# SPECIAL USES AND ABUSES OF THE FIAT-SHAMIR PASSPORT PROTOCOL

(extended abstract)

Yvo Desmedt [a], Claude Goutier [b] and Samy Bengio [a]

[a] Dépt. I.R.O., Université de Montréal,
C.P. 6128, succ. A, Montréal (Québec), H3C 3J7 Canada

[b] Centre de calcul, Université de Montréal,
C.P. 6128, succ. A, Montréal (Québec), H3C 3J7 Canada

**Abstract**

*If* the physical description of a person would be unique and adequately used and tested, *then* the security of the Fiat–Shamir scheme is *not* based on *zero-knowledge*. *Otherwise* some new frauds exist. The Feige–Fiat–Shamir scheme always suffers from these frauds. Using an extended notion of subliminal channels, several other *undetectable* abuses of the Fiat–Shamir protocol, *which are not possible with ordinary passports*, are discussed. This technique can be used by a terrorist sponsoring country to communicate 500 new words of secret information each time a tourist passport is verified. A non-trivial solution to avoid these subliminal channel problems is presented. The notion of *relative* zero-knowledge is introduced.

## 1 Introduction

Fiat and Shamir proposed (at several conferences *e.g.*, [12,11,16]) a protocol for identification which enables any user to prove his identity to any other user without shared or public keys. A variant of this protocol was proposed by Feige, Fiat and Shamir [10].

In 1986 Desmedt and Quisquater [8] already discussed a fraudulent use of the Fiat–Shamir protocol. Their remark was mainly that the Fiat–Shamir protocol identifies *secret information* instead of identifying the person. Thus some persons (*e.g.*, Alice) could *deliberately* "create" a second person (*e.g.*, using cloning) such that both can claim to be Alice. Their solution to this problem is not considered in this paper, except when appropriated.

In our paper we first explain the first version [16] of the Fiat–Shamir protocol, the more general version [12] and the Feige–Fiat–Shamir version [10] (see Section 2). We show that the Feige–Fiat–Shamir scheme suffers from *new* and *well-known old* fraudulent techniques (see Section 3). The Fiat–Shamir scheme suffers from the same problems *if* physical description would not be unique or not adequately tested, *else* its security is not based on zero-knowledge (see Section 3). In Section 4 we discuss several frauds which are in fact extensions of the subliminal channel idea of Simmons [17]. We will show that several subliminal channels can be brought in all the actual versions of the (Feige–)Fiat–Shamir schemes. Their dangers will be briefly discussed in the same section. Section 5 presents a solution to solve the subliminal channel problem in the Fiat–Shamir and Feige–Fiat–Shamir scheme.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 21-39, 1988.

Some of the frauds which will be discussed in this paper could be misinterpreted as being politically oriented. To avoid this, non-existing countries will be taken as example, so we will speak about $\alpha$land, $\beta$land and so on.

# 2 The (Feige–)Fiat–Shamir protocol

The protocol is explained in the case it is used for passport purposes. Evidently it can also be used for other identification purposes such as credit cards. Several other applications were discussed by Fiat–Shamir [11].

We will first explain the basic version of the protocol [16], then the more general version [12] and finally the latest version [10].

## 2.1 The basic version

The protocol uses as many public keys as there are countries (more generally as there are centers who issue cards or passports). We will use the symbol (integer) $n$ for the public key of a country (center), where $n = p \cdot q$ such that $p$ and $q$ are secret primes only known to the center. Remark that the authentification problem of the public key is extremely reduced since the number of countries is small.

Let us now explain the start-up of the system. There exists a standard keyless (pseudo-random) one-way function $f$. Let us call $I$ the "name" of an individual (*e.g.*, Alice) who wants to receive a passport from the center. To be unique $I$ (the "name") contains relevant information about the individual; *e.g.*, the name, address and ***physical description.*** For each individual the center picks a (small) $j$ such that $m = f(I, j)$ is a quadratic residue (mod $n$). The center calculates the smallest $\sqrt{m} \pmod n$ and gives it to the individual. We will refer to $\sqrt{m}$ as the secret identification of the individual.

If Alice wants to identify herself to Bob then they use the following ping-pong protocol. First she tells Bob her nationality, her "name" ($I$) and $j$. So Bob knows which $n$ to use. Bob calculates $m$ corresponding with $I$ and $j$. Then the ping-pong part starts:

**Step 1** Alice chooses a ***random*** $s \pmod n$ which we will further call $\sqrt{t}$ and Alice squares it (mod $n$) to obtain $t$. She sends $t$ to Bob.

**Step 2** Bob sends Alice one ***random*** bit $e$.

**Step 3** Alice sends then $\alpha = \sqrt{t} * \sqrt{m^e}$.

**Step 4** Bob verifies by squaring. (This is trivial, because he has to verify that $\alpha^2 = t * m^e \pmod n$ and he knows $m$ and $t$, because Alice has sent that.)

Somebody else could have claimed to be Alice with a probability of 1/2. To decrease this success of frauding the protocol is repeated as many times as required for security. We will call Bob the verifier and Alice the passport holder.

Shamir claimed at Marseille [16] that the last protocol is a zero-knowledge one.

The attentive reader may have remarked that the *original Shamir protocol* is slightly *different*. Indeed Shamir claims it is better to use $\sqrt{m^{-1}}$ instead of $\sqrt{m}$ to avoid calculations of inverses modulo $n$ [10]. We now show that this claim is exaggerated and that our version is faster.

## 2.2 This slightly modified version is faster than the original

In the original version Bob has to verify in Step 4 that $t = \gamma^2 * m^e \pmod{n}$, where $\gamma = \sqrt{t} * \sqrt{m^{-e}} \pmod{n}$ and $\gamma$ has been sent by Alice in Step 3.

First remark that from a *mathematical point of view* the verification $\alpha^2 \equiv t * m^e$ and the verification $t \equiv \gamma^2 * m^e$ are *identical*, because $\alpha \equiv m^e * \gamma \pmod{n}$ and because $\gcd(m, n) = 1$. *However* the two verifications differ from a *computational point of view*. Indeed to do this verification step (in Shamir's original version) Bob has to *wait* until he received $\gamma$ from Alice, *then* he has to square it and multiply it with $m$ (when $e = 1$). In our version Bob can multiply $t$ and $m$ (if $e = 1$) *while* he is *waiting that Alice calculates and sends* $\alpha$, *then* when he receives $\alpha$ he has only to square it to verify that $\alpha^2 = (t * m^e)$, where the right-hand side was calculated *before* (as just explained).

So no inverses have to be calculated in the protocol in any of the two cases. In the two cases a squaring operation has to be done and, if $e = 1$, an additional multiplication. *However* our version is faster because a part of the calculation can be done in *parallel* (while Alice is calculating and sending).

The same remark about speed is also valid for the Fiat–Shamir [12] and the Feige–Fiat–Shamir [10] protocol. *So from now on, when we explain or use the other versions, we will use the faster adaptation.*

## 2.3 The Fiat–Shamir protocol

The differences are small (except some proofs) between the first version (discussed in Section 2.1) and the more general Fiat–Shamir protocol. Instead that *only one* $j$ exists, $k$ such $j^i$ exists, so that $k$ $m_i$ $(1 \leq i \leq k)$ and $k$ $\sqrt{m_i}$ exist. In the ping-pong protocol Bob sends $k$ $e_i$ in Step 2. In Step 3 now Alice sends

$$\alpha = \sqrt{t} * \prod_{e_i=1} \sqrt{m_i} \pmod{n}.$$

Bob verifies (in Step 4 by squaring, this means calculates first (in parallel with Step 3) $\beta = t * \prod_{e_i=1} m_i$ and when he receives $\alpha$, he squares it to verify that $\alpha^2 = \beta \pmod{n}$.

## 2.4 The Feige–Fiat–Shamir scheme

By reading [10] and comparing it with [12] the differences between the Fiat–Shamir and Feige–Fiat–Shamir protocol seem small, *however* they are important. The fact that the prover does not reveal that a number is, or is not, a quadratic residue, is *not* extremely *important* in the *context of our paper*. The important difference is that in their new scheme [10, pp. 214-215] *the role of the center is enormously reduced*. We now explain this, by emphasizing this last fact.

The *only* role of the center is to publish an $n$ of the appropriate form (the product of two large primes each of the form $4r + 3$). *And then* the center *closes*. Each individual chooses $k$

random numbers $S_i \pmod n$. He then chooses each $m_i = \pm S_i^2 \pmod n$, where the sign is decided randomly (and independently). He keeps the $S_i$ secret and makes the $m_i$ public.

*Remark at this point the* enormous *difference with previous protocols.* In previous protocols the *center* was calculating *square roots*, while here the *individual* calculates *squares*. *This remark will play a very important role in Section 3.2.*

The ping-pong protocol to prove Alice's identity is very similar to the Fiat–Shamir protocol. Details are not important in this context, for them see [10].

# 3 Physical description and related problems and frauds

In this section we first show that *if* the physical description of a person is unique and adequately used and tested, *then* the security of the Fiat–Shamir scheme is *not* based on *zero-knowledge*. Otherwise some new (and also old) frauds exist, which can severly affect the security of the identification.

## 3.1 Security aspects of Fiat–Shamir not related to zero-knowledge

In this subsection we assume that the physical description is *unique* and is used as a part of $I$ (see Section 2.1), which is an input of the one-way function $f$. We also assume that each time that Alice's passport is verified, her $I$ is adequately tested. This means that the verification of the physical description *is always done by the verifier* and with a 100% accuracy. In that case it is trivial to understand that the security of the Fiat–Shamir protocol is not based on zero-knowledge. Indeed there is no danger for Alice to reveal her $\sqrt{m_i}$ each time she wants to prove her identity. The verification of the identity would then be that Alice gives her $I$, that her physical description is tested and verified and then she reveals her $j_i$ and her $\sqrt{m_i}$ to the verifier. There is no danger that the verifier or friends of the verifier or who so ever (else than Alice) can afterwards (or at the same moment) claim to be Alice. Indeed when they would try to use it, their physical description will be tested giving another $I'$, giving another $m'$, so $\sqrt{m}$ (of Alice) is not useful to them. To demonstrate it completely, suppose that they could use $\sqrt{m}$, then they could forge fake individuals! This last fraud is impossible in the Fiat–Shamir scheme due to the one-way function and square-root operation.

The above reasoning is nothing else than applying the ideas from Simmons [19] to the Fiat–Shamir protocol. Readers who are more interested in a comparison between the two systems (Fiat–Shamir and Simmons [19]) are referred to [1].

The conclusion of the above is that the ping-pong protocol is simply a waste of time and effort. The main security aspect is the fact that the physical description is unique and adequately used and tested. To better understand its importance we now discuss what happens with the Fiat–Shamir and Feige–Fiat–Shamir protocol [10] when physical description is not unique.

## 3.2 Major frauds possible in the Feige–Fiat–Shamir protocol

*From now on we assume* that the physical description of the individual is not used in the identification system or is not unique or is not adequately checked (*e.g.*, a fraud with the physical description

is possible ). We remark immediately that the *Feige–Fiat–Shamir* protocol [10, pp. 214–215] does *not use the physical description.* Trying to do this is nevertheless difficult, due to the fact that an individual can not calculate square roots of random numbers.

Before, in 1986, Desmedt and Quisquater [8] already discussed a fraud in the case that physical description is not unique or adequately used and checked. In such case at least three other frauds or problems are possible with passports. *Some of these frauds and problems are well-known, due to the fact that some of them are also possible with ordinary passports. However they were never cited before in the context of the security of the Feige–Fiat–Shamir protocol. We also now discuss frauds which are not possible with ordinary passports.*

Before discussing these three frauds and problems we mention that more frauds are discussed in [1]. Some of the problems we will discuss now can be solved. Discussing these solutions is out of the scope of this paper, which focus on the abuses of the protocols. Readers interested in the solutions can find them in [1] and [5].

### 3.2.1 Individuals having several identities

In the Feige–Fiat–Shamir protocol the center vanishes after publishing the $n$. The work to publish the $m_i$ is left entirely to each individual . A clever individual can however make several entries into the public file (repeating several times the process of making new $m_i$) to have more than one name (identity) at the same moment. This trick is very useful for persons who wants to fraud with taxes. Another application of this fraud is that it allows you to commit a crime and disappear. Hereto you first publish several identities. One of them you never use. Then later, you identify yourself with the one you never use and commits the crime immediately so that the one who verified your identity is a witness. A search starts to find you back, however you have stopped to use that identity!

Consequently each individual must have *only one identity*. (If pseudonyms are used (as in [4]), then one individual may only go under the name of one pseudonym in one organization.) So we conclude that an organization (which we call the *center*) has to exist which verifies that one individual has only one identity! So the center has to manage the public file of the $m_i$. The center has to be trusted that an individual will not receive two identities. *However* if physical descriptions are not unique or not tested or similar problems exist, *the center itself is not able to recognize an individual when he applies a second time for an identity.*

Two solutions exist such that the center can guarantee the above uniqueness. The first one uses the terrifying idea of tamperfree babies which are uncloneable and containing a *unique* number (or name) as a part of their genetic code [1]. So this solution makes individuals testable unique. The other solution is not water-tight. In the last solution each individual can only apply for an identity when he is born. In fact his parents have to do this (or those who care for him). In several countries no fingerprints are taken from the newborn, so parents could ask the doctor for two birth-certificates and so apply for two identities. So if physical description is not tested or not unique (or similar), then the uniqueness of an individual in the end is based on trust.

We here remark that the uniqueness aspect of an individual is not a part of the definition of identity in the Fiat–Shamir [12] and in the Feige–Fiat–Shamir sense [10]. So the above fraud does not break the Feige–Fiat–Shamir protocol from a strictly mathematical point of view. *We*

*also remark that some of the above aspects are well-known to officials dealing with identification as immigration departments, counselors and so on.*

### 3.2.2 The mafia fraud

We call this fraud the mafia fraud as a consequence of Gleick's article [13] quoting Shamir (related to the protection of credit cards with his [12] protocol): "I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me".

Let us now explain the fraud. $A$ identifies himself to $B$. The latter is collaborating with $C$ and $C$ impersonates $A$ and tries to claim to be $A$. Then, $D$ checks the identity of $C$ who is claiming to be $A$. To make it easier to understand, $B$ is the owner of a mafia-owned restaurant, $C$ is a member of the same mafia-gang and $D$ is a jeweller. $A$ and $D$ are not aware of the following fraud. At the moment that $A$ is ready to pay and ready to prove his identity to $B$, $B$ informs $C$ that the fraud is starting. This is done by using a secret radio-link between $C$ and $B$. The identification card of $C$ communicates also, using such a radio-link, with the equipment of $B$. At this point, $C$ makes his choice of the diamond he wants to buy and so $D$ is starting to check "$C$'s" (in fact $A$'s) identity. While $D$ is checking the identity, $C$ and $B$'s role is only to sit in the middle between $A$ and $D$. So $B$ and $C$ pass all questions and all answers related to the mathematical part of the identification going from $D$ to $A$ and vice-versa. So even if $D$ is aware that an identification procedure over the telephone could not work, another person could come physically to his store and $D$ would not be aware that he is remotely checking $A$'s identity. Evidently this fraud does not work in all circumstances *e.g.*, when the verification of $C$'s claimed identity by $D$ cannot be synchronized with the verification of $A$'s identity by $B$. In our example the fraud is facilitated because $A$ goes frequently to mafia-owned stores. Nevertheless Shamir claims [13] that there is no danger.

A similar fraud is possible when $A$ *is willing to collaborate* with $C$ immediately! For more details see [1].

It is important to remark here that the above fraud is a real-time fraud. This does not exclude its generality, related to the Feige–Fiat–Shamir protocol because that protocol only works in real-time. Indeed they mentioned in [10, p. 214] that identification is a real-time operation!

### 3.2.3 Renting passports

*The fraud we discuss now is also possible with ordinary passports. However it was never cited in the context of the "secure" Feige–Fiat–Shamir scheme.*

We now explain why a user is sometimes willing to hire out his passport. Suppose that the identification system is used for passport purposes. Brigitte is not able to receive a visa to travel to $\alpha$land. However she has a good reason to travel to $\alpha$land. She is rich, but does not want to bribe the visa-office, because she does not like to start her trip with a lot of trouble. Alice proposes to hire her passport to Brigitte. In other words, Alice simply tells Brigitte her secret identification $\sqrt{m}$. (Remark that this fraud will not be detected by $\alpha$land.) The advantage for Alice is not only money, but now she can commit a crime with a perfect alibi. Hereto Alice commits a crime while Brigitte is travelling in $\alpha$land (pretending to be Alice). Alice has evidently a perfect alibi, because Alice (in fact Brigitte) has proven several times (at the moment of the crime) that she was in $\alpha$land. Remark that this last fraud is very close to Russian roulette. Indeed Brigitte could

also have committed a crime while she is renting Alice's identification system and be certain she will not be arrested. She commits this crime in the neighbourhood of Alice's home. Brigitte first identifies herself as being Alice (which is possible), then commits the crime (*e.g.*, in the same room) and runs away! Alice can evidently pretend that she hired her secret to Brigitte, but who will believe her!

One could conclude that the identification protocol is in fact a protocol of identification of the secret $\sqrt{m}$ instead of identifying the individual. This is the same conclusion as in [8]. To overcome this problem Desmedt and Quisquater proposed a technique that prevents copying of $\sqrt{m}$. Remark that their solution does however not solve this fraud!

Because the above fraud is also possible with the actual passports (*e.g.*, by tampering with the photo) it seems to be inherent to passports in general. This remark remains valid even if biologic information related to the individual is a part of the $I$ as a consequence of cloning (see also [8]).

The tamperproof babies solution (see Section 3.2.1 and [1]) solves the above problem. The only practical solution that the authors see is that each individual is forced to show his passport very frequently, (*e.g.*, each day, at each corner of the street) as in a police state. Then the above fraud can be extremely reduced.

An important conclusion here is that some frauds are possible if the user allows somebody to fraud. One could compare this with the first ideas about signatures. After that Diffie and Hellman [9] proposed the idea of signature, Saltzer [15] said that its security was limited when the undersigned claimed that his secret key was stolen, while it was in fact deliberately made public. The idea of the fraud with passports is similar. The above remarks *generalize* to all cases wherein somebody considers *loosing* (partially) *his identification secret* as of *minor importance.*

In the following sections frauds *which are not possible with ordinary passports*, are discussed. In the new frauds one does not necessarily loose his identification secret.

# 4 Traffic-analysis-free communication using the (Feige–) Fiat–Shamir protocol

## 4.1 An extension of the subliminal channel idea

Simmons [17] presented the idea of a subliminal channel as a part of a channel with authentication facilities. Simmons assumed that two prisoners are allowed to send *messages* in full view of the warden such that the messages are completely open (and presumably innocuous) to the warden. The last one however agrees that the prisoners may authenticate the *communication.* Simmons explains how a subliminal channel can be set up [17].

The idea of Simmons can trivially be extended to the identification protocol of Fiat–Shamir. The main idea is that instead of choosing $\sqrt{t}$ and/or $e$ randomly, *they are a part of a secret message.*

A *further generalization* of the idea of subliminal channel is that the subliminal channel is not used by the sender to communicate with the addressee. The sender uses it to communicate with an eavesdropper.

Finally we introduce the notion of *subliminal protocol*. When a protocol is used in full view of a warden, it is possible that it "hides" another protocol. In the best case (or worst case, depending of the point of view) the warden is *not able to detect that such a subliminal protocol is used*. The word "hided" has to be interpreted in its widest sense. An example of such a subliminal protocol will be used in Section 4.2.

It is very important to remark that the above generalizations are quite different from the original idea of Simmons. This is very clear from the viewpoint of *traffic-analysis*. Indeed if one looks at the use of "normal" (actual) passports, it happens frequently that one does *not speak* during its verification. In some countries when you arrive at the border you give your passport, it is verified and the agent does not even tell you that you are allowed to walk in. He simply looks to the passport of the next person. So here *nothing is communicated* except the specific message: "I am Alice". So traffic-analysis of such a message is worthless, while in Simmons idea the warden knows that a message is sent (the one the warden is able to read). A similar remark is true for our second generalization. The traffic analyst does not know who is eavesdropping. So a traffic-analyst will not be able to tell if a communication between passport verifier (or the passive eavesdropper) and passport holder (or the passive eavesdropper) is under way!

*From now on* we assume that all countries agreed to use the Fiat–Shamir protocol for passport purposes, instead of the paper or plastic document. All countries signed an agreement about it. We also assume that its use is yet very general. Several applications of this subliminal channel idea to passports , to credit cards and so on are discussed in Section 4.4. We will now discuss how to use the subliminal channel idea in the basic, the general Fiat–Shamir and the Feige–Fiat–Shamir protocol. There are mainly two cases: the verifier or the passport holder wants to send a message using a subliminal channel. Setting-up a *secure* subliminal channel is much more complicated in the last case than in the first one. Remark that the center can always communicate a very little bit, by choosing a special $j$ (not applicable to the Feige–Fiat–Shamir scheme). $j$ in fact can contain a few bits of information. We will no further discuss this last case, because it is not a real communication channel.

Let us now explain how the verifier Bob can communicate in a subliminal way to the passport holder or to an eavesdropper. Hereto he does not choose the collection of $e$'s randomly but he lets them correspond to the encrypted message, using a secret key system or a public key system. So $\mathbf{e} = (e_1, e_2, \ldots, e_l)$ corresponds with $E_k(M)$, where $M$ is the message. Remark that if the message is intended for an eavesdropper, then Alice (the passport holder) is not able to predict the $e$'s. So Bob is still verifying Alice's identity with the same accuracy!

As already mentioned the set-up of a secure subliminal channel in which the passport holder communicates is much more difficult. First of all if the verifier is willing to cheat enormously there is no problem to set up a subliminal channel. The cheating consists in dropping the verification step (Step 4) in the Fiat–Shamir (or Feige–Fiat–Shamir) protocol. Indeed suppose that there is no warden who controls the protocol, the following cheating is possible. The passport holder sends the encrypted message as $t$. The verifier sends $e$. Of course, sometimes the passport holder is not able to give the correct answer. When this happens the passport holder simply sends a random number (mod $n$). The verifier willing to cheat, does simply not verify that the passport holder did not answer correctly.

From now on we assume that there is a warden who reads all what verifier and passport holder send. He performs himself the verification step. We could also easily assume that all this is done in public. So that everybody knows what $t$, $e$ and so on are. A warden was also used by Simmons [17].

In the case that the passport holder communicates, there are *several dangers* that the passport holder *wants certainly to avoid.* Indeed he is willing to communicate with the passport verifier, but he prefers (if possible) not to loose his identification secret. He also wants that the center who issued the passport is not able to detect that a subliminal channel is used! He does not want that others (*e.g.*, the warden) detect what is going on. *General* solutions will be proposed in which we assume that the receiver of the subliminal channel does not collaborate with others to help them in detecting that a subliminal channel was used. This seems a very reasonable assumption. Also in Simmons case [17] the same assumption is valid without being mentioned by Simmons, similarly in [18].

In [6] the *general solutions will be proven to be secure against detection of their use and against revealing (a part) of the identification secret* by using reasonable assumptions, *such as* the assumption of no collaboration by the receiver (or by the sender) to help others to detect the subliminal channel or to prove that it has been used, the assumption that factorization is hard and that it is infeasible to detect if a number $q$ (for which the Jacobi symbol $(q \mid n) = 1$) is a quadratic residue (mod $n$) (without the collaboration of the center or others who knows the factorization of $n$). *The encryption system used in the subliminal channels is a secure probabilistic public key system (e.g., the Blum–Goldwasser one based on RSA [2, pp. 298]) or a secure conventional system (e.g., based on a good pseudo-random generator, e.g. [3], used in a (synchronous) stream cipher).*

There exist several cases related to the introduction of a subliminal protocol (in which the passport holder communicates) in the Feige–Fiat–Shamir scheme. Hereto we will first discuss in Section 4.2 how to introduce it in the basic Fiat–Shamir scheme. Then we discuss how two different subliminal protocols can be introduced in the general Fiat–Shamir scheme (see Section 4.3). We will not discuss in detail how to introduce one in the Feige–Fiat–Shamir scheme. The reader can easely figure out that the same techniques as in Section 4.3 are applicable.

## 4.2 Introducing the subliminal protocol in the basic Fiat–Shamir

In our subliminal protocols Alice wants to send a message (using the subliminal channel). She is the passport holder. The receiver of the subliminal channel is Daisy. The verifier of the passport is Bob. It makes no difference if Bob and Daisy would be the same person, *so no collaboration of the verifier is required*, *e.g.*, by choosing the $e$ in a special way. Daisy could for example be eavesdropping.

Let us now describe the subliminal protocol which is used during the basic Fiat–Shamir protocol. Alice wants to send the message $M$ to Daisy. Every user, so also Alice use a known number $y$ such that the Jacobi symbol $(y \mid n) = -1$. (Such $y$ can easily be generated in random polynomial time.) This $y$ may even be standard.

**Step 1** Alice decides not to choose $\sqrt{t}$ randomly, but to do the following. Alice authenticates $M$ and encrypts it to obtain $C$. She selects a random bit $v \in \{0, 1\}$. She selects a

random number (mod $n$). We will call this random number $\sqrt{r}$. She squares it (mod $n$) and multiplies it with $C$ and with $y^v$ to obtain $Cry^v \pmod{n}$ and uses it as $\sqrt{t}$ for the basic Fiat–Shamir protocol, this means $\sqrt{t} = Cry^v \pmod{n}$. She now follows the basic Fiat–Shamir protocol, this means she squares $\sqrt{t}$ and sends it to Bob. (In other words she sends $C^2r^2y^{2v} \pmod{n}$ to Bob.)

**Step 2** Bob chooses a (really) random $e$ and sends it to Alice (as in the basic Fiat–Shamir protocol).

**Step 3** Alice follows the basic Fiat–Shamir protocol, so if $e = 1$ she sends $\sqrt{t * m} \equiv Cry^v\sqrt{m} \pmod{n}$, else $Cry^v \pmod{n}$. (She is able to do this.)

**Step 4** Bob verifies (as in the basic Fiat–Shamir protocol).

**Step 5** When $e$ was one, Alice restarts her subliminal protocol, so she restarts at Step 1. (This means she reencrypts $M$, which will give a *different* $C$ and chooses again randomly the $\sqrt{r}$ and a random $v$.) Else (when $e$ was zero) she continues the basic Fiat–Shamir protocol with $\sqrt{t} = \sqrt{r}$. So she sends $r$.

**Step 6** Bob sends to Alice one random bit $e$ (a new one).

**Step 7** Alice follows the basic Fiat–Shamir protocol and answers what was asked. (She is able to do that because she knows $\sqrt{m}$ and $\sqrt{r}$.)

**Step 8** Bob verifies.

In the case that $e = 0$ in Step 2, Daisy will later be able to receive the message $M$ (if the ping-pong protocol was not halted at that stage (after Step 4)). From now on we assume that we are in the case $e = 0$ (in Step 2) and that the basic Fiat–Shamir protocol was not halted after Step 4. It is important to remark that Daisy also knows that $e$ was 0 and so knows in which case she is. Thus Daisy knows that Alice has sent to Bob $Cry^v$ as answer in Step 3. Alice sends then $r$ in Step 5. So Daisy is now able to try to calculate $C$ and consequently she is able to find $M$. Hereto she tries first $v = 0$, if she finds garbage for $M$ then she tries $v = 1$, if she still finds garbage then Alice did not use (at this stage) the subliminal protocol. It is clear that the signature (or authentication) by Alice is necessary.

In [6] the security of the subliminal protocol is proven, after having introduced the term *relative zero-knowledge*. Loosely speaking relative zero-knowledge means that a protocol can be zero-knowledge relative to Charles but not relative to Edward. The following theorems guarantee the security.

**Theorem 1** *It is infeasible for others than the receiver (and evidently the sender) of the subliminal channel to detect the use of the subliminal protocol. This is especially true for the center who issued the passport.*

*Proof.* See [6]. □

So for others it is infeasible to detect if the subliminal channel is used or not. The following theorem tells that there is no danger for Alice that she might reveal a part of her identification secret by using the subliminal channel. Hereto it is sufficient to prove that our *subliminal protocol* is zero-knowledge *relative to the sender Alice.*

**Theorem 2** *If the assumptions used for setting up our subliminal protocol are valid, then our subliminal protocol is zero-knowledge relative to Alice.*

*Proof.* See [6]. □

Let us make a technical remark which is not of practical importance. If there is a collaboration between the center and Alice, then the protocol is not zero-knowledge *relative* to *the entity* formed by Alice and the center. In practice this collaboration is excluded, as we did in our assumptions.

## 4.3 Introducing the subliminal protocol in the general Fiat–Shamir

If one would try to adapt the above subliminal channel (see Section 4.2) trivially to the *general* Fiat–Shamir protocol, the speed would decrease exponentially when $k$ increases. Indeed one could adapt it such that the subliminal part starts only if *all* the $k$ $e_i$ would be zero (see Step 5). This subliminal channel idea has to be rejected because it is completely impractical. So better solutions will be presented.

Two cases now mainly exist. In the first one the passport holder is willing to discuss a secret protocol with the verifier so that the verifier cheats by choosing his $e_i$ such that his subliminal channel becomes easier to build! So the $e_i$ are the output of a secure pseudo-random generator and both, passport holder and verifier know the secret key and seed. This first case is discussed in Section 4.3.1. The second solution can be used if the receiver of the subliminal channel is the eavesdropper and not the verifier. In this case the verifier will probably not collaborate by selecting the $e_i$ in a special way! This second case is discussed in Section 4.3.2.

### 4.3.1 The passport holder sending to the verifier

Let us explain the subliminal protocol which is used during the general Fiat–Shamir protocol. Alice (the passport holder) wants to send the message $M$ to Bob (verifier). Every user, so also Alice use a known number $y$ such that the Jacobi symbol $(y \mid n) = -1$. (Such $y$ can easily be generated in random polynomial time.) This $y$ may even be standard.

**Step 1** Alice decides not to choose $\sqrt{t}$ randomly, but to do the following. Alice calculates the $e_1, e_2, \ldots, e_k$ that Bob will send her in Step 2 (using the common pseudo-random generator). Alice authenticates the message $M$ and encrypts it to obtain $C$. She selects a random bit $v \in \{0,1\}$. She selects a random number (mod $n$). We will call this random number $\sqrt{r}$. She squares it (mod $n$) and multiplies it with $C$, with $y^v$ and with $\prod_{e_i=1} \sqrt{m_i}$ to obtain $Cry^v \prod_{e_i=1} \sqrt{m_i}$ and uses it as $\sqrt{t}$ for the general Fiat–Shamir protocol. She now follows the general Fiat–Shamir protocol, this means she squares $\sqrt{t}$ and sends it to Bob. (In other words she sends $C^2 r^2 y^{2v} \prod_{e_i=1} m_i \pmod{n}$ to Bob.)

**Step 2** Bob calculates $e_1, e_2, \ldots, e_k$ similarly as Alice and sends them to Alice.

**Step 3** Alice answers as in the general Fiat–Shamir protocol, *even if* the $e_i$ that she just has calculated differ from the one that Bob just has sent.

**Step 4** Bob verifies (as in the general Fiat–Shamir protocol).

**Step 5** When the $e_i$ that Alice has calculated in Step 1 do *not* correspond with the $e_i$ that Bob has sent in Step 2, *then* Alice restarts her subliminal protocol, so she restarts at Step 1. This means she reencrypts $M$, which will give a *different* $C$ *from before* and chooses again randomly the $\sqrt{r}$ (and so on). Else (when $e_i$ match) she continues the general Fiat–Shamir protocol with $\sqrt{t} = \sqrt{r}$. So she sends $r$.

**Step 6** Bob sends to Alice random bits, $e_i$.

**Step 7** Alice follows the general Fiat–Shamir protocol and answers what was asked. (She is able to do that because she knows $\sqrt{m_i}$ and $\sqrt{r}$.)

**Step 8** Bob verifies.

In the case that the $e_i$ matched, Bob is able to receive the message $M$. Indeed in that case Alice answers (in Step 3) $Cry^v \prod_{e_i=1} m_i$. Because Bob knows also the $m_i$ and because he received the $r$ in Step 5, he is able to figure out $Cy^v$.

The proof of the security of the last subliminal channel is similar to the one in Section 4.2 (for details see [6]).

*If* Alice *really trusts* Bob, *then* she can double the capacity of her subliminal channel. Hereto it is sufficient that she sends $C^2 \prod_{e_i=1} m_i$ in Step 1 (where $e_i$ is the output of the pseudo-random generator). She can then drop Step 5–8. ***However if Bob does not send the same*** $e_i$ ***in Step 2***, then *Alice gets into real trouble.* Indeed then she has the choice: either to answer, but then she looses some secret about her $\sqrt{m_i}$; or either she can refuse to answer or sending a wrong answer. It is clear that she will have trouble with Bob or with the warden (who tries to catch subliminal channel users). Remark that it can also be a simple misunderstanding due to lack of synchronization of the pseudo-random generators.

We here finally remark that the above subliminal channel could also have been used in the case of the basic Fiat–Shamir scheme, when the passport holder communicates with the verifier. Nevertheless that this last idea is more optimal, the authors didn't want to make the reading of Section 4.2 too complicated by splitting it into two cases.

### 4.3.2 The passport holder communicating with the eavesdropper

The startup and conditions are similar as in Section 4.3.1, *except* that the encrypted message $M$ is intended for Daisy (eavesdropper), and except that the *center of the passport holder has to collaborate partially.* This collaboration exists in choosing $n$ as the product of two primes and the center has to publish a number $z$ which is a quadratic non-residue with Jacobi symbol $(z \mid n) = 1$ ($-1$ is such a number if $n$ is the product of two primes each of the form $4r + 3$). If the center refuses to do this, then the following subliminal channel can still be used (hereto replace $z$ by 1), but the center can detect its use. The subliminal protocol has also to be adapted, because Bob (the verifier) is not aware of the use of the subliminal channel by Alice and Daisy. The authors

found their inspiration for the following subliminal protocol from the use of GF($2^m$) in several factoring algorithms.

**Step 1** Alice decides not to choose $\sqrt{t}$ randomly, but to do the following. Alice authenticates $M$ and encrypts it to obtain $C$. She selects a random bit $v_1 \in \{0,1\}$. She selects a random number (mod $n$), which we will call $\sqrt{r_1}$. She squares it (mod $n$) and multiplies it with $C$ and with $y^{v_1}$ to obtain $Cr_1y^{v_1} \pmod n$ and uses it as $\sqrt{t}$ for the basic Fiat–Shamir protocol, this means $\sqrt{t} = Cr_1y^{v_1} \pmod n$. She now follows the general Fiat–Shamir protocol, this means she squares $\sqrt{t}$ and sends it to Bob.

**Step 2** Bob chooses a (really) random $\mathbf{e}^1 = (e_1^1, \ldots, e_k^1)$ and sends it to Alice (as in the general Fiat–Shamir protocol).

**Step 3** Alice follows the general Fiat–Shamir protocol, so answers. Alice and Daisy each store the binary vector $\mathbf{e}^1$. They each set the number $w = 1$.

**Step 4** Bob verifies (as in the general Fiat–Shamir protocol).

**Step 5** *If* $\mathbf{e}^1$ can be written as $\mathbf{e}^1 = \mathbf{0}$ *or* as $\mathbf{e}^1 \equiv b_2\mathbf{e}^2 + b_3\mathbf{e}^3 + \cdots + b_w\mathbf{e}^w \pmod 2$ (where $b_j$ are binary), *then* go to Step 9, *else* the following happens. Alice and Daisy increase $w$ by 1. Alice selects random bits $v_w$ and $u_w$ and a random number (which we call) $\sqrt{r_w}$ (mod $n$). Alice then sends random bits $r_w^2y^{2v_w}z^{2u_w} \pmod n$ to Bob.

**Step 6** Bob chooses a (really) random $\mathbf{e}^w$.

**Step 7** Alice follows the general Fiat–Shamir protocol, so answers. Alice and Daisy each store the binary vector $\mathbf{e}^w$.

**Step 8** Bob verifies as in the general Fiat–Shamir protocol. *Jump back to Step 5.*

**Step 9** Alice sends to Bob $r_1\prod_{b_j=1} r_j \pmod n$. So now Daisy is able to calculate $C$ and $M$. Indeed Alice has sent $\alpha = Cr_1y^{v_1}\prod\sqrt{m_i^{e_i^1}}$ in Step 3 and has sent $\beta_j = Cr_jy^{v_j}z^{u_j}\prod_i\sqrt{m_i^{e_i^j}}$ in Steps 7. Daisy can now make the product $\alpha\prod_{b_j=1}\beta_j \equiv C\gamma\eta r_1\prod_{b_j=1} r_j \pmod n$ where $\eta \equiv y^{v_1}\prod_{b_j=1} y^{v_j}z^{u_j} \pmod n$

$$\gamma \equiv \prod_i \sqrt{m_i^{e_i^1+\sum_{j=2}^w b_j e_i^j}} \pmod n.$$

Because $e_i^1 + \sum_{j=2}^w b_j e_i^j \equiv 0 \pmod 2$, only powers of $m_i$ are in $\gamma$ and no powers of $\sqrt{m_i}$, so Daisy can calculate $\gamma$ herself and find C. Hereto Daisy has to eavesdrop what Alice has just sent $(r_1\prod_{b_j=1} r_j)$ and has to figure out what $\eta$ is. So Daisy has to try all possible $v_1, v_2, \ldots, v_w$ and all $u_2, \ldots, u_w$, so maximum $k^2$ trials.

**Step 10** The protocol continues as before. This means that $r_1\prod_{b_j=1} r_j$ is treated as $t$. So Bob chooses the next $e_i$ and Alice answers and Bob verifies.

The reader wondering about the problem that Bob (the verifier) can decide to stop in a stage that is not the end of the subliminal protocol, has to take the following into consideration. If Daisy is able to intercept the next verification of Alice's passport (by who so ever) then no problem exists.

Proofs of security can be found in [6].

This subliminal protocol can also be used when the passport holder wants to communicate with the *verifier* knowing the verifier's public key, but having no secret key in common. Although, this last problem can sometimes trivially be avoided. Indeed the Fiat–Shamir scheme does not exclude that the passport verifier sends his $j_i$ under some permutation. If $k \geq 40$ then the number of possible permutations is large enough to send (under encrypted form, using the verifier's public key) the actual secret DES key and seed which will be used. This key and seed could then be used to make the pseudo-random which was required in the subliminal protocol of Section 4.3.1.

## 4.4 Applications

We now discuss applications of our subliminal channels. One example is discussed separately in Section 5.1.3. It is clear that there are extremely dangerous uses of the discussed subliminal channel. It is not the purpose of this paper to help criminals, so the authors restrict themselves. We discuss briefly some examples.

The use by criminals to communicate secretly is a major danger when the Fiat–Shamir protocol would be adapted for passports without modifications. It can also be used by the godfather to communicate in a tamper-free way with the mafia members. Criminals infiltrated in the police can use it to communicate with their gang, to avoid for example that the gang is caught up.

If citizens of $\beta$land are allowed to choose their random themselves, they can ask politic asylum in $\alpha$land, even if the secret police of $\beta$land watches them extremely closely. Hereto it is sufficient to use one of the subliminal protocols using the public key of $\alpha$land, specially published for this purpose. If banks use the Fiat–Shamir protocol then bank-clerks could use it to slip information about the customs of the bank, to a company or gang or state in an undetectable way. Suppose now that a machine is used for checking the identity of the customer of the bank. The programmer of the machine can however use the subliminal channel to leak information in one or the other direction. Industrial espionage could easily be done using this method. A visitor visiting a company has to check in. The one who verifies the visitor's identity can use the subliminal channel. People forced by the secret police of $\beta$land to fly out $\alpha$land against their will can also alert $\alpha$land using the subliminal channel and the public key of $\alpha$land.

By combining the ideas that the verifier can communicate with the passport holder *and* vice-versa, another interaction can be hidden inside the verification interaction. In extreme one can have a zero-knowledge protocol hidden inside another zero-knowledge protocol. For more details see [6].

## 4.5 Efficiency

Let us define the efficiency of a subliminal channel as the rate of the subliminal channel divided by the rate of the main channel. In [6] is proven that the efficiency of the subliminal channels

discussed in Section 4.2, 4.3.1 and 4.3.2 are respectively: $1/2*1/3$, $1/2*1/2$, $1/2*1/(k+2)$. The first $1/2$ always originates from the fact that if the subliminal message is sent hidden in $t$, then Alice can no longer send new subliminal messages when she has to answer, otherwise the verifier and/or warden will detect that.

# 5 How to avoid subliminal channels into the (Feige–)Fiat–Shamir protocol

## 5.1 An attempt

An anonymous reader of a preliminary version [7] of this paper proposed the following solution to overcome the subliminal channel:

> On the subliminal channels, the authors should consider the following. A truly random source will be built into the hardware of a Fiat–Shamir device. This random source would have to be circumvented during execution of the subliminal channel. This modification would be detected by physical inspection at the time.

There are however several *problems* related to this solution (similar to the one already mentioned in [7, p. 14]). The main ones are that

1. the above solution can not be verified,
2. the above technique is not necessarily water-tight. So the passport holder can still send subliminal information,
3. excluding the use of the subliminal channel by the passport holder enables *terrorist sponsoring countries to use it*!

We now discuss these problems in more detail.

### 5.1.1 Problems with verification

The problem is that the solution can not be verified adequately. The Fiat–Shamir protocol (among other applications) is also intended for passport purposes. In such application each country has its own passport center. So the following problem appears: are all countries honest? Indeed will all countries enforce their centers to put a really random source in their hardware Fiat–Shamir passport device, *even if the centers or some organizations sponsored by the government have all advantages* not *to do it*!?

Related to the last questions two possibilities exist. The first one is that the center puts indeed a truly random source in the passports and the second is the opposite. Remark however that as a consequence of the tamperfree aspect, it is impossible to know which is the case. We now discuss these two cases in respectively Section 5.1.2 and Section 5.1.3.

### 5.1.2 Solution not water-tight

Let us now suppose that indeed a truly random source would be used inside the tamperfree passport. Then the passport holder can still communicate. Hereto he uses his passport. When a certain bit of $t$ corresponds with the first bit of his ciphertext, then he sends this $t$ to the verifier, else he does not send it to the verifier. In the last case he answers himself instead. The passport device is not able to see a difference between an interaction with the real verifier or with the passport holder himself who simulates a verification step. The passport holder continues similarly with the next bits of the ciphertext.

The reader could first remark that the warden will observe that an extra device is put in the middle between the passport device and the verifier, in order to have a filter effect on the outcoming $t$. If the passport holder is clever, he avoids detection using, *e.g.*, the following technique. He puts a chip on the surface of the passport device. This chip has to filter out the unwanted $t$, using the described method. He repaints the surface, so that it would have the same appearance. The reader who is now remarking that this will be detected is arguing that documents and/or devices can be made which have an unforgeable appearance. So he is arguing that the actual passports are secure by using unforgeable stamps. But wasn't the motivation for the invention of the Fiat–Shamir scheme not that such unforgeable stamps do not exist?

The reader could also argue that the capacity of the subliminal channel is extremely low. However such channels can also be dangerous [20].

### 5.1.3 The solution helps terrorist sponsoring countries

Suppose now that the center of $\beta$land puts a memory chip in the passport device, instead of a truly random source. The contents of the memory chip corresponds with the $\sqrt{t}$, which will be consecutively used by the passport device. So $\sqrt{t}$ corresponds with consecutive bits stored in the memory chip. The center now claims that they are so friendly to inform the warden what the $t$ are that the device will use. The warden can have the impression that this is indeed a very kindly idea of the center. Indeed the above subliminal channel (see Section 5.1.2) is now no longer possible (without detection), *if* the center does not collaborate with the passport holder. *However* even if it is true that there is *no collaboration*, then the *center itself* is able to *use the subliminal protocol for its own purposes* (or for governmental use).

The center can now indeed abuse the passport(s) by choosing the $\sqrt{t}$ such that $t$ corresponds with the encrypted message $C$ (or a part of it) that the center wants to send! So $\beta$land could use the passport system to transmit information to terrorists who live in $\alpha$land, through their citizens who are not aware of the fraud. The efficiency of this subliminal channel is 50%. If $n$ is about 200 digits, $k = 1$ and the ping-pong protocol is repeated only 30 times, then (using an inefficient source coder) 500 words of information can be sent. *There is no doubt that the identification protocol becomes more dangerous* if the above *"solution" is used*, than without it!

Similar remarks hold for the choice of $e$.

## 5.2 A secure solution

By borrowing an idea from [5] we now propose a secure solution. In this solution we do *not* discuss how to avoid a subliminal message inside $j$ or inside the identity. Our solution guarantees that the following identification ping-pong protocol is subliminal-free (for a proof see [6]).

The main idea (originating from [5]) is to use an *active warden* who acts as an *active* eavesdropper. The active warden has to be *trusted* that he will act exactly as described. Indeed if he wants he can modify the transmissions such that a legitimate identity turns out to be rejected by the verifier. We trust the warden that he will not attempt to influence this rejection. In order to guarantee the subliminal-freeness, the active warden must be trusted not to collaborate with the passport holder and not with the verifier (and not with the center who issued the passport) and trusted that he will not introduce himself a subliminal channel. Full detail of these trust aspects can be found in [6].

The active warden could correspond with a special governmental organization of the country which is visited by Alice ($\alpha$land). So the warden may not correspond with some foreign country, even not the country of citizenship of Alice ($\beta$land). If $\beta$land insists to be active warden (to avoid that Alice asks politic asylum), then a second warden of $\alpha$land is necessary (to avoid abuse by $\beta$land). Our solution allows such a combination. Evidently the solution we present, has only sense if no extra channels exist, which are not watched by the warden. Let us describe it for the general Fiat–Shamir scheme (similar for the Feige–Fiat–Shamir version).

**Step 1** Alice chooses a $\sqrt{t} \pmod n$ and sends $t$ to Bob (through the active warden).

**Step 2** The active warden receives $t$ from Alice and chooses truly random bits $f_1, f_2, \ldots, f_k$ and chooses a truly random $r$. The active warden sends then $t * r^2 * \prod_{f_i=1} m_i^{-1} \pmod n$ to Bob

**Step 3** Bob sends $e_1, e_2, \ldots, e_k$ to Alice (through the active warden).

**Step 4** The active warden receives the bits from Bob and sends $e_1 \oplus f_1, e_2 \oplus f_2, \ldots, e_k \oplus f_k$ to Alice (where $\oplus$ is the exlusive or).

**Step 5** Alice answers, this means she sends

$$\alpha \equiv \sqrt{t} * \prod_{e_i \oplus f_i = 1} \sqrt{m_i} \pmod n$$

to Bob, through the warden.

**Step 6** The active warden receives $\alpha$ and *checks it. If* the answer is wrong, *then* the active warden stops the ping-pong protocol and takes Alice into custody. So using this arrest Alice can communicate one bit to Bob, but the price is high! *Else* (when the answer is correct) the active warden sends

$$\beta \equiv \pm \alpha r \prod_{\overline{e_i} \wedge f_i = 1} m_i^{-1} \pmod n$$

where $\pm$ is chosen randomly by the warden and where $\overline{e_i}$ corresponds with the logic complement of $e_i$ and where $\wedge$ is the logic "and". The reader can easely verify that $\beta$ corresponds with the answer that Bob expects.

**Step 7** Bob verifies that $\beta$ is correct.

The necessary proofs can be found in [6]. *We remark that if Bob has indeed chosen his $e_i$ randomly then the zero-knowledge proof convinces two individuals at the same time.*

# 6 Conclusion

In our paper we came up with several abuses of the (Feige–)Fiat–Shamir protocol. The importance of physical description was analyzed. When the physical description is used appropriately then zero-knowledge techniques are not necessary for secure passports, else some main weaknesses appear, as in the Feige–Fiat–Shamir scheme. These weaknesses can be solved (see [1], [5] and [14]), but these solutions were out of the scope of this paper. The use of subliminal channels inside passports protocols was analyzed and is clearly a major danger. It is infeasible to detect their use. Subliminal channels are also possible and sometimes preventable in other zero-knowledge protocols (see [6]). This can now easely be figured out by the reader who understands all details of the above protocols. This fact allows to think about the fact that "zero-knowledge proofs" and "zero-knowledge about zero-knowledge proofs" are not necessarily forced to be zero-knowledge.

A problem with the (Feige–)Fiat–Shamir protocol and several other identification systems is that eavesdroppers can easely figure out who is travelling and when. They have simply to do the verification on their own.

It becomes clear that the (Feige–)Fiat–Shamir schemes are not the ultimate passport protocols. Other passport protocols having several advantages and one of them also allowing identification over the telephone, are coming up ([5] and [14]). We can expect that in the near future very secure passport systems, which satisfy our current notion about passports and which are doing nothing more or less than identifying and which are more secure and better from all points of view than the ones used today, will appear.

# References

[1] S. Bengio, G. Brassard, Y. Desmedt, C. Goutier, and J-J. Quisquater. Aspects and importance of secure implementations of identification systems. June 1987. Submitted to the Journal of Cryptology.

[2] M. Blum and S. Goldwasser. An efficient probabilistic public–key encryption scheme which hides all partial information. In *Advances in Cryptology. Proc. of Crypto'84 (Lecture Notes in Computer Science 196)*, pages 289–299, Springer–Verlag, New York, 1985. Santa Barbara, August 1984.

[3] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo–random bits. *Siam J. Comput.*, 13(4):850–864, November 1984.

[4] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, February 1981.

[5] Y. Desmedt. A subliminal-free authentication system and its use for identification. In preparation.

[6] Y. Desmedt and C. Goutier. Abuses of zero-knowledge proofs, in particular the Fiat-Shamir identification protocol. In preparation.

[7] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the Fiat–Shamir passport protocol. February 28, 1987. Submitted version of the paper.

[8] Y. Desmedt and J.–J. Quisquater. Public key systems based on the difficulty of tampering (Is there a difference between DES and RSA?). Presented at CRYPTO'86, Santa Barbara, California, U. S. A., August 11–15, 1986, extended abstract will appear in Advances in Cryptology, Proc. of Crypto'86, Lecture Notes in Computer Science, Springer–Verlag, 1987.

[9] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22(6):644–654, November 1976.

[10] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *Proceedings of the Nineteenth ACM Symp. Theory of Computing, STOC*, pages 210 – 217, May 25–27, 1987.

[11] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. August 3–11, 1986. Presented at the International Congress of Mathematicians, ICM 86, Berkeley, California, U.S.A.

[12] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. August 11–15, 1986. Presented at Crypto'86, Santa Barbara, California.

[13] J. Gleick. A new approach to protecting secrets is discovered. *New York Times*, pp. C1 and C3, February 18, 1987.

[14] J.-J. Quisquater. Signatures, identifications et controles d'accès. December 16, 1986. Lecture given at INRIA (France).

[15] J. Saltzer. On digital signatures. *ACM Operating Syst. Rev.*, 12(2):12 – 14, April 1978.

[16] A. Shamir. Interactive identification. March 23–29, 1986. Presented at the Workshop on Algorithms, Randomness and Complexity, Centre International de Rencontres Mathématiques (CIRM), Luminy (Marseille), France.

[17] G. J. Simmons. The prisoners' problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology. Proc. of Crypto 83*, pages 51–67, Plenum Press N.Y., 1984. Santa Barbara, California, August 1983.

[18] G. J. Simmons. The secure subliminal channel (?). In H. C. Williams, editor, *Advances in Cryptology. Proc. of Crypto 85 (Lecture Notes in Computer Science 218)*, pages 33–41, Springer–Verlag, 1986. Santa Barbara, California, August 18–22, 1985.

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

[20] D. Slater. A note on the relationship between covert channels and application verification. *ACM, SIG Security Audit & Control Review*, 5(1):22, 1987.