

Cryptographic Applications of Pseudo-Telepathy Games

Ivan Fialík

Laboratory of Quantum Information Processing and Cryptography,
Faculty of Informatics MU

MEMICS 2009

November 14, 2009

- 1 Introduction
- 2 Pseudo-Telepathy Games
- 3 User Identification
- 4 Identification Scheme

- Quantum information processing allows us to solve tasks that we cannot solve in the classical world.
- Can it be used also to solve some distributed problems without any form of direct communication among the parties?
- The answer is negative if the parties compute a value of some function on their inputs and the whole result of the computation must become known to at least one party.
- The answer is positive if each party has its own input, computes its own output and we are interested only in correlations between the inputs and the outputs.

Pseudo-Telepathy Games

Two party games

- A two party game \mathcal{G} is a sextuple

$$\mathcal{G} = (X, Y, A, B, P, W)$$

where X, Y are **input sets**, A, B are **output sets**, P is a subset of $X \times Y$ known as a **promise** and $W \subseteq X \times Y \times A \times B$ is a **winning condition**.

Pseudo-Telepathy Games

Two party games II

- Before the game begins, Alice and Bob are allowed to discuss strategy and exchange any amount of classical information, including values of random variables.
- Alice and Bob may also share unlimited amount of quantum entanglement.
- Afterwards, Alice and Bob are separated from each other and they are not allowed to communicate any more till the end of the game.

Pseudo-Telepathy Games

Two party games III

- Alice and Bob are given inputs $x \in X$ and $y \in Y$, respectively.
- Their task is to produce $a \in A$ and $b \in B$, respectively.
- The pairs (x, y) and (a, b) are called a **question** and an **answer**, respectively.
- Alice and Bob **win the game** if either $(x, y) \notin P$ or $(x, y, a, b) \in W$.
- A **strategy** of Alice and Bob **is winning** if it always allows them to win.

Pseudo-Telepathy Games

Definition (Brassard, Cleve, Tapp, 1999)

- We say that a two-party game is **pseudo-telepathic** if there is no classical winning strategy, but there is a winning strategy, provided Alice and Bob share quantum entanglement.

Pseudo-Telepathy Games

A general quantum strategy

- Alice and Bob share an entangled state $|\psi\rangle$.
- After they have been given their inputs $x \in X$ and $y \in Y$, the players apply on their parts of $|\psi\rangle$ unitary transformations U_x and U_y , respectively.
- Finally, the players perform measurements M_x and M_y on their parts of $|\psi\rangle$ which give them their outputs $a \in A$ and $b \in B$, respectively.

User Identification

Introduction

- An identification scheme is an interactive protocol in which the prover Peggy tries to convince the verifier Victor of her identity.
- The aim of the adversary Eve is to impersonate Peggy, i.e. to make Victor believe that he communicates with Peggy while actually communicating with Eve.
- Static identification schemes.
 - 1 knowledge (e. g. passwords)
 - 2 possessions (e. g. smart cards)
 - 3 physical characteristics (e. g. finger prints)
- Dynamic identification schemes (randomness employed).

User Identification

Definition - identification scheme

- An **identification scheme** S is a triplet

$$S = (G, P, V)$$

where G is a probabilistic polynomial algorithm generating identification information and P, V are probabilistic polynomial interactive algorithms which specify the actual identification procedure.

- The algorithm G takes as input a string 1^k , where $k \in \mathbb{N}$ is a security parameter, and outputs a pair (s, i) where s is called a private key and i is called a public key.
- The input of P is a pair (s, i) and the input of V is a public key i .
- After an interaction with P , V either accepts or rejects.

User Identification

Definition - adversary

- An **adversary** is a pair (P_a, V_a) of probabilistic polynomial interactive algorithms.
- The input of V_a is a public key i and after several interactions with the algorithm P , it outputs a string h .
- The input of P_a is the string h .
- The algorithm P_a interacts with V and tries to make it accept for the input i .

- An identification scheme should satisfy the following conditions:
 - 1 (Completeness) If both Peggy and Victor are honest, Victor will complete the protocol by accepting Peggy's identity.
 - 2 (Transferability) Information obtained from the interaction with Peggy does not enable Victor to impersonate her to a third party Charles.
 - 3 (Impersonation) No adversary Eve is able to impersonate Peggy to Victor with non-negligible probability.

Identification Scheme

- The identification scheme consists of protocols $\text{Init}(G, k)$ and $\text{Ident}(G, k)$ where

$$G = (X, Y, A, B, P, W)$$

is a pseudo-telepathy game and k is a security parameter.

- The goal of the first protocol is to ensure that Peggy and Victor share $k \geq 1$ copies of the entangled state $|\psi\rangle$ required by the quantum winning strategy for G .
- In the second protocol Victor is convinced of Peggy's identity if she proves herself to be the party which Victor shares the copies of the state $|\psi\rangle$ with.

Identification Scheme

Initialization

For $i \in \{1, \dots, k\}$ Victor creates an entangled state $|\psi_i\rangle = |\psi\rangle$, where $|\psi\rangle$ is a state required by the quantum winning strategy for G , and sends a part of $|\psi_i\rangle$ to Peggy.

Identification Scheme

Identification

For $i \in \{1, \dots, k\}$ Peggy and Victor perform the following actions:

- 1 Victor chooses a question $(x, y) \in_R P$ and sends x to Peggy.
- 2 Peggy applies to her part of $|\psi_i\rangle$ the unitary transformation U_x and performs the measurement M_x on her register, as required by the quantum winning strategy for G .
- 3 Peggy sends the outcome a of her measurement to Victor.
- 4 Victor applies to his part of $|\psi_i\rangle$ the unitary transformation U_y and performs the measurement M_y on his register, as required by the quantum winning strategy for G . Let b be the outcome of his measurement.
- 5 Victor verifies whether $(x, y, a, b) \in W$.

Victor accepts if and only if all the verifications have been successful.

Conclusions and Open Problems

- Pseudo-telepathy games are two party cooperative games for which there is no classical winning strategy, but there is a winning strategy based on sharing quantum entanglement by the players.
- We have proposed a simple user identification scheme based on playing some pseudo-telepathy game by the parties.
- How suitable are particular pseudo-telepathy games for the proposed scheme?
- Can pseudo-telepathy games be of any use also for other cryptographic problems (e. g. message authentication)?