CORNELL TECH

Rafael Pass

Professor
Department of Computer Science
Cornell University and Cornell Tech

Ph.D, MIT, 2006
first name at cs.cornell.edu

Cornell Tech, 2 W Loop Rd
New York, NY 10044

Summary

I am a Professor in the Department of Computer Science at Cornell University and at Cornell Tech. I obtained my Ph.D in 2006 in the Theory of Computation group at MIT with Silvio Micali as advisor.
Previously, I completed my Licentiate Thesis (M.S.) under the supervision of Johan Hastad.

My research focuses on Cryptography and its interplay with Computational Complexity and Game Theory; lately, I have become increasingly interested in the theoretical foundations of blockchains.

My work has been supported by a NSF Career Award, a Microsoft Faculty Fellowship, an AFOSR Young Investigator Award, an Alfred P. Sloan Foundation Fellowship, a Wallenberg Academy Award, a Google Faculty Award, as well as grants from AFOSR, BSF and DARPA.

My CV: pdf (Aug 2017)

Lecture Notes

- ***R. Pass: A Course in Networks and Markets.*** pdf (last updated Aug 2017)
  An Meng course (with additional advanced material) in Algorithmic Game Theory focused on Networks and Markets.
- ***R. Pass and W. Tseng: A Course in Discrete Structures.*** pdf (last updated Aug 2011)
  A undergraduate course in basic Discrete Mathematics, with applications in Cryptography and Game Theory.
- ***R. Pass and A. Shelat: A Course in Cryptography.*** pdf (last updated Jan 2010)
  An upper-level introductory undergraduate course in Cryptography.

Projects

- **anonize.org**: An anonymous and accountable survey system.
  Our system is e.g., used in the Brave browser (founded by Mozilla co-founder Brendan Eich) to

enable large-scale anonymous and accountable collection of browsing statistics.
- **Thunderella:** Open source implementation of a Fast and Scalable Blockchain (coming soon)

Teaching

- CS 5854 Networks and Markets (Meng) [Fa 17] [Fa 16]
- CS 6830 Cryptography (Ph.D) [Sp 17] [Sp 16] [Fa 14] [Fa 11] [Fa 09] [Fa 08] [Fa 06]
- CS 5831 Security Protocols and Privacy (MEng) [Sp 14]
- CS 5830 Cryptography (MEng) [Fa 13]
- CS 4830 Introduction to Cryptography (undergraduate) [Fa 10] [Fa 08] [Fa 07]
- CS 2800 Discrete Structures (undergraduate) [Sp 13] [Sp 12] [Sp 11]
- CS 6810 Theory of Computing (Ph. D) [Sp 08]
- CS 787 Topics in Cryptography [Sp 07]
- CS 7893 Crypto breakfast (Ph. D) every semester since 08
- NBAY 5400 Tech for Business (MBA) [Fa 16] [Fa 15]

Current Ph.D. Students

- Antonio Marcedone
- Andrew Morgan
- Naomi Ephraim

Graduated Ph.D. Students

- Muthuramakrishnan Venkitasubramaniam (CI Fellow at NYU, now tenured at U. Rochester)
- Huijia (Rachel) Lin (postdoc at MIT & BU, now tenure-track at UCSB)
- Wei-lung Dustin Tseng (now at Google)
- Lior Seeman (joint with Joseph Halpern, now at Uber Research)
- Edward Lui (now at start-up)
- Adam Bjorndahl (informally co-advised with Joseph Halpern, now tenure-track at CMU)
- Karn Seth (now at Google)
- Sidharth Telang (now at Google)

Current and Previous Post Docs

- Ilan Komargodski (Ph.D. Weizmann)
- Antigoni Polychroniadou (Ph.D Aarhus, joint with Elaine Shi and Muthu Venkitasubramaniam)
- Gilad Asharov (Ph.D. Bar-Ilan, Simons fellow)
- Elette Boyle (Ph.D. MIT, now tenure-track at IDC)
- Kai-min Chung (Ph.D. Harvard, now tenured at Academia Sinica)
- Mohammad Mahmoody (Ph.D. Princeton, now at tenure-track at UVA)

Program Commitees

- 15th Theory of Cryptography Conference (TCC 17).
- 37th Annual International Cryptology Conference (CRYPTO 17).
- 14th Theory of Cryptography Conference (TCC 16).
- 10th Annual Conference on Security and Cryptography for Networks (SCN 16).
- 6th Innovations in Theoretical Computer Science Conference (ITCS 16).
- 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS 15).
- 5th Innovations in Theoretical Computer Science Conference (ITCS 15).
- 34th Annual International Cryptology Conference (CRYPTO 2014).
- 31th Annual International Conference on Theory and Applications of Cryptographic Techniques (EuroCrypt 2014).

- 26th Annual IEEE Computer Security Foundations (CSF 2013).
- 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012).
- 31th Annual International Cryptology Conference (CRYPTO 2011).
- 30th Annual International Cryptology Conference (CRYPTO 2010).
- 1st Innovations in Computer Science (ICS 2010).
- 29th Annual International Cryptology Conference (CRYPTO 2009).
- 6th Theory of Cryptography Conference (TCC 09).
- 39th ACM Symposium on Theory of Computing (STOC 08).
- 35th International Colloquium on Automata, Languages and Programming (ICALP 08)..
- RSA Conference 2008, Cryptographers Track (CT-RSA 08).
- 34th International Colloquium on Automata, Languages and Programming (ICALP 07).
- 4th Theory of Cryptography Conference (TCC 07).

Papers

2017

- ***Two-Round and Non-interactive Concurrent Non-Malleable Commitment from Time-Lock Puzzles*** (FOCS 17)
  H. Lin, R. Pass and P. Soni pdf
- ***Analysis of the Blockchain Protocol in Asynchronous Network***s (EUROCRYPT 17)
  R. Pass, L. Seeman and A. Shelat pdf
- ***Formal Abstractions for Attested Execution Secure Processors*** (EUROCRYPT 17)
  Rafael Pass, Elaine Shi, Florian Tramer pdf
- ***FruitChains: A Fair Blockchain*** (PODC 17)
  R. Pass and E. Shi pdf
- ***The Sleepy Model of Consensus*** (ASIACRYPT 17)
  R. Pass and E. Shi pdf
- ***A Knowledge-Based Analysis of the Blockchain Protocol*** (TARK 17)
  J. Halpern and R. Pass pdf
- ***Hybrid Consensus: Efficient Consensus in the Permissionless Model*** (DISC 17)
  R. Pass and E. Shi pdf
- ***Socially Optimal Mining Pools*** (manuscript 2017)
  B. Fisch, R. Pass and A. Shelat pdf
- ***Can We Access a Database Both Locally and Privately?*** (manuscript 2017)
  E. Boyle, Y. Ishai, R. Pass, and M. Wootters pdf
- ***Oblivious Computation with Data Locality*** (manuscript 2017)
  G. Asharov, H. Chan, K. Nayak, R. Pass, L. Ren and E. Shi pdf
- ***Snow White: Provably Secure Proofs of Stake*** (manuscript 2017)
  P. Daian, R. Pass and E. Shi pdf

2016

- ***Sequential Equilibrium in Games of Imperfect Recall*** (KR 16)
  J. Halpern and R. Pass pdf
- ***Indistinguishability Obfuscation with Non-trivial Efficiency*** (PKC 16)
  H. Lin, R. Pass, K. Seth, and S. Telang pdf
- ***Bounded KDM Security from iO and OWF*** (SCN 16)
  A. Marcedone, R. Pass, and A. Shelat pdf
- ***Computational Extensive-Form Game***s (EC 16)
  J. Halpern, R. Pass, and L. Seeman pdf
- ***Impossibility of VBB Obfuscation with Ideal Constant-Degree Graded Encodings*** (TCC 16)
  R. Pass and A. Shelat pdf

- ***Lower Bounds on Assumptions Behind Indistinguishability Obfuscation*** (TCC 16)
  M. Mahmoody, A. Mohammed, S. Nematihaji, R. Pass, and A. Shelat pdf
- ***Output-Compressing Randomized Encodings and Applications*** (TCC 16)
  H. Lin, R. Pass, K. Seth, and S. Telang pdf
- ***Oblivious Parallel RAM and Applications*** (TCC 16)
  Elette Boyle, Kai-Min Chung, Rafael Pass pdf

2015

- ***Tight Revenue Bounds with Possibilistic Beliefs and Level-k Rationality*** (Econometrica 2015)
  J. Chen, S. Micali, R. Pass pdf supplement
- ***Algorithmic rationality: Game theory with costly computation*** (J. Economic Theory 2015)
  J. Halpern and R. Pass pdf
- ***Limits of Extractability Assumptions with Distributional Auxiliary Input*** (ASIACRYPT 15)
  E. Boyle and R. Pass pdf
- ***Micropayments for Decentralized Currencies*** (CCS 15)
  R. Pass and A. Shelat pdf
- ***Constant-Round Concurrent Zero-Knowledge from Indistinguishability Obfuscation*** (CRYPTO 15)
  K. Chung, H. Lin and R. Pass pdf
- ***Large-Scale Secure Computation: Multi-party Computation for (Parallel) RAM Programs*** (CRYPTO 15)
  E. Boyle, K. Chung, R. Pass pdf
- ***Voting with Coarse Beliefs*** (ITCS 15)
  S. Leung, E. Lui, and R. Pass pdf
- ***Better Outcomes from More Rationality*** (ITCS 15)
  J. Chen, S. Micali, R. Pass
  Superseeded by Tight Revenue Bounds with Possibilistic Beliefs and Level-k Rationality (Econometrica 2015)
- ***Succinct Randomized Encodings and their Applications*** (STOC 15)
  N. Bitansky, S. Garg, H. Lin, R. Pass and S. Telang pdf
  Invited to SIAM Journal of Computing, special issue for selected papers of STOC 2015.
- ***From Weak to Strong Zero-Knowledge and Applications*** (TCC 15)
  K. Chung, E. Lui, and R. Pass pdf
- ***Tight Parallel Repetition Theorems for Public-Coin Arguments Using KL-Divergence*** (TCC 15)
  K. Chung and R.Pass pdf
- ***Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma*** (TCC 15)
  V. Goyal, H. Lin, O. Pandey, R. Pass, and A. Sahai pdf
- ***Outlier Privacy*** (TCC 15)
  E. Lui, and R. Pass pdf
- ***Bayesian Games with Intentions*** (TARK 15)
  A. Bjorndahl, J. Halpern, and R Pass pdf

2014

- ***Concurrent Zero Knowledge, Revisited*** (J. Cryptology 2014)
  R. Pass, W. Tseng and M. Venkitasubramaniam pdf
- ***On the Impossibility of Black-Box Transformations in Mechanism Design*** (SAGT 2014)
  R. Pass, K. Seth pdf
- ***ANONIZE: A Large-Scale Anonymous Survey System*** (Oakland 14, IEEE Security & Privacy 2015)
  S. Hohenberger, S. Myers, R. Pass and A. Shelat pdf

Invited to the special issue in IEEE Security & Privacy for selected papers from Oakland 14.

- ***Not Just an Empty Threat: Subgame-Perfect Equilibrium in Repeated Games Played by Computationally Bounded Players*** (WINE 2014)
  J. Halpern, R. Pass and L. Seeman. pdf
- ***One-way Functions and (Imperfect) Obfuscation*** (FOCS 14)
  I. Komargodski, T. Moran, M. Naor, R. Pass, A. Rosen and E. Yogev. pdf
- ***On the Impossibility of Tamper-Resilient Cryptography*** (CRYPTO 14)
  P. Austrin, K. Chung, M. Mahmoody, R. Pass and K. Seth. pdf
- ***Indistinguishability Obfuscation from Semantically-secure Multilinear Graded Encodings*** (CRYPTO 14)
  R. Pass, K. Seth and S. Telang. pdf
- ***Reasoning About Rationality*** (KR 14, GEB 2016)
  A. Bjorndahl, J. Halpern and R. Pass. pdf
- ***The Truth Behing the Myth of the Folk Theorem*** (ITCS 14)
  J. Halpern, R. Pass, and L. Seeman. pdf
- ***On Extractability (a.k.a. Differing-Input) Obfuscation*** (TCC 14)
  E. Boyle, K. Chung, R. Pass pdf
- ***4-Round Resettably-Sound Zero-Knowledge*** (TCC 14)
  K. Chung, R. Ostrovsky, R. Pass, I. Visconti and M. Venkitasubramaniam. pdf
- ***Statistically-secure ORAM with \tilde{O}(log^2 n) Overhead*** (AsiaCrypt 14)
  K. Chung, Z. Lui and R. Pass. pdf

2013

- ***Knowledge-Preserving Interactive Coding*** (FOCS 13)
  K. Chung, R. Pass and S. Telang. pdf
- ***Constant-round Concurrent Zero-knowledge from P-Certificates*** (FOCS 13)
  K. Chung, H. Lui and R. Pass. pdf
- ***From Unprovability to Enviromental Friendly protocols*** (FOCS 13)
  K. Chung, H. Lui and R. Pass. pdf
- ***Simultaneous Resettability From One-way Functions*** (FOCS 13)
  K. Chung, R. Ostrovsky, R. Pass and I. Visconti. pdf
- ***Non-black-box Simulation from One-way Functions and Applications to Resettable Security*** (STOC 13, SICOMP 2016)
  K. Chung, R. Pass and K. Seth. pdf
  SIAM Journal of Computing, special issue for selected papers of STOC 2013.
- ***Sequential Equilibrium in Computational Games*** (IJCAI 13)
  J. Halpern and R. Pass. pdf
- ***Conservative Belief and Rationality*** (Games and Economic Behavior 13)
  J. Halpern and R. Pass. pdf
- ***Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments*** (TCC 13, Computational Complexity 2016)
  R. Pass. pdf
  Invited to the JoC special issue of selected papers from TCC 13.
  Invited to the TCC 10-year anniversary special issue in Computational Complexity.
- ***Randomness Dependent Security*** (TCC 13)
  E. Birrell, K. Chung, R. Pass and S. Telang. pdf
- ***Game Theory with Translucent Players*** (TARK 13)
  J. Halpern and R. Pass. pdf
- ***Language-based Games*** (TARK 13)
  A. Bjorndahl, J. Halpern and R. Pass. pdf
- ***On the Power of Many One-Bit Provers*** (ITCS 13)

P. Austrin, J. Hastad, and R. Pass. pdf
- **On the Power of Non-uniform Proofs of Security** (ITCS 13)
  K. Chung, H. Lin, M. Mahmoody, and R. Pass. pdf
- ***A Cryptographic Treatment of Forecast Testing*** (ITCS 13)
  K. Chung, E. Lui, and R. Pass. pdf
- ***A Simple ORAM*** (manuscript 2013)
  K. Chung and R. Pass. pdf

2012

- ***Concurrent Zero-knowledge, Revisited*** (Journal of Cryptology 12)
  Rafael Pass, Wei-lung Tseng, and M. Venkitasubramaniam. pdf
- ***Crowd-blending Privacy*** (Crypto 12)
  J. Gehrke, M. Hay, E. Lui and R. Pass. pdf
- ***The Curious Case of Non-interactive Commitments: On The Power of Black-box v.s. Non-black-box Use of Primitives*** (Crypto 12)
  M. Mahmoody and R. Pass. pdf
- ***Black-box Constructions of Composable Protocols Without Set-up*** (Crypto 12)
  H. Lin and R. Pass. pdf
- ***I m doing as Well as a I Can: Modeling People and Rational Finite Automata*** (AAAI 12)
  J. Halpern, R. Pass, and L. Seeman. pdf
- ***The Knowledge Tightness of Parallel Zero-knowledge*** (TCC 12)
  K. Chung, R. Pass and W. Tseng. pdf
- ***Multi-verifier Signatures.*** (Journal of Cryptology 12)
  T. Roeder, R. Pass, and F. Schneider. pdf
- ***Unprovable Security of Two-Message Zero-Knowledge*** (manuscript 2012)
  K. Chung, E. Lui, M. Mahmoody, and R. Pass. pdf

2011

- ***The Randomness Complexity of Parallel Repetition.*** (FOCS 11)
  K. Chung and R. Pass. pdf
- ***Approximately Strategy-Proof Voting.*** (IJCAI 11)
  Eleanor Birrell and R. Pass. pdf
- ***Constant-round Non-malleable Commitments from Any One-way Function.*** (STOC 11, JACM 2015)
  Huijia Lin and R. Pass. pdf
- ***Limits of Provable Security from Standard Assumptions.*** (STOC 11)
  R. Pass. pdf
- ***Public-coin Parallel Zero-knowledge for NP*** (Journal of Cryptology 11)
  Rafael Pass, Alon Rosen and Wei-lung Tseng. pdf
- ***Algorithmic Rationality: Adding Cost of Computation to Game Theory.*** (SIGECOM 11)
  J. Halpern and R. Pass. pdf
- ***Reasoning About Justified Belief.*** (TARK 11)
  A. Bjorndahl, J. Halpern and R. Pass. pdf
- ***Concurrent Non-malleable Zero Knowledge with Adaptive Inputs.*** (TCC 11)
  H. Lin and R. Pass. pdf
- ***Towards Privacy in Social Networks: A Zero-knowledge Based Definition of Privacy.*** (TCC 11)
  J. Gehrke, R. Pass and E. Lui. pdf
- ***Towards Non-black-box Separations in Cryptography.*** (TCC 11)
  R. Pass, M. Venkitasubramaniam and W. Tseng. pdf

- ***Renegotiation-Safe Protocols.*** (ICS 11)
  R. Pass and A. Shelat. pdf

2010

- ***Adaptive Hardness and Composable Security from Standard Assumptions.*** (FOCS 10, SICOMP 2016)
  R. Canetti, H. Lin and R. Pass. pdf
  SIAM Journal of Computing, special issue for selected papers of FOCS 2010.
- ***Concurrent Non-malleable Zero Knowledge Proofs.*** (Crypto 10)
  H. Lin, R. Pass, M. Venkitasubramaniam and W. Tseng. pdf
- ***I Don t Want to Think About it Now: Decision Theory with Costly Computation.*** (KR 10)
  J. Halpern and R. Pass. pdf
- ***Constant-round Non-malleable Commitments from Sub-Exponential One-way Functions.*** (EuroCrypt 10)
  R. Pass and H. Wee. pdf
- ***Eye for an Eye: Efficient Concurrent Zero Knowledge in the Timing Model***. (TCC 10)
  R. Pass, M. Venkitasubramaniam and W. Tseng. pdf
- ***Private Coins versus Public Coins in Zero-Knowledge Proof Systems.*** (TCC 10)
  R. Pass and M. Venkitasubramaniam. pdf
- ***An Efficient Parallel Repetition Theorem.*** (TCC 10)
  J. Hastad, R. Pass, D. Wikstrom and K. Pietrzak. pdf
- ***Game Theory with Costly Computation: Formulation and Application to Protocol Security.*** (ICS 10)
  J. Halpern and R. Pass. pdf
  This paper is significantly extended in the following two working papers:
  Algorithmic Rationality: Game Theory with Costly Computation and *A Computational Game-theoretic Framework for Cryptography*).
- ***Algorithmic Rationality: Game Theory with Costly Computation.***
  J. Halpern and R. Pass. pdf (preliminary version in ICS 10)
- ***A Computational Game-theoretic Framework for Cryptography.***
  J. Halpern and R. Pass. pdf (preliminary version in ICS 10)

2009

- ***On the Composition of Public-coin Zero Knowledge***. (Crypto 09, SICOMP 11)
  R. Pass, W. Tseng and D. Wikstrom. pdf
- ***A Logical Characterization of Iterated Admissibility.*** (TARK 09)
  J. Halpern and R. Pass. pdf
- ***An Epistemic Characterization of Zero Knowledge.*** (TARK 09)
  J. Halpern, R. Pass and V. Raman. pdf
- ***Iterated Regret Minimization: A New Solution Concept.*** (IJCAI 09, Games and Economic Behavior 12)
  J. Halpern and R. Pass. pdf
  Non-malleability Amplification. (STOC 09)
  H. Lin and R. Pass. pdf
- ***A Unified Framework for Concurrent Security: Universal Composability from Stand-alone Non-malleability.*** (STOC 09)
  H. Lin, R. Pass and M. Venkitasubramaniam. pdf
- ***Black-box Constructions of Two-party Protocols from One-way Functions.*** (TCC 09)
  R. Pass and H. Wee.

2008

- ***Adaptive One-way Functions and Applications.*** (Crypto 08)

O. Pandey, R. Pass and V. Vaikuntanathan. pdf
- ***Precise Concurrent Zero Knowledge.*** (EuroCrypt 08)
  O. Pandey, R. Pass, A. Sahai, W. Tseng and M. Venkitasubramaniam. pdf
- ***Concurrent Non-malleable Commitments from One-way Functions.*** (TCC 08)
  H. Lin, R. Pass and M. Venkitasubramaniam. pdf
- ***On Constant-Round Concurrent Zero Knowledge.*** (TCC 08)
  R. Pass and M. Venkitasubramaniam. pdf

2007
- ***Precise Zero Knowledge.***
  S. Micali and R. Pass. pdf
  Manuscript, December 2007.
  This version combines results from Local Zero Knowledge and Precise Cryptography
- ***Precise Cryptography.***
  S. Micali and R. Pass. pdf
  Manuscript, September 2007. See Precise Zero Knowledge.
- ***Relations Among Notions of Non-malleability for Encryption.*** (AsiaCrypt 07)
  R. Pass, V. Vaikuntanathan and A. Shelat. pdf
- ***Bounded-CCA Secure Encryption.*** (AsiaCrypt 07)
  R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat and V. Vaikuntanathan. pdf
- ***Cryptography from Sunspots: How to Use an Imperfect Reference String.*** (FOCS 07)
  R. Canetti, R. Pass and A. Shelat. pdf
- ***An Efficient Parallel Repetition Theorem for Arthur-Merlin Games.*** (STOC 07)
  R. Pass and M. Venkitasubramaniam. pdf
- ***Universally Composable Protocols with Global Set-up.*** (TCC 07)
  R. Canetti, Y. Dodis, R. Pass and S. Walfish. pdf

2006
- ***A Precise Computational Approach to Knowledge.***
  R. Pass. pdf
  Ph.D Thesis. Massachusetts Institute of Technology, July 2006.
- ***Input-Indistinguishable Computation.*** (FOCS 06)
  S. Micali, R. Pass, A. Rosen. pdf
- ***Construction of a Non-Malleable Encryption Scheme From Any Semantically Secure One.*** (Crypto 06)
  R. Pass, A. Shelat and V. Vaikuntanathan. pdf
- ***On Arthur-Merlin Games and the Possibility of Basing Cryptography on NP-Hardness.*** (Complexity 06)
  R. Pass. pdf
  Invited to Computational Complexity, special issue on Conference of Computational Complexity 2006.
- ***Local Zero Knowledge.*** (STOC 06)
  S. Micali and R. Pass.
  See *A Precise Computational Approach to Knowledge* for a longer version.

2005
- ***Concurrent Non-Malleable Commitments.*** (FOCS 05, SICOMP 08)
  R. Pass and A. Rosen. pdf
  SIAM Journal of Computing, special issue for selected papers of FOCS 2005.
- ***Unconditional Characterizations of Non-Interactive Zero-Knowledge.*** (CRYPTO 05)
  R. Pass and A. Shelat. pdf
- ***Secure Computation Without Authentication.*** (CRYPTO 05)

B. Barak, R. Canetti, Y. Lindell, R. Pass and T. Rabin. pdf
- ***New and Improved Constructions of Non-Malleable Cryptographic Protocols.*** (STOC 05, SICOMP 08)
  R. Pass and A. Rosen. pdf
  SIAM Journal of Computing, special issue for selected papers of STOC 2005.

2004

- ***Universally Composable Protocols with Relaxed Set-up Assumptions.*** (FOCS 04)
  B. Barak, R. Canetti, J. Nielsen and R. Pass. pdf
- ***Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority.*** (STOC 04)
  R. Pass. pdf
- ***On the Possibility of One-Message Weak Zero-Knowledge.*** (TCC 04)
  B. Barak and R. Pass. pdf
- ***Alternative Variants of Zero-Knowledge Proofs.***
  R. Pass. pdf
  Licentiate (Master s) Thesis. ISBN 91-7283-933-3, 2004.

2003

- ***Bounded-Concurrent Secure Two-Party Computation in a Constant Number of Rounds.*** (FOCS 03)
  R. Pass and A. Rosen. pdf
- ***On Deniabililty in the Common Reference String and Random Oracle Models.*** (CRYPTO 03)
  R. Pass.
  See Part II in *Alternative Variants of Zero-Knowledge Proofs* for a longer version.
- ***Simulation in Quasi-Polynomial Time and Its Application to Protocol Composition.*** (EUROCRYPT 03)
  R. Pass.
  See Part I in *Alternative Variants of Zero-Knowledge Proofs* for a longer version.

This material is based upon work supported by the National Science Foundation, AFOSR, U.S. Department of Homeland Security, BSF,
Sloan Foundation, IBM and Microsoft. Any opinions, findings, and conclusions or recommendations expressed in this publications are those of
the author(s) and do not necessarily reflect the views of the NSF, AFOSR, DHS, BSF, Sloan Foundation, IBM or Microsoft.