my PhD. Yuval has deeply influenced my attitude towards research (without even knowing it). I have learnt a lot from Yuval about how not to quit working on a problem until you get the right results. Yuval has been almost like a third (!) advisor to me.

I would like to thank Ramarathnam Venkatesan for hosting me for two summers in Microsoft Redmond. Venkie has taught me a lot of Mathematics and working with him was always fun. I would also like to thank him and his family for the all the dinners at their house. My grocery expenses during those summers were close to zero.

I thank Ilya Mironov for hosting me for a summer in Microsoft SVC. I learnt a lot about Differential Privacy from Ilya. I thank him for patiently teaching me so much at a time when I had no background in the area. Working with him has been a pleasure.

I would like to thank my co-authors for doing all the work in my papers: Alexandra Boldyreva, Nishanth Chandran, Yi Deng, Serge Fehr, Sanjam Garg, Jens Groth, Yuval

Ishai, Abhishek Jain, Jonathan Katz, Virendra Kumar, Steve Lu, Ilya Mironov, Payman Mohassel, Mohammad Mahmoody-Ghidary, Ryan Moriarty, Rafail Ostrovsky, Omkant Pandey, Amit Sahai, Adam Smith, Ramarathnam Venkatesan, Akshay Wadia, and Brent Waters. I hope they will continue doing the same in future.

Special thanks go to Omkant Pandey for our seemingly infinite arguments about all things non-technical and technical. Omkant kept me from doing productive work several times successfully and made me miss quite a few submission deadlines. On the positive side, Omkant taught me a lot about zero-knowledge, non-malleability, and general philosophy of research.

Thanks to Nishanth Chandran, Abhishek Jain, and Ryan Moriarty for all the technical discussions and fun times. I thank others in the current group for contributing to my great experience at UCLA: Paul Bunn, Sanjam Garg, Ran Gelles, Brett Hemenway, Abishek Kumarasubramanian, Steve Lu, Claudio Orlandi, Bhavani Shankar, Ivan Visconti, and Akshay Wadia. Special thanks to Abishek Kumarasubramanian for his generous help back when I was suffering from RSI.

I would like to thank my PhD committee members: Paul Balmer, Yuval Ishai, Adam Meyerson, Rafail Ostrovsky, and Amit Sahai.

Finally I would like to thank my mother for her love and unconditional support in whatever I have chosen to do in my life.

VITA

1983	Born, Bulandshahr, U.P., India.
2000–2004	B.Tech. Computer Science, Institute of Technology – BHU, India.
2005–2007	M.S. Computer Science, UCLA.
2005–2009	Ph.D. student, Department of Computer Science, UCLA.
2005–2008	Research Assistant, Department of Computer Science, UCLA. For 4 academic quarters during this time period.
Fall 2006	Research Fellow. Institute for Pure and Applied Mathematics, UCLA.
Fall 2007	Teaching Assistant, Department of Computer Science, UCLA.
2008	Microsoft Research Graduate Fellowship.
2009	Google Outstanding Graduate Student Research Award.

PUBLICATIONS

Yi Deng, Vipul Goyal and Amit Sahai, ”Resolving the Simultaneous Resettability Conjecture and a New Non-Black-Box Simulation Strategy”. In FOCS 2009. IEEE Symposium on Foundations of Computer Science, Atlanta, USA, Oct 2009.

Nishanth Chandran, Vipul Goyal, Ryan Moriarty and Rafail Ostrovsky, ”Position Based Cryptography”. In CRYPTO 2009. Advances in Cryptology, Santa Barbara, USA, August 2009.

Vipul Goyal and Amit Sahai, ”Resettably Secure Computation”. In EUROCRYPT 2009. Advances in Cryptology, Germany, April 2009.

Vipul Goyal, Steve Lu, Amit Sahai and Brent Waters, ”Black-box Accountable Authority Identity Based Encryption”. In CCS 2008. ACM Conference on Computer and Communications Security, Alexandria, USA, November 2008

Alexandra Boldyreva, Vipul Goyal and Virendra Kumar, ”Efficient Revocation in Identity Based Encryption”. In CCS 2008. ACM Conference on Computer and Communications Security, Alexandria, USA, November 2008.

Vipul Goyal, Abhishek Jain, Omkant Pandey and Amit Sahai, ”Bounded Ciphertext Policy Attribute Based Encryption”. In ICALP 2008. International Colloquium on Automata, Languages and Programming, Iceland, July 2008.

Vipul Goyal, Payman Mohassel and Adam Smith, ”Efficient Two Party and Multi Party Computation against Covert Adversaries”. In EUROCRYPT 2008. Advances in Cryptology, Turkey, April 2008.

Nishanth Chandran, Vipul Goyal and Amit Sahai, ”New Constructions for UC Secure Computation with Tamper-Proof Hardware”. In EUROCRYPT 2008. Advances in Cryptology, Turkey, April 2008.

Vipul Goyal and Jonathan Katz, ”Universally Composable Multi-Party Computation with an Unreliable Common Reference String”. In TCC 2008. Theory of Cryptography Conference, New York, USA, March 2008.

Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky and Amit Sahai, ”Concurrent Statistical Zero Knowledge Arguments for NP from One Way Functions”. In ASIACRYPT 2007. Advances in Cryptology, Malaysia, Dec 2007.

Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky and Amit Sahai, ”Covert Multi-Party Computation”. In FOCS 2007. IEEE Symposium on Foundations of Computer Science, Providence, USA, Oct 2007.

Vipul Goyal, ”Reducing Trust in the PKG in Identity Based Cryptosystems”. In CRYPTO 2007. Advances in Cryptology, Santa Barbara, USA, August 2007.

Vipul Goyal, ”Certificate Revocation using Fine Grained Certificate Space Partitioning”. In FC 2007. Financial Cryptography and Data Security Conference, Trinidad and Tobago, February 2007.

Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, ”Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”. In CCS 2006. ACM Conference on Computer and Communications Security, Alexandria, USA, November 2006.

ABSTRACT OF THE DISSERTATION

Stronger Notions of Secure Computation

by

Vipul Goyal

Doctor of Philosophy in Computer Science

University of California, Los Angeles, 2009

Professor Amit Sahai, Co-chair

Professor Rafail Ostrovsky, Co-chair

The concept of secure computation protocols was introduced in the seminal works of Yao and Goldreich et al. In this setting, a set of parties wish to compute a joint function of the inputs which they individually hold. The protocol for computation of this function should be such that it does not leak any information about the individual inputs (other than what is leaked by the output itself). General feasibility results for secure computation were obtained by Yao and Goldreich et. al. in mid 1980's. Since then, designing secure computation protocols satisfying stronger security notions has been an active area of research. In this dissertation, we consider two different stronger notions of secure computation.

We first consider the notion of resettable security where the security of a party should be maintained even if it uses the same randomness in multiple protocol executions. A well known problem left open by previous works in this area is whether it is possible to have a secure zero-knowledge protocol in which both parties may be resettable. We resolve this question in the positive by constructing such a protocol. At the heart of our construction is a novel non-black-box simulation strategy, which we believe to be of independent interest.

We then consider the notion of covert computation where the parties can run a protocol without knowing if other parties are also participating in the protocol or not. At the end of the protocol, if all parties participated in the protocol and if the function output is favorable to all parties, only then the output is revealed. In this dissertation, we present the first construction for covert multi-party computation. In order to achieve this goal, we introduce a number of new techniques. One central technical contribution is the development of zero-knowledge proofs to garbled circuits technique. Along the way, we also develop a definition of covert computation as per the Ideal/Real model simulation paradigm.

The results presented in this dissertation stem from two papers which are respectively joint work with Amit Sahai, and with Nishanth Chandran, Rafail Ostrovsky and Amit Sahai.