Research Statement

Mohammad Mahmoody

June 2018

My research is focused on **foundations of cryptography**, which is the science of designing *provably* secure protocols based computationally intractable problems. My specialization is in identifying the **limitations of computational assumptions** in cryptography. Namely, a main theme in my research is to identify barriers against basing cryptographic protocols on well-studied computational assumptions. I have also studied **trade-offs** that emerge between efficiency of cryptographic protocols and assumptions behind their designs. My research has helped develop the field of **separations** (i.e., barriers) in cryptography, with a focus on more modern primitives such as program obfuscation and functional encryption. The second theme in my research investigates the power and limitations of **physical assumptions** in cryptography, where e.g., we aim to avoid computational assumptions by relying on tamper-proof properties of hardware. In this line of work, I have studied the possibility of basing cryptographic tasks on stateless tamper-proof hardware and related mathematical tools such as zero-knowledge (and interactive) probabilistically checkable proofs (PCPs). Finally, a more recent direction in work investigates **tampering attacks in cryptography and learning** systems. This line of work studies vulnerabilities that are could be exploited by adversaries who tamper with the randomness of algorithms in cryptography and other settings. When attacking a learner, an adversary might tamper with the training data of the learner (i.e., do a poisoning attack) or the test example (i.e., do an evasion attack). My research investigates **provable bounds** in both of these settings.

**Research group and support.** My research group currently consists of three PhD students and two post-doctoral researchers. One PhD student and two Masters students have previously graduated from my group. I support my group’s research through NSF CAREER award (on cryptographic separations), a subcontract from UC Berkeley (on extending non-black-box separations), two UVa’s SEAS Innovation Award (on adversarial learning and adversarial fairness) and external fellowships.

**Publishing venues and the alphabetical order of authors.** My works in cryptography appear in top conferences dedicated for foundations of cryptography such as Crypto, TCC, and Eurocrypt. As it is the tradition in Theoretical Computer Science, almost all of my papers list authors in the alphabetical order.

**Computational Assumptions in Cryptography**

Modern cryptography has given rise to protocols whose security is based on well-defined and well-studied mathematical puzzles (e.g., factoring large integers) that are believed to be computationally hard to solve. Unfortunately, however, we are yet far from *proving* such hardness results in mathematics. Yet, proving the security of almost all cryptographic protocols requires resolving the notorious $P \neq NP$ question. As a result, cryptographic security heavily relies on computational hardness **assumptions**. A core theme in my
research aims at identifying the power of computational intractability assumptions in cryptography. Over the years, my research has taken major steps toward understanding the limitations of computational assumptions in cryptography through a theory of cryptographic separations.

**Private-key encryption from NP-hardness.** Since P ≠ NP is a necessary requirement for the security of almost all cryptographic tasks, a holy grail in cryptography is to base security of protocols solely on the assumption that P ≠ NP. Together with Haitner and Xiao [HMX10, MX10], I came up with mathematical explanations as to why so far, despite tremendous effort by researchers, designing encryption schemes with NP-hard security has remained elusive. In particular, we show that in order to achieve NP-hard cryptography, we need to first resolve long-standing open questions in computational complexity about the existence of program-checkers for Boolean satisfiability, or alternatively, we have to construct interactive proofs with “low complexity” provers in forms that are not known to exist yet.

**Public-key cryptography from private-key primitives.** Secure private-key cryptography can be based on secure hash functions, while public-key cryptography is predictably more challenging and is usually based on structured problems from mathematics. Such problems, however, have also more potential for enabling attacks that exploit this very structure. Therefore, one of the most fundamental questions in cryptography is whether we can base public-key encryption on private-key primitives such as secure hash functions. In 1989, Impagliazzo and Rudich [IR89] showed that a large class of techniques, called black-box, are incapable of achieving this goal. However, black-box techniques are only part of the toolkit used by cryptographers, so extending their result to non-black-box techniques, or coming up with a non-black-box protocol has remained as one of the most important problems in foundations of cryptography.

- In a recent work with Garg, our joint postdoc Hajiabadi and my PhD student Mohammed [GHMM18] we show that even a popular and powerful non-black-box technique in cryptography based on garbled circuits [Yao86] is not capable of basing public-key encryption on private key encryption. We proved our result in a model that was recently developed by us [GMM17a] expanding previous models of [BKSY11, AS16]. This model includes a large class of natural non-black-box constructions beyond the fully-black-box framework of Reiongold et al. [RTV04]—see below for more explanations.

- While a PhD student, together with Barak [BM09] we studied whether one can base relaxed forms of public-key encryption (with only a polynomial security) on secret-key encryption. We proved optimal bounds for the exact achievable security of such relaxed public-key encryption schemes based on ideal hash functions. Our security bound for this problem showed that a seminal work of Merkle [Mer74] was indeed optimal, and this resolved a long standing open question of [IR89].

**Separations and trade-offs for secure multi-party computation.** In a body of works, I studied the complexity of the assumptions that are necessary for secure computation protocols. In such a protocol, mutually distrustful entities engage to compute a joint function on their local private inputs.

- In two works with Maji and Prabhakaran [MMP14a, MMP14b] we characterized the black-box power of private-key as well as public-key cryptography in secure computation. We showed that random oracles (or even strong forms of public-key encryption) cannot help us in weakening the assumptions behind secure computation systems, at least as long as the construction is black-box.
In a recent work with Garg, Masny, and Meckler [GMMM18], I studied the possibility of very efficient oblivious transfer (OT) extension protocols. OT is the building block of secure computation [Kil88, IPS08], but since it is a costly operation, researchers have suggested efficient ways [IKNP03] to extend a few base OT operations into many constructed OT operations while only using cheap symmetric-key cryptographic operations that can be obtained from a random oracle. The solution of [IKNP03], however, adds one more round of communication between the parties. It was open whether such extra round of communication is necessary, till we proved in [GMMM18] that such cost is indeed inherent.

**Complexity of powerful encryption primitives.** During the twenty first century, cryptography has gone through a revolution of exploring the feasibility of highly structured tasks at the cost of relying on newly introduced and less studied assumptions. One such success story led to development of strong encryption primitives such as identity based encryption [Sha84, BF03], predicate encryption [KSW08] and functional encryption [BSW10, O’N10]. Understanding the computational assumptions necessary for achieving any of these powerful primitives is of great importance. Together with Goyal, Kumar and Lokam [GKLM12], and my PhD student Mohammed [MM15], we took major steps toward answering the above question by studying the power of identity-based encryption (IBE). In an IBE scheme, the encryptor does not need to know the public-key of the specific person that it is sending its message to, and only knowing a single master public key is sufficient. We proved these limitation results for IBE by demonstrating cryptographic primitives that cannot be obtained from IBE in a black-box way.

**Complexity of assumptions for program obfuscation.** Program obfuscation was first formally studied in the theory community by Barak et.al [BGI+12] where they showed that very strong forms of obfuscation are impossible, but it took till the work of Garg et al. [GGH+13] where the first useful form of obfuscation, called indistinguishability obfuscation (IO), was proposed based on the existence of multi-linear maps. In a series of works [MMN+16b, MMN16a, GMM17a, GMM17b] all co-authored with my PhD student Ameer Mohammed (whose thesis was on this subject) as well as Garg, Pass, shelat, and my Masters student Nematihaji, we proved strong lower-bounds on standard assumptions that can be used to construct IO. These were the first, and so far the only such results proved for assumptions behind IO.

**New framework for non-black-box separations.** Together with Garg and my PhD student Mohammed [GMM17a], we proved strong non-black-box impossibility results for IO from powerful assumptions such as predicate encryption. A major contribution of this work was to introduce a new model for framing a broad class of non-black-box techniques as “monolithic” subroutine calls. This model is non-black-box under the original framework developed by Reingold et al [RTV04] and the subsequent extensions of [BKSY11, AS16], yet it includes natural techniques widely used in cryptography. This new model sets the stage for a new class of separations in cryptography that are more meaningful with respect to the known techniques.

**Tampering Attacks in Cryptography and Learning**

In the fields of algorithm design and cryptography, we typically assume that honest parties have access to uniform and independent randomness, and indeed many tasks (e.g., secure multi-party encryption) are otherwise impossible [DOPS04]. In particular, “standard” security proofs no longer hold if adversaries can tamper with the randomness of honest parties. Such attacks also emerge in the area of adversarial machine learning where we also deal with tampering attacks of various forms.
**Tampering attacks in Cryptography.** Together with Austrin, Chung, Pass and Karn [ACM+14], we studied the possibility of achieving security in cryptography if the randomness of the parties might be under attack by **efficient** viruses who can read everything but can only change the randomness of the system in a limited way. Such viruses could be generated by “traditional” powerful adversaries who do not have direct access to the honest parties’ devices. We obtained a comprehensive characterization for the tasks that are possible to achieve in this setting.

**Provable bounds in adversarial machine learning.** In works with my PhD student Saeed Mahloujifar [MM17, MDM18a] we studied tools and techniques for tampering attacks that are powerful enough to be applied to domains **outside** cryptography, and in particular to the domain of **adversarial machine learning**. In particular, we showed [MM17] how to increase the error in a learning algorithm in polynomial time by tampering only with $p$ fraction of the training data. As opposed to many heuristic attacks in this area, our work led to **provable** bounds (of attack success) by efficient attackers. In a follow-up work [MDM18b], we study how similar ideas can also be applied to **evasion** attacks where the goal of the adversary is to find adversarial examples that are close to honestly generated ones, but are misclassified by the trained model.

**Tamper-proof hardware and unconditional cryptography.** On the other hand, assuming **strong** forms of tamper proof assumptions about hardware lead to positive results that are otherwise impossible [Kat07]. A candidate approach for achieving **unconditional** security without relying on computational assumptions is to use alternative **physical** models of interaction [DOPS04]. In a sequence of works with Goyal, Ishai, Sahai and Xiao [GIMS10, IMS12, MX13], I showed how to build cryptography on **physical** assumptions by using physical models that obtain the needed “intractability” through the tamper-proof nature of the hardware rather than computational hardness against efficient software. In particular, we explored the power and limitations of potential **resettable** “tamper-proof” hardware (where adversary can reset the hardware by cutting its power) and identified cryptographic tasks that are achievable in this model.

**Future Plans**

**Power and limitations of non-black-box constructions.** My future goal is to continue studying the limitations of computational assumptions and techniques in foundations of cryptography. Towards this goal, I plan to expand my research group and collaborate with new colleagues in other schools. On the other hand, when it comes to **positive** results, I also plan to study the **power** of non-black-box techniques such a garbling schemes in cryptography. Particularly,

**Adversarial agents, beyond attacking learners.** My second major plan for the future is to expand my research in provable bounds in adversarial machine learning. Leveraging on our initial results [MM17, MDM18a, MDM18b], I plan to study **provable** methods in achieving robustness of classifiers and learning systems. Furthermore, I plan to study how strategic agents (i.e., adversaries, as we call them in cryptography) can affect decision making processes in which utility measures other than the optimality of the choices are under attack. In particular, I plan to study the power and limitation of attackers who attack the **fairness** of sequential decision making algorithms. Due to the ever increasing role of automatic decision making systems, understanding the answer to this question is more important than ever.
References


[HMX10] Iftach Haitner, Mohammad Mahmoody, and David Xiao. A new sampling protocol and applications to basing cryptographic primitives on the hardness of NP. In IEEE Conference on Computational Complexity, 2010. 2


[MX10] Mohammad Mahmoody and David Xiao. On the power of randomized reductions and the checkability of SAT. In IEEE Conf. on Computational Complexity, 2010. 2

[MX13] Mohammad Mahmoody and David Xiao. Languages with efficient zero-knowledge PCPs are in SZK. Theory of Cryptography Conference (TCC), 2013. 4


