Research Statement

Dakshita Khurana
dakshita@cs.ucla.edu

Introduction

I am interested in Cryptography, and more broadly, Theoretical Computer Science. Cryptography deals with enabling collaboration among mutually distrusting participants. Such collaboration has become even more imperative because of the recent proliferation of computational devices that must jointly compute on large amounts of distributed private data. This is enabled by one of the core areas in cryptography: secure computation.

Secure computation, first introduced three decades ago [Yao86, GMW87, BGW88], allows potentially adversarial participants to compute jointly on private data, while learning nothing beyond the prescribed output of the computation. This has wide applications, especially to privacy-preserving computation over sensitive medical and genomic data, military research and auctions. As an interesting illustrative example, consider satellites launched by two different countires, that would like to prevent a collision between their satellites while keeping their own trajectories private. Secure computation provides a solution to this problem.

The last thirty years have seen significant research on secure computation. The main goal of this research has been the design of protocols and proof techniques that provide strong security guarantees while requiring minimal overhead. Despite this research, there are many scenarios where existing secure computation protocols do not apply. Underlying this failure is a paucity of techniques for achieving security in various situations. I mainly work on devising new techniques and protocols for such scenarios.

Research Experience

My research so far has been focused in three broad areas, which I highlight below.

1. **Minimizing Interaction in Secure Computation.**
   So far, protocols with provable security have required introducing additional interaction where participants perform various checks at different points. This means that participants they must go back-and-forth multiple times in their communication. However, such increased interaction introduces additional delays due to latency or unavailability of participants.

   A major focus of my research is on designing secure protocols that entail *minimal interaction*, do not require any central trust or setup assumptions, and many a times require each participant to only send only a single message. Most of these protocols overcome known barriers against the round complexity of these tasks. These protocols can be broadly divided into two categories:

   Non-Malleability: Preventing Man-in-the-Middle Attacks.
   An important requirement in multi-party secure computation (MPC), is security against man-in-the-middle attacks. Here, an adversary may intercept data from other parties and try to modify it arbitrarily, before passing it off as its own. In MPC, such security guarantees are required to ensure that the inputs of malicious parties are independent of honest party inputs. The basic cryptographic primitive that achieves such security guarantees is called a non-malleable commitment.

Apart from being an essential ingredient of secure MPC protocols, non-malleable commitments have several other applications. For example, in online sealed-bid auctions, it is imperative to ensure that a man-in-the-middle attacker cannot generate his own bid as a function of the bids of other players.

Obtaining non-malleable commitments without setup and in as few rounds as possible, has remained a very interesting open problem in cryptography for the past 25 years. The number of rounds required for non-malleable commitments, have a direct impact on the round complexity of secure MPC. Ideally, we would like to have non-interactive non-malleable commitments without the need to make central setup assumptions.

(a) Some of my recent work [GKS16] (FOCS 2016), constructs non-malleable commitments in two rounds. This work overcomes a known barrier against two-round constructions of non-malleable commitments, by satisfying a slightly weaker, yet, standard notion of security. Furthermore, this protocol requires only one participant to send two consecutive messages. This protocol has implications to *non-malleable codes*, an exciting new area of research at the helm of theoretical computer science and cryptography.

(b) Even more recently, in [KS17] (FOCS 2017) we constructed two-message non-malleable commitments satisfying the standard strong notion of security, where each participant sends a single message. These were previously believed to be impossible to construct, however our work demonstrates that previous barriers incorrectly placed implicit restrictions on the power of the security proof. Our results have several implications to secure computation that have been explored in follow-up work [ACJ17, BGJ$^+$17].

(c) In another work [GJK15], we study non-malleability in context of multi-prover interactive proofs, which have numerous applications in cryptography and beyond. We give the first constructions of non-malleable multi-prover interactive proofs. An additional advantage of our protocols are that they are among the extremely few known non-malleable protocols to achieve unconditional security.

Zero-Knowledge Proof Systems.

The notion of interactive proofs has been fundamental in theoretical computer science. While the most basic notion is not concerned with privacy and only offers correctness guarantees, most cryptographic applications require it to be supplemented with a privacy guarantee for the prover. The typical guarantee is that of zero-knowledge, which intuitively means that the proof of any statement does not reveal any information beyond the validity of the statement itself.

Nearly all MPC protocols with security against malicious adversaries require a mechanism to enforce correct behaviour of participants, while preserving privacy. This is typically accomplished via the use of zero-knowledge proofs and arguments.

Since their introduction three decades ago, an extensive line of research has been dedicated to studying the round complexity of zero-knowledge arguments. In recent work [JKKR17] (CRYPTO 2017) and followups done during internships at Microsoft Research New England, we focus on the setting where only two messages of communication are available to the prover and the verifier. While previous protocols only provided extremely feeble privacy guarantees when limited to just two messages, we develop new protocols and techniques that have much stronger guarantees. Very roughly, among other results, in [JKKR17] we construct a two-message protocol which satisfies a distributional variant of the zero-knowledge property for statements that are chosen by the prover from a cryptographic distribution, in the second round of the protocol. Interestingly, we show that this already suffices for many applications of zero-knowledge arguments in cryptographic settings.

We explore applications of the resulting proof systems to several round-optimal protocols, including the following:

(a) In the same work [JKKR17], we show how to use these arguments to give the first constructions of three message commitments that are simultaneously arguments of knowledge, via polynomial hardness assumptions. We also show that the same techniques yield optimal variants of secure computation.

(b) In [Khu17] (TCC 2017) we use arguments constructed in [JKKR17] to obtain the first non-malleable commitments from polynomial hardness assumptions, in three messages.

(c) In [KS17], we show that the privacy guarantees provided by the protocols in [JKKR17] suffice for obtaining two-message non-malleable commitments. We also show how to augment the privacy properties to achieve *simulation soundness*, which guarantees that a prover cannot cheat even when he can observe fake proofs of other related statements.

(d) Finally, in [BGJ+17] (TCC 2017), we show how to use the augmented protocols to obtain optimal secure computation in a setting where multiple such protocols could be executed simultaneously.

2. **Information-theoretic Secure Computation from Imperfect Setup Assumptions, that Better Approximate the Real World.**
   Secure computation can also be performed with information-theoretic or unconditional security (i.e. with provable security even in a world where P = NP) if parties are given access to certain trusted resources. An orthogonal line of research has been exploring what kinds of resources are necessary and/or sufficient to compute any functionality, with information-theoretic security guarantees.

   - My work [KMS16, BKOV17] (Eurocrypt 2016 and 2017 respectively) shows how ”leaky” versions of resources such as leaky binary symmetric channels [KMS16] or leaky physically unclonable functions [BKOV17], can be used in place of ideal setups, in order to facilitate information-theoretic secure computation. These ”leaky” resources provide a far more accurate modeling of real-world scenarios, where it is often impossible to fix the exact characteristic of a channel.
   - Some of my other work [KKM+16] (Eurocrypt 2016) considers the question of transforming a uni-directional resource between two parties, into one that is useful in both directions – this could be a protocol, a physical phenomenon, etc. This question, in its most basic form, was posed 25 years ago by Crepeau and Santha. In [KKM+16], we show how to transform a secure implementation of some functionality in one direction into an unconditionally secure implementation of the same functionality in the reverse direction.
   - In [AIKP15] (ICALP 2015), we study the complexity class defined by functions that admit information-theoretic randomized encodings, a key primitive that enables secure computation. We prove general separations between this and various other complexity classes.
   - Finally, in [GKM+16, KMS14] (ICALP 2016, Asiacrypt 2014), we explore connections between differential privacy and secure computation. In [GKM+16], we show how to obtain unconditional secure computation from (distributed) differentially private protocols that satisfy certain optimality constraints on the accuracy versus privacy ratio.

3. **Indistinguishability Obfuscation and Functional Encryption.**
   A program obfuscator is a (randomized) compiler that takes a computer program (represented, e.g., as a binary circuit) and outputs a computationally equivalent program, but

one that is harder to reverse engineer. Recent advances in cryptographic study, starting with [GGH$^+$13] give candidate constructions of *indistinguishability obfuscators* (iO) [BGI$^+$01, GGH$^+$13], that have proven to be extremely useful. Starting with the works of [GGH$^+$13, SW14], it has been shown that iO would have far-reaching applications, significantly expanding the scope of problems to which cryptography can be applied. In the following papers, we exhibit some such applications:

- In [HJK$^+$16] (Asiacrypt 2016), we show how to combine indistinguishability obfuscation with truly random functions, to obtain constructions of *distributional samplers*. Unlike (uniform) random functions, distributional samplers can be used to obtain secure samples from any given distribution.
- In [KRS15] (Asiacrypt 2015), we showed how indistinguishability obfuscation can be used to give the first constructions of multi-party non-interactive key exchange, improving a prior work [BZ14] that achieved key exchange for only an a-priori bounded number of participants. Naturally, our techniques also showed how to make the size of parameters for NIKE independent of the number of participants.
- Functional encryption is a special kind of encryption scheme that allows creating functional secret keys, such that a secret key for a function f can be used to evaluate a ciphertext encrypting a value x, to yield $f(x)$ and no additional information about x. General constructions of functional encryption were obtained recently using indistinguishability obfuscation (iO) in [GGH$^+$13] and followup work. In a very recent work [BKSW17], we study the classes of existing popular encryption schemes that can be generically upgraded to achieve functional encryption, assuming the existence of iO.
- Finally, in a recent work [ABKS17], we generalize the class of cryptographic pseudorandom generators that can be used to obtain constructions of indistinguishability obfuscation based on tri-linear maps.

Future Directions

I am excited to continue pushing boundaries of what can be achieved, in secure computation and beyond. I would like to work on further expanding and deepening our understanding of cryptography in the context of secure computation, as well as working on new problems in related fields such as verifiable outsourcing, non-malleable codes and learning theory.

A lot of the theory developed for secure computation has also found its way to more practical security applications, including cloud computing and verifiable outsourcing. Succinct zero-knowledge arguments are now being used in actual cryptocurrency [MGGR13]. I am also excited about potential future collaborations that would help further bridge the gap between theory and practice. In particular, I am interested in exploring how blockchain technology can be used to enable more efficient cryptographic protocol design, and how ideas from protocol design can help obtain better blockchains.

References

[ABKS17] Prabhanjan Ananth, Zvika Brakerski, Dakshita Khurana, and Amit Sahai. Constructing obfuscation using preprocessing-friendly pseudo-independence generators. Manuscript, 2017.

[ACJ17] Prabhanjan Ananth, Arka Rai Choudhuri, and Abhishek Jain. A new approach to round-optimal secure multiparty computation. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 468–499. Springer, 2017.

[AIKP15] Shweta Agrawal, Yuval Ishai, Dakshita Khurana, and Anat Paskin-Cherniavsky. Statistical randomized encodings: A complexity theoretic view. In Magnús M. Halldórsson, Kazuo Iwama, Naoki Kobayashi, and Bettina Speckmann, editors, *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*, volume 9134 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2015.

[BGI$^+$01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2001.

[BGJ$^+$17] Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Dakshita Khurana, and Amit Sahai. Round optimal concurrent MPC via strong simulation. To Appear in TCC, 2017.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10. ACM, 1988.

[BKOV17] Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, and Ivan Visconti. Unconditional uc-secure computation with (stronger-malicious) pufs. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 382–411, 2017.

[BKSW17] Saikrishna Badrinarayanan, Dakshita Khurana, Amit Sahai, and Brent Waters. Upgrading to functional encryption. Manuscript, 2017.

[BZ14] Dan Boneh and Mark Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 480–499. Springer, 2014.

[FC16] Marc Fischlin and Jean-Sébastien Coron, editors. *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*. Springer, 2016.

[GGH$^+$13] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 40–49. IEEE Computer Society, 2013.

[GJK15] Vipul Goyal, Aayush Jain, and Dakshita Khurana. Witness signatures and non-malleable multi-prover zero-knowledge proofs. *IACR Cryptology ePrint Archive*, 2015:1095, 2015.

[GKM$^+$16] Vipul Goyal, Dakshita Khurana, Ilya Mironov, Omkant Pandey, and Amit Sahai. Do distributed differentially-private protocols require oblivious transfer? In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, volume 55 of *LIPIcs*, pages 29:1–29:15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[GKS16] Vipul Goyal, Dakshita Khurana, and Amit Sahai. Breaking the three round barrier for non-malleable commitments. In Irit Dinur, editor, *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 21–30. IEEE Computer Society, 2016.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 218–229. ACM, 1987.

[HJK$^+$16] Dennis Hofheinz, Tibor Jager, Dakshita Khurana, Amit Sahai, Brent Waters, and Mark Zhandry. How to generate and use universal samplers. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 715–744, 2016.

[JKKR17] Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Ron Rothblum. Distinguisher-dependent simulation in two rounds and its applications. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 158–189. Springer, 2017.

[Khu17] Dakshita Khurana. Round optimal concurrent non-malleability from polynomial hardness. To Appear in TCC, 2017.

[KKM$^+$16] Dakshita Khurana, Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai. All complete functionalities are reversible. In Fischlin and Coron [FC16], pages 213–242.

[KMS14] Dakshita Khurana, Hemanta K. Maji, and Amit Sahai. Black-box separations for differentially private protocols. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 386–405. Springer, 2014.

[KMS16] Dakshita Khurana, Hemanta K. Maji, and Amit Sahai. Secure computation from elastic noisy channels. In Fischlin and Coron [FC16], pages 184–212.

[KRS15] Dakshita Khurana, Vanishree Rao, and Amit Sahai. Multi-party key exchange for unbounded parties from indistinguishability obfuscation. In Tetsu Iwata and Jung Hee

Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 52–75. Springer, 2015.

[KS17] Dakshita Khurana and Amit Sahai. How to achieve non-malleability in one or two rounds. To Appear in FOCS, 2017.

[MGGR13] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013*, pages 397–411. IEEE Computer Society, 2013.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In David B. Shmoys, editor, *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 475–484. ACM, 2014.

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*. IEEE Computer Society, 1986.