Università degli Studi di Salerno

Dottorato di Ricerca in Informatica e Ingegneria dell'Informazione
Ciclo 30 - a.a. 2016/2017

Tesi di Dottorato / Ph.D. Thesis

Round and Computational Efficiency of Two-Party Protocols

Abstract

Supervisor
Prof. Giuseppe PERSIANO

Candidate
Michele CIAMPI

Ph.D. Program Director
Prof. Pasquale CHIACCHIO

Dipartimento di Ingegneria dell'Informazione
ed Elettrica e Matematica Applicata
Dipartimento di Informatica

Abstract

A cryptographic protocol is defined by the behaviour of the involved parties and the messages that those parties send to each other. Beside the functionality and the security that a cryptographic protocol provides, it is also important that the protocol is *efficient*. In this thesis we focus on the efficiency parameters of a cryptographic protocol related to the computational and round complexity. That is, we are interested in the computational cost that the parties involved in the protocol have to pay and how many interactions between the parties are required to securely implement the functionality which we are interested in. Another important aspect of a cryptographic protocol is related to the computational assumptions required to prove that the protocol is secure. The aim of this thesis is to improve the state of the art with respect to some cryptographic functionalities where two parties are involved, by providing new techniques to construct more efficient cryptographic protocols whose security can be proven by relying on better cryptographic assumptions.

The thesis is divided in three parts. In the first part we consider *Secure Two-Party Computation* (2PC), a cryptographic technique that allows to compute a functionality in a secure way. More precisely, there are two parties, Alice and Bob, willing to compute the output of a function f given x and y as input. The values x and y represent the inputs of Alice and Bob respectively. Moreover, each party wants to keep the input secret while allowing the other party to correctly compute $f(x, y)$. As a first result, we show the first secure 2PC protocol with black box simulation, secure under standard and generic assumption, with optimal round complexity in the simultaneous message exchange model. In the simultaneous message exchange model both parties can send a message in each round; in the rest of this thesis we assume the in each round only one party can send a message.

We advance the state of the art in secure 2PC also in a relaxed setting. More precisely, in this setting a malicious party that attacks the protocol to understand the secret input of the honest party, is forced to follow the protocol description. Moreover, we consider the case in which the parties want to compute in a secure way the *Set-Membership* functionality. Such a functionality allows to check whether an element belongs to a set or not. The proposed protocol improves the state of the art both in terms of performance and generality. In the second part of the thesis we show the first 4-round *concurrent non-malleable commitment* under one-way functions. A commitment scheme allows the sender to send an encrypted message, called commitment, in such a way that the message inside the commitment cannot be opened until that an *opening* information is provided by the sender. Moreover, there is a unique way in which the commitment can be open. In this thesis we consider the case in which the sender sends the commitment (e.g. trough a computer network) that can be eavesdropped by an adversary. In this setting the adversary can catch the commitment C and modify it thus obtaining a new commitment C' that contains a message related to the content of C. A non-malleable commitment scheme prevents such attack, and our scheme can be proved secure even in the case that the adversary can eavesdrop multiple commitments and in turn, compute and send multiple commitments.

The last part of the thesis concerns *proof systems*. Let us consider an $\mathcal{NP}$-language, like

the language of graph Hamiltonicity. A proof system allows an entity called *prover* to prove that a certain graph (instance) contains a Hamiltonian cycle (witness) to another entity called *verifier*. A proof system can be easily instantiated in one round by letting the prover to send the cycle to the verifier. What we actually want though, is a protocol in which the prover is able to convince the verifier that a certain graph belongs to the language of graph Hamiltonicity, but in such a way that no information about the cycle is leaked to the verifier. This kind of proof systems are called *Zero Knowledge*. In this thesis we show a non-interactive Zero-Knowledge proof system, under the assumption that both prover and verifier have access to some honestly generated *common reference string* (CRS). The provided construction improves the state of the art both in terms of efficiency and generality. We consider also the scenario in which prover and verifier do not have access to some honestly generated information and study the notion of *Witness Indistinguishability*. This notion considers instances that admit more than one witness, e.g. graphs that admit two distinct Hamiltonian cycle (as for the notion of Zero Knowledge, the notion of Witness Indistinguishability makes sense for all the languages in $\mathcal{NP}$, but for ease of exposition we keep focusing our attention of the language of graph Hamiltonicity). The security notion of Witness-Indistinguishability ensures that a verifier, upon receiving a proof from a prover, is not able to figure out which one of the two Hamiltonian cycles has been used by the prover to compute the proof. Even though the notion of Witness Indistinguishability is weaker than the notion of Zero Knowledge, Witness Indistinguishability is widely used in many cryptographic applications. Moreover, given that a Witness-Indistinguishable protocol can be constructed using just three rounds of communication compared to the four rounds required to obtain Zero Knowledge (with black-box simulation), the use of Zero-Knowledge as a building block to construct a protocol with an optimal number of rounds is sometimes prohibitive. Always in order to provide a good building block to construct more complicated cryptographic protocols with a nice round complexity, a useful property is the so called *Delayed-Input* property. This property allows the prover to compute all but the last round of the protocol without knowing the instance nor the witness. Also, the Delayed-Input property allows the verifier to interact with the prover without knowing the instance at all (i.e. the verifier needs the instance just to decide whether to accept or not the proof received by the prover). In this thesis we provide the first efficient Delayed-Input Witness-Indistinguishable proof system that consists of just three round of communication.