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

Delayed-Input and Non-Malleable Cryptographic Protocols

Luisa Siniscalchi

Supervisor: **Prof. Ivan Visconti**

PhD Program Director: **Prof. Pasquale CHIACCHIO**

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

Abstract

A major goal in the design of cryptographic protocols is to reduce the number of communication rounds. Since a cryptographic protocol usually consists of a composition and interplay of some subprotocols and cryptographic primitives, the natural approach to save rounds consists in playing all subprotocols in parallel. Unfortunately this approach often fails since a subprotocol in order to start could require as input the output of another subprotocol. In such cases the two subprotocols must be played sequentially therefore penalizing the overall round complexity.

In this thesis we provide *delayed-input* cryptographic protocols that can be played in parallel with other subprotocols even in the above scenario where the output of a subprotocol is required as input by the other subprotocol. We show the actual impact of our *delayed-input* cryptographic protocols by improving the round efficiency of various applications.

More precisely, this thesis includes the following results:

1. The first OR-composition technique for Σ-protocols that requires only one statement to be fixed when the protocol starts, while the other statement can be defined in the last round. Our OR-composition technique does not require computational assumptions.

2. The first efficient 4-round resettable witness indistinguishable argument of knowledge. We make use of subexponential hardness assumptions and of our OR-composition technique. Previous constructions required 5 rounds.

3. The first 4-round delayed-input (i.e., the theorem and the witness can be used just to compute the last round of the protocol) one-many (also many-many synchronous) non-malleable zero-knowledge (NMZK) argument of knowledge Π_{NMZK} from one-way functions.

4. The first 4-round (round optimal for black-box simulation) multi-party coin tossing protocol from one-to-one one-way functions. This construction makes use of Π_{NMZK}. Previous constructions required much strong computational assumptions.

5. The first 3-round concurrent non-malleable commitment scheme from subexponentially hard one-way permutations. The protocol is also delayed input and public coin.