Identification Tokens — or: Solving The Chess Grandmaster Problem

Thomas Beth
Fakultät für Informatik
Universität Karlsruhe
Germany

Yvo Desmedt[*]
Dept. EE & CS
Univ. of Wisconsin – Milwaukee, U.S.A.

Abstract. *Fiat and Shamir have proposed to use zero-knowledge interactive proofs to obtain secure identification mechanisms. Real time attacks in which active eavesdroppers relay questions and answers or in which the prover helps deliberately an impersonator have been described [4]. In this paper a solution against such frauds is given and (based on some physical assumptions) it is proved that the solution protects against the real-time attacks.*

1 Introduction

The use of zero-knowledge interactive proof systems for identification purposes was proposed by Fiat and Shamir [7]. Later Fiat and Shamir [8] have extended this idea to the process of identification *without* having to rely on physical description (see also [6]).

In this paper we will describe interactive proof systems and the process of identification from a game theoretic viewpoint. The game model is an essential tool in this paper. It will allow us to formalize the concept of the so called *mafia* and *terrorist* fraud [4] based on the idea of simultaneous display [2]. The *purpose* of this paper is to present a model which allows to *solve* the "Chess Grandmaster" problem, into which the identification problem will be converted. Such a model enables us to present an identification scheme which is provably secure against the aforementioned real-time attacks. This scheme does not rely on physical description of the individual who is identifying himself. We are not concerned about the rental fraud [4], but we will discuss it briefly at the end.

[*] Work done while visiting the EISS, University of Karlsruhe, West Germany.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 169-176, 1991.

2 Interactive proofs: a formal game theoretic viewpoint

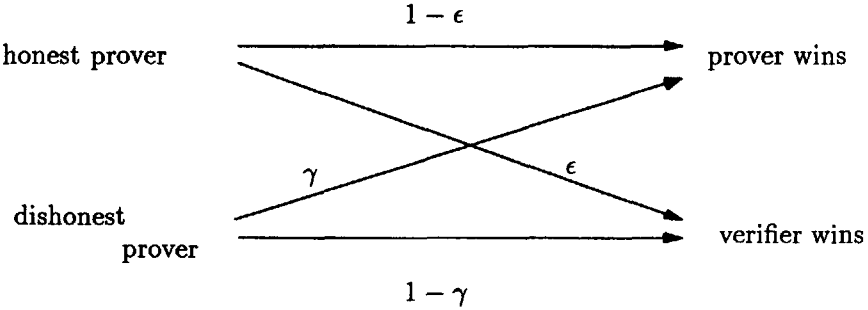
2.1 THE LOGICAL LINK

Interactive proofs [9] are probabilistic games in a formal sense as we now explain.

We define games following [2, p. 71], via the notion of a game tree. An interactive proof of membership [9] consists of a prover A and a verifier B, who formally correspond to probabilistic Turing machines communicating with each other according to a protocol (A, B). On their common input tape is a binary string x for which A proves that x is an element of a given set L (a "language"). The execution tree of the protocol can be interpreted as a game tree and we call A and B players. We now assume that the verifier B follows the described protocol (which in the literature is noted as B being the honest verifier. But the reader is warned to attach too much interpretation to the word "honest"). For the prover there is not such a restriction. When the game starts the prover basically has two options, which are:

- to input an $x \in L$ and to follow A's protocol.
- to input an $x \notin L$ and to follow any protocol.

(In the formal definition of interactive proof the input is written on the common input tape, to let this fit with our purposes we have followed the above approach). Let ϵ and γ respectively be the failure and the cheating probabilities, which are related to completeness and soundness. We now say that if the verifier accepts (x) then the prover wins the game, else the verifier wins. This game aspect of zero-knowledge is the only property of this concept we will need in this paper. (An almost identical reasoning is valid for proofs of knowledge.) Due to the completeness and soundness properties we obtain the following transitions:



2.2 THE IMPACT

In game theory there is [2, p. 75]:

> *a famous story of the little girl who played ... against two Chess Grandmasters ... How was it that she managed to win one of the games? Anne-Louise played Black against Spassky. White against Fisher. Spassky moved*

first, and Anne-Louise just copied his move as the first move of her game against Fisher, then copied Fisher's reply as her own reply to Spassky's first move, and so on.

We will refer to the above as the *Chess Grandmaster problem* and call the fraud the *little girl's fraud.* It is clear that two games are played which we call: game 1 and game 2. Because zero-knowledge can be described as a game, the above scenario is valid in the context of Fiat-Shamir like identification. The *main purpose of this paper* is to find solutions for this Chess Grandmaster problem and to apply these solutions to cryptography.

Observe that when the little girl plays against the Right player, she is copying (mimicking) the Left player and when she plays against the Left player she is copying (mimicking) the Right player.

2.3 Relation with identification

Related to identification, the Chess Grandmaster problem corresponds to the mafia fraud [4]. The mafia fraud uses a pair of two cooperative persons in the middle, resembling the little girl in the Chess Grandmaster problem.

One can wonder to what the so called "terrorist fraud" [4] corresponds in game theory, which in short reads as follows: a citizen of α-land is helping deliberately a terrorist enter α-land. Hereto the citizen helps the terrorist answer questions asked by the immigration officer. From a game theoretic point of view, the difference between the mafia fraud and the terrorist fraud vanishes, when carefully analyzed.
These analogies imply the following very important conclusions:

Observation 1 *Secure identification cannot be solved based on techniques which can properly be modeled using game theory.*

Therefore, to *make secure identification schemes one has to rely on a different model.*

Observation 2 *Each time a solution is presented against the mafia fraud, then this solution can,* in theory, *be extended to protect against the terrorist fraud.*

Hereto it is sufficient that the prover's part of the secure protocol is embedded into a tamperfree system which enforces the prover to follow the protocol, for so far it is technically feasible to enforce it.

3 A new practical solution against the Chess Grandmaster problem

Suppose that Grandmasters want to make sure that they are not fooled by the little girl. In other words they want to be sure that if the little girl wins the chess game, it was her brain that allowed her to win, without having to tap the brain of another

Chess Grandmaster. To solve this problem all chess players will from now on follow the following protocol:

```
Step 1 Before the two players start the chess "game"[1] they agree on a certain $t$,
       where $t$ is a time period expressed in seconds. (As usual they then agree who
       should start the "game".) We prefer to call the one who starts the "game"
       $F$ (for first or Fisher) and the other player $S$ (for second or Spassky).
Step 2 $F$ opens the "game" and at the same time he resets his clock and sets
       $z := 0$.
Step 3 $S$ resets his clock. ($S$ thinks about his first move.) $S$ makes his move at
       *precisely* time $t$ and sets $y := t$.
Step 4 $F$ reads from the clock the time $e$. *If* $e - z \neq t$,
         *then* $F$ stops playing and the protocol terminates ($F$ assumes that he was
           fooled)
         *else if* $S$ won the "game"
           *then* $F$ stops playing and the protocol terminates
           *else* ($F$ thinks and) at *precisely* time $e + t$ he makes his move and
             sets $z := e + t$.
Step 5 $S$ reads from the clock the time $f$. *If* $f - y \neq t$,
         *then* $S$ stops playing and the protocol terminates ($S$ assumes that he was
           fooled)
         *else if* $F$ won the "game"
           *then* $S$ stops playing and the protocol terminates
           *else* ($S$ thinks and) at *precisely* time $f + t$ he makes his move and
             sets $y := f + t$.
Step 6 Goto Step 4.
```

Observe that we have used two symbols e and f to indicate elapsed time respectively of F and of S. This means that both have their own clock and do not trust outside clocks.

Theorem 1 If *the little girl G needs at least a time $l > 0$ to communicate the moves between "game 1" and "game 2"* and *F and S follow the protocol,* and *the number of moves m in the game is more than 2 (so $m \geq 3$),* then *the little girl's fraud is detected by F or S.*

Proof. When a little girl G is present, "game 1" is played by F against G and "game 2" is played by G against S and G copies moves as described earlier. Suppose that in Step 1 of the protocol of "game 1" F and G agree on time t_1 and in "game 2" G and S agree on time t_2 (t_1 and t_2 are not necessarily identical). F makes his first move at moment 0 for "game 1" and sets $z := 0$. (Starting at another moment than 0

[1] We have used quotation marks because what we have described is no longer a formal game.

would only make the notations heavier for no reason.) To copy this move to "game 2", G needs the time $l_1 \geq l > 0$. So the move arrives there at the *moment* l_1 and at that moment S resets *his* clock. Then S makes his move (still on "game 2") at time $l_1 + t_2$ and sets $y := t_2$. To copy this move to "game 1", G needs the time $l_2 \geq l > 0$ (there is no need that $l_1 = l_2$). So the move arrives in "game 1" at the moment $l_1 + t_2 + l_2$. F now reads the time e and checks that $e - z \neq t_1$. Now $e = l_1 + t_2 + l_2$ and $z = 0$. So, *at this point* F will not always detect the fraud. Indeed if $t_1 = l_1 + t_2 + l_2$ it will not be detected *at this point*. So if F has detected the fraud the proof of the theorem ends at this stage.

So we now assume that the fraud was not yet detected, implying that:

$$t_1 = l_1 + t_2 + l_2. \tag{1}$$

F will now make his move at time $l_1 + t_2 + l_2 + t_1$. To copy this move to "game 2", G needs the time $l_3 \geq l > 0$. So the move arrives there at the moment $l_1 + t_2 + l_2 + t_1 + l_3$. S now reads the time f on *his* clock. *His* clock reads: $f = t_2 + l_2 + t_1 + l_3$ and $y := t_2$. So $f - y = l_2 + t_1 + l_3$ and S checks if $f - y \neq t_2$. In order that the fraud would not be detected one needs that:

$$t_2 = l_2 + t_1 + l_3. \tag{2}$$

However combining equations (1) and (2) we obtain $l_1 + 2l_2 + l_3 = 0$ but because all $l_i \geq l > 0$ this is impossible. So S will detect the fraud. □

Remarks:

1. We emphasize that according to the above theorem F *or* S will detect the fraud. This could imply that one of the two remains in the dark about it. Rivest pointed out that when the little girl plays chess against *many* (deterministic) robots, she could win of one robot and the loosing robot will not detect the fraud. Hereto she will *abort* some games, start new games and copy the moves of older games. When the robots' games are influenced by random and are sufficiently independent, it is unlikely that this fraud will work. Indeed moves of old games will be useless. Zero-knowledge based identification scheme are in fact such random games, so in this context the above problem is nil. A more formal discussion of this multi-game problem will be given in the final paper.

2. In some informal discussions some scientists had the intuition that the above theorem could easily be generalized by systems they proposed us. All those turned out to be insecure. Let us just describe one variation. In it, F and G agree in Step 1 on two times t and t'. F will use as response time t and S's response time will be t'. When the little girl is in the middle we obtain t_1 as F's response time, and t'_1, t_2 as G's response times in game 1 and respectively game 2, and t'_2 as S's response time. By reading the last observation in Section 2.2 one can check that when $t'_1 \geq t'_2 + 2l$ and $t_2 \geq t_1 + 2l$, then the little girl can always defraud the system.

3. It may appear that the above mathematical solution is physically unfeasible as to question of precision. The next section will address this problem.

4 Converting the solution into a secure identification scheme

4.1 Solving the mafia fraud

Before adapting our solution to identification, observe that the speed of light is not infinite. So when F sends a signal to S (makes his move) the communication time is l/c, where c is the speed of light and l is the distance between F and S.

Cryptosystems [1] have been proposed which security depends on physical assumptions. We follow a similar approach. Beside some computational complexity assumption, we need the following physical assumptions:

- The speed of light is constant [5] and cannot be influenced (by an opponent).
- An opponent cannot slow down or speed up an individual's time, taking into account that time is a relative concept to speed of F vice versa S and the gravitational field.

and the following engineering assumptions:

- One cannot influence the *clock* of an opponent, and all other aspects of time used inside a secure device.
- One cannot be made invisible.

Let us now explain the identification scheme[2].

In the identification scheme prover and verifier measure independently the *relative* distance between themselves. The required accuracy depends on the crowdedness of their environment. In some applications (such as identification in banks) it is easy to guarantee that the area is not too crowded and in such circumstances the verifier can organize himself that he knows the distance. The above protocol is then followed, in which the "game" is a zero-knowledge proof[3].

Inexpensive quartz technology gives a sufficient precision [11] for our purposes as will be fully explained in the final paper.

[2] For simplicity we assume in this abstract that prover and verifier are on this planet (time is relative to the gravity field) and that they do not move relative to each other (in the final paper we will explain that excluding rocket technology the speeds which can be obtained by individuals with modern technology on this planet is too small to be significant).

[3] Because $P \subset ZKIP$ we evidently have to assume that it is hard for an opponent to check membership and/or to calculate the knowledge.

4.2 Solving the terrorist fraud

To adapt the above to make it secure against the mafia fraud, we rely on a trusted center who makes and distributes electronic identity cards (credit cards, etc.). The devices made by the center are *tamperfree.* Moreover it are those devices *themselves* (and not the carriers of those) which will execute the protocol (it is measure the relative distance and so on). In many circumstances it is very realistic to assume that small automatic devices can perform the above (as will be explained in the full paper).

5 Final observations and conclusions

5.1 Observations

Earlier a method [3] has been proposed to avoid the mafia fraud. In that solution a prover signs as message the exact, *absolute* location he is standing on earth. To identifying himself he proves to the verifier in zero-knowledge the knowledge of this signature. This method does not protect against the terrorist fraud. Using our Observation 2, one can solve that problem when the identification device itself measures this location (cf. the final paper).

As said in the introduction we have not been concerned about the rental fraud in which some prover borrows his identity device to somebody else. It seems that solutions need to take the physical description of the individual into consideration. However when one relies on this description, it is easier that the center just signs the individual's description [4, 10, 12]. A solution which doesn't require physical description is that the identification device is attached to the individual and that taking the device off will be detected by the device itself, which then deactivates itself. Under some circumstances it is only required that this device remains attached for a few hours (see final paper).

5.2 Conclusion

Because the speed of light is finite and constant we have provided a practical solution to the mafia and terrorist fraud. Its applications go beyond identification.

Acknowledgement

The authors thank Louis Guillou and Shimon Even for having observed that the mafia fraud is similar to the little girl who played simultaneously chess against two Chess Grandmasters. This inspired the game approach followed in this paper. The authors thank Gilles Brassard, Jim Massey, Ron Rivest, and Rainer Rueppel for discussions related to this paper.

6 References

[1] C. H. Bennett and G. Brassard. An update on quantum cryptography. In *Advances in Cryptology. Proc. of Crypto'84 (Lecture Notes in Computer Science 196)*, pp. 475–480. Springer-Verlag, New York, 1985. Santa Barbara, August 1984.

[2] J. H. Conway. *On numbers and games*. Academic Press Inc., London,U.K., 1976.

[3] Y. Desmedt. Major security problems with the "unforgeable" (Feige-)Fiat-Shamir proofs of identity and how to overcome them. In *Securicom 88, 6th worldwide congress on computer and communications security and protection*, pp. 147–159. SEDEP Paris France, March 15–17, 1988.

[4] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the Fiat-Shamir passport protocol. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto '87 (Lecture Notes in Computer Science 293)*, pp. 21–39. Springer-Verlag, 1988. Santa Barbara, California, U.S.A., August 16–20.

[5] A. Einstein. *Relativitätstheorie*. Friedr. Vieweg, Braunschwig, 1916.

[6] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. *Journal of Cryptology*, 1(2), pp. 77–94, 1988.

[7] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, *Advances in Cryptology, Proc. of Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 186–194. Springer-Verlag, 1987. Santa Barbara, California, U. S. A., August 11–15.

[8] A. Fiat and A. Shamir. Unforgeable proofs of identity. In *Securicom 87*, pp. 147–153, March 4–6, 1987. Paris, France.

[9] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *Siam J. Comput.*, 18(1), pp. 186–208, February 1989.

[10] P. D. Merillat. Secure stand-alone positive personnel identity verification system (ssa-ppiv). Technical Report SAND79–0070, Sandia National Laboratories, March 1979.

[11] N. F. Ramsey. Precise measurement of time. *American Scientist*, 76, pp. 42–49, January–February 1988.

[12] G. J. Simmons. A system for verifying user identity and authorization at the point-of sale or access. *Cryptologia*, 8(1), pp. 1–21, January 1984.