A Study on Cryptographic Protocols: Achieving Strong Security for Zero-knowledge Proofs and Secure Computation

Susumu Kiyoshima

Abstract

This thesis studies *zero-knowledge proofs* and *secure computation*, two of the most fundamental protocols in cryptography. Zero-knowledge proofs are counter-intuitive protocols that allow provers to convince verifiers of the correctness of mathematical statements without revealing any additional knowledge about the statements, and secure computation protocols are powerful protocols that enable mutually distrustful parties to jointly compute any public functions on their secret inputs without compromising the correctness of the outputs and the privacy of the inputs. Zero-knowledge proofs are fundamental in cryptography because they are used as key building blocks in numerous other protocols, and secure computation protocols are fundamental in cryptography because their powerful generality allows us to obtain strong feasibility results about cryptographic protocols.

The focus of this thesis is to obtain new constructions that (provably) satisfy strong security notions such as *concurrent security* and *leakage resilience*. Concurrent security guarantees that a protocol remains secure even when it is executed multiple times in an arbitrary schedule, and leakage resilience guarantees that a protocol remains secure even when adversaries obtain leakages of honest parties' secret internal memories. Concurrent security is motivated by the use of cryptographic protocols on large asynchronous networks like the Internet, and leakage resilience is motivated by the development of various "side-channel" attacks that obtain partial information of honest parties' secret memories via physical measurements on their implementations.

This thesis gives four theoretical results about the problem of achieving strong security at as low cost as possible, where the cost is defined in terms of (asymptotic) efficiency and hardness assumptions. At a high level, these four results can be viewed as a step to solve a fundamental problem about concurrent security and leakage resilience, that is, the problem of constructing secure computation protocols that satisfy concurrent security and leakage resilience with optimal efficiency under minimum assumptions. Specifically, these four results concern natural simplified versions of this fundamental problem (where the simplification is to focus on zero-knowledge protocols rather than secure computation and/or to focus on only either concurrent security or leakage resilience) and show that concurrent security and leakage resilience can be achieved at much lower cost than previously known. Concretely, the results of this thesis are the following.

The first result is about *statistical concurrent non-malleable zero-knowledge arguments*, which are zero-knowledge protocols that currently satisfy the strongest notion of concurrent security in the plain model (i.e., in the model where no trusted third party is available). This thesis shows, in essence, that statistical concurrent non-malleable zero-knowledge protocols can be obtained at no additional cost in terms of hardness assumptions. In other words, this thesis constructs a statistical concurrent non-malleable zero-knowledge argument that is proven secure under the same assumption as the best constructions of (standard) zero-knowledge protocols.

The second result is about *leakage-resilient zero-knowledge arguments*, which are zero-knowledge protocols that satisfy leakage resilience. While the existing constructions are either inefficient in terms of round complexity or secure only under a strong hardness assumption, the construction in this thesis has optimal asymptotic efficiency in terms of round complexity and is secure under a weak hardness assumption.

The third result is about *non-black-box concurrent zero-knowledge arguments*, which are concurrently secure zero-knowledge protocols whose security is proven via a specific technique called *non-black-box simulation*. The motivation behind this result is the long-standing open question of constructing constant-round concurrent zero-knowledge protocols (i.e., concurrent zero-knowledge protocols that have optimal asymptotic efficiency in terms of round complexity), which is known to be solvable only via non-black-box simulation. This thesis gives a construction that has more than constant number of rounds just like the existing construction, but it has an arguably simpler proof of security and therefore can be a useful starting point of future research.

The last result is about *composable secure multi-party computation protocols*, which are secure computation protocols that satisfy concurrent security in a strong sense. The construction in this thesis is proven secure under a well-studied security definition called *angel-based UC security*. Compared with the existing constructions, which are inefficient either because of "non-black-box" use of underlying cryptographic primitives or because of large round complexity, the construction in this thesis is efficient thanks to its "black-box" use of the underlying cryptographic primitives and small round complexity.