J. Cryptology (1991) 4: 175–183

Journal of Cryptology

Secure Implementation of Identification Systems[1]

Samy Bengio and Gilles Brassard
Département IRO, Université de Montréal,
Montréal, Québec, Canada H3C 3J7

Yvo G. Desmedt
Department of EE & CS, University of Wisconsin–Milwaukee,
Milwaukee, WI 53201, U.S.A.

Claude Goutier
Centre de calcul, Université de Montréal,
Montréal, Québec, Canada H3C 3J7

Jean-Jacques Quisquater
Département de Génie électrique (FAI), Université de Louvain
B-1348 Louvain-la-Neuve, Belgium

Abstract. In this paper we demonstrate that widely known identification systems, such as the public-file-based Feige–Fiat–Shamir scheme, can be *insecure* if proper care is not taken with their implementation. We suggest possible solutions. On the other hand, identity-based versions of the Feige–Fiat–Shamir scheme are conceptually more complicated than necessary.

Key words. Authentication, Digital signature, EFT, Fake equipment, Faraday cage, Fraud, Identification, Identity card, Zero-knowledge.

1. Introduction

One of the best-known modern identification systems consists of the "zero-knowledge proofs of identity" of Feige, Fiat and Shamir [10], which was presented at several conferences [20], [11], [21], [12], [9]. It was also discussed in several newspapers, e.g., [13]. Identifying a person is a frequently performed operation. A credit card, for example, can be thought of as an identity card. Other examples are drivers' licenses, passports, and cards that are used for granting access to facilities.

[1] Date received: June 23, 1987. Date revised: May 22, 1991. Gilles Brassard's research is supported in part by Canada's NSERC. A part of this research was done while Yvo Desmedt was sponsored by NFWO (the Belgian NSF). A later part was done while he was visiting professor at the Département IRO, Université de Montréal. A part of his research is now supported by NSF Grants NCR-9004879 and NCR-9106327. This research was done while Jean-Jacques Quisquater was at the late Philips Research Laboratory, Belgium. Parts of this research were presented at Crypto '86, Crypto '87, and Securicom '88.

If the protection of the identification system is not adequate, several frauds are possible, such as creating fake identities, copying the identity card of somebody in order to use it later, and so on. In particular, these frauds can be attempted by somebody who has previously participated *or is currently participating* in an authentication protocol as the verifying party.

In fact, Feige, Fiat and Shamir have suggested not one, but two significantly distinct schemes. In one system [10, pp. 85–88], each user chooses a secret key and publishes the corresponding public key in a directory. We refer to this as the *public-file-based* identification system. In the other system [10, pp. 88–89], a trusted authority gives each user a secret key partially based on the user's *physical description* (such as digitized information about the fingerprints, hand geometry, voice print, retinal prints, and so on [23, p. 15]). We refer to this as the *identity-based* identification system. In either system, when someone wishes to establish his identity, he gives a zero-knowledge proof [14] that he knows the secret key, which does not reveal it nor any information that could help a would-be impersonator figuring it out.

In this paper we show that the public-file-based Feige–Fiat–Shamir identification system is *insecure* if additional appropriate care is not taken with its implementation. Moreover, the identity-based Feige–Fiat–Shamir identification system can be simplified considerably, with no loss of security, under the assumptions that the user's physical description cannot be faked, and that either a strong enough digital signature scheme exists or the integrity of an authority-maintained public file can be guaranteed.

The reader should also be aware that Burmester and Desmedt [4] have discovered oversights in the basic Feige–Fiat–Shamir schemes, which make them vulnerable to attacks that are *very simple and easy to mount*. Fortunately, these attacks are obvious to counter once one is aware of their existence. We do not discuss them here.

Before we proceed we should make clear that our intent is *not* to claim that the public-file-based Feige–Fiat–Shamir identification system is fatally flawed. Rather, we wish to point out that one should be aware of possible frauds that can be performed if it is not implemented with sufficient care.

2. Security Problems with the Public-File-Based System

In this section we assume that the physical description of the individual is *not* used in the authentication process. Let us first review the basic template of this identification system. Initially, some parameters are set up by a trusted center, which destroys itself after its task is completed (for instance, the center's purpose is to create an RSA integer whose factorization is unknown to all). After this initialization, any user who wishes to join the system selects a secret key, which we call his SID, and transforms it into a public key, which we call his ID. He registers the latter in a public directory under his name. Whenever he wishes to establish his identity, he proves in zero-knowledge [14] that he knows the SID corresponding to his public ID. This is done in a way that yields no information about the SID. Thus, the person to whom he has just identified has not gained any information that might *subsequently* help him turn around and misrepresent himself to a third party. Of course,

it must be easy to compute the ID from the SID, whereas the reverse process must be computationally infeasible.

In his ICM 86 paper (International Congress of Mathematicians), Shamir claims to describe an identification system "which is provably secure against passive or active attacks if factoring is difficult" [21, p. 1491]. Later, in their SECURICOM 87 paper, Fiat and Shamir claim that "The security of our scheme can be formally proved even under the most adversarial conditions with the sole assumption that factoring large numbers is difficult " [12, p. 149]. Again, in their STOC 87 paper (ACM Symposium on the Theory of Computing), Feige, Fiat and Shamir reiterate that "We describe a novel scheme which is provably secure if factoring is difficult" [9, p. 210]. Similarly, Gleick claims to have quoted Shamir when he wrote in the *New York Times* (concerning the protection of credit cards with this 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" [13]. Despite all this assurance, the public-file-based Feige–Fiat–Shamir identification system is easy to defraud, as we now explain, unless additional care is taken with its implementation. This is ironic because Feige, Fiat and Shamir say about the usual (very insecure) system based on a personal identification number (PIN) that "A sophisticated adversary who cooperates with a dishonest verifier can [...] misrepresent himself successfully [...]" [10, p. 85], which is *precisely* what is going to happen in the fraud we now describe!

2.1. *The Middleperson Attack*

All you need is a secret radio link between two dishonest associates. This attack will be possible because no physical description is used in the public-file-based Feige–Fiat–Shamir system, and the identification process consists solely in one party answering questions asked by the other. In this fraud, four people are involved, two of them (A and D) are *not* aware that the fraud is going on, the other two (B and C) have masterminded the fraud. The purpose of the fraud is to allow C to "prove" to D that he is in fact A. In order to do this, B and C have to wait until A decides to prove his identity to B (and they will not have to wait long if indeed A goes to B's mafia-owned store a million times!). At the same moment, C initiates the identification protocol in order to convince D that he is A. During the identification protocol between C and D, D sends challenges to C. Because C does not really know A's secret, he cannot answer by himself. Instead, C transmits to B the questions coming from D (using the secret radio link), and B asks them to A as he would his own challenges. Unsuspectingly, A answers B's challenges because he thinks that he is authenticating to B. This allows B to communicate the answers back to C, who gives them to D. The whole procedure can be repeated as many times as necessary. At the end, D is convinced that the person in front of him is A. In other words, B and C are simply sitting in the middle. For this reason, we call this fraud the *middleperson attack*. Notice that this fraud has to be performed in real time. Once the interaction between A and B is over, the answers that B has obtained from A are worthless for further use.

This fraud can be compared with someone who plays chess simultaneously against two Chess Grandmasters and wins from one (see p. 75 of [5] or the delightful story *Unicorn Variations* by Zelazny [25]).

2.2. *Other Frauds Related to the Public-File-Based System*

Several other frauds, which further impair the security of the public-file-based Feige–Fiat–Shamir system, can be mounted. Let us mention only a few of them here.

A variant of the above fraud is when A is aware of the fraud and is willing to collaborate with C: each time C has to prove his identity, A gives him the necessary answers. (B has no role in this setting.) Let us illustrate this fraud. Assume that A is willing to help C enter a country. D is the custom officer controlling C's identity. Each time C has to prove "his" identity (in fact A's identity) to D, C communicates questions and answers from A to D and vice versa. A secret radio-link (or more sophisticated techniques) can be used for communicating these questions and answers. The custom officer will allow C to enter the country, because he thinks that A is entering. We call this fraud the *terrorist fraud* because its consequences could be disastrous if C were a terrorist.

Nothing prevents criminals from making fake ID-cards with a "pure" public-file-based identification system because each user is responsible for choosing his own secret key and publishing the corresponding public key in the directory. Thus, any user can produce several secret keys and compute their corresponding public keys. He can publish them together with fake names. Well-known frauds can be used by individuals who have several identities (see [7]). By definition, such frauds are untraceable. An obvious solution is to have an authority control the directory: you have to prove your identity (*not* using the identification protocol of Feige–Fiat–Shamir, of course) in order to be granted one entry in the directory.

More importantly, the owner of an ID should *never* be allowed to know his own SID. Otherwise, he could give his secret key to others, who could then claim to be him. For instance, some businesspeople might wish to "copy" themselves to save time, so that their clones could handle public relations. Even though this fraud was originally suggested [8] in the context of an identity-based system [20], it applies just as well in the more general context considered here. This is similar to the fraud in which a user would deliberately allow his secret key to "leak" in order to deny a previously signed document [19]. To prevent these frauds, the (ID, SID) pairs should be created by a trusted authority, who would enter the ID in the directory, and issue to the user a tamper-proof ID-card that knows the SID. The authority should then erase its own knowledge of the SID (but is the authority really trustworthy?). It must also be infeasible for the user to recompute his SID from the information he has, even with the help of his own card.

Because no physical description is used, hiding one's SID from the owner of the corresponding ID-card is not enough to prevent all frauds in which the owner is a willing party. For instance, the identification card itself can be rented. This allows crimes with perfect alibis to take place, as explained in [7]. If the physical description of a person is not used or not tested adequately, it is very hard to prevent this fraud, unless we are willing to resort to very frequent identification controls, such as in a police state, which would be totally unacceptable in many countries.

Finally, a fraud can occur due to loss or theft of the ID-card. Indeed, as Simmons has pointed out [23], an identification system (which does not check the physical

description of the individual) "is identifying the key rather than the individual". We address this issue in Section 3.2.

2.3. *Abuses of Identification Systems*

In addition to the frauds described above, the Feige–Fiat–Shamir identification systems can be *abused*. This means that they can be used for purposes other than those officially intended. For example, they allow spies to use the identification process to implement an undetectable subliminal channel [22] (a special case of a covert channel [16]). This makes it possible to send secret information in a traffic-analysis-free way. The reader interested in these abuses and how to fight them can find more details in [7].

In this paper we do not discuss abuse-freeness of identification systems. Nevertheless, we wish to point out that the solution we give below to the middleperson attack and the terrorist fraud has the disadvantage that it opens the door very wide to such abuse. In a companion paper we explain how this door can be shut tight [1].

3. Solutions for the Public-File-Based System

The main purpose of this section is to give one possible solution to deal with the middleperson attack and the terrorist fraud. Completely different (and probably more practical) solutions to the middleperson attack were given by Desmedt [6] and independently by Quisquater. More recently, Beth and Desmedt [2] have found two other solutions, which are secure against both the middleperson attack and the terrorist fraud.

Before we get started, it should be pointed out that many people have suggested solving the threats described in Section 2 by use of *mutual* (two-way) identification. The idea is that the individual identifying himself should know the party receiving the identification information. However, this does *not* provide any additional protection against the middleperson attack: challenges and answers can be forwarded back and forth between the dishonest associates.

3.1. *Thwarting the Middleperson Attack and the Terrorist Fraud*

The middleperson attack and the terrorist fraud are made possible only because the conspirators are able to *communicate* via a secret radio link. Therefore, these threats disappear automatically as soon as we prevent communication with the outside world while the identification protocol is in progress. For instance, we could isolate in a Faraday cage[2] the devices participating in the protocol until the identification is completed.

---

[2] Recall that the purpose of a Faraday cage is to block out electromagnetic radiations [24, p. 825]. Actually, this might not be sufficient since other means of communication between fraudulent users could exist (such as ultrasounds). We refer the reader to [1] for a more complete discussion of how to implement what is called there an *identification cage*, that is a cage that prevents (or at least detects) all known means of communication with the outside world. For simplicity, we use ordinary Faraday cages in this paper.

Assume that A wishes to prove his identity to B. For this, A hands his ID-card to B, perhaps after activating it through the use of a PIN (see Section 3.2). Then B puts A's card in a box known as the *interrogation device*, which contains both the hardware and software necessary to handle the mathematical aspects of the identification. The actual protocol takes place between A's ID-card and B's interrogation device after B closes his device's door, which turns it into a Faraday cage. After the protocol is completed (which can be determined by a timer), B opens his device, which informs him of whether or not A's identification is successful. If B is satisfied, he gives back to A his ID-card.

Notice that if B is dishonest, as in the middleperson attack, nothing prevents him from having a fake interrogation device that is *not* a Faraday cage at all. This would allow B's device to transmit information about A's answers to selected challenges. However, this would be useless for B because he would have no one with whom to share such information. Indeed, if C is trying to impersonate A while identifying to D, C's (fake) ID-card is safely within D's Faraday cage, which prevents it from obtaining information from B.

As an additional safeguard, A should verify, after getting his ID-card back from B, that he was handed his genuine card. For this, he could run an identification protocol with his own card. Also, B should check that his interrogation device was not *damaged* by A's ID-card. After all, A's card was perhaps itself a hostile device, capable of drilling a hole in B's Faraday cage or other nasty behaviour. More details along these lines can be found in [1].

3.2. *Protection Against Robbery and Loss of the Identity Card*

The risks of robbery and loss of the identity card are carefully taken into consideration in most designs, and solutions are usually trivial. For instance, if it becomes known that someone's ID-card has been stolen, this card should be blacklisted, as is done currently with credit cards. In order to offer additional protection, the card should only start working after having identified its carrier (for instance through the use of a PIN—a personal identification number). Unfortunately, trying to do this perfectly is like solving a vicious circle.

The use of such a PIN does not avoid more sophisticated attacks. For instance, a clever thief who wishes to steal someone's PIN could replace that person's identity card by a fake, which contains a radio transmitter that will communicate the PIN to the thief when the unsuspecting victim supplies it to the card.

4. Simplification of the Identity-Based System

We now consider the identity-based Feige–Fiat–Shamir identification system. In this section we therefore assume that the physical description of the individual *is* used in the authentication process. Furthermore, we make the assumption that each individual has a unique physical description, which can be checked with 100% accuracy, and which cannot be deceived by a clever impersonator. Otherwise, the protection offered by an identity-based system is not only illusory, but it is downright dangerous if it makes someone believe that he is well protected when in fact

he is not. Clearly, the attacks described in Section 2 apply just as well in the context of an identity-based system if an impersonator is able to mimic the physical description of the person he wishes to impersonate.

Let us first review the identity-based version of the Feige–Fiat–Shamir identification system. In an identity-based scheme, the ID reflects the individual's name, physical description, and perhaps additional information such as his address, social security number, credentials that the authority is granting the individual, and so on. Then the SID is computed by the trusted authority from the ID, thanks to an appropriate trapdoor known only by the authority. When the individual wishes to identify himself, he gives his ID in the clear, which the identifying party can compare with the individual's physical characteristics, and then the individual allows his ID-card to convince *in zero-knowledge* the verifying party's interrogation device that his ID-card knows the SID corresponding to this ID.

The point we wish to make is that, from a conceptual point of view, it is needlessly complicated to use a zero-knowledge protocol when the individual's physical identity can be tested accurately. Indeed, *a public-key system is just as secure* provided that the authority's signature scheme is strong enough. Whenever the individual wishes to identify himself, it is sufficient for him to reveal his (ID, SID) pair in the clear, in order to allow the verifying party to check that the SID is the authority's valid signature of the ID, and that the ID reflects the individual's physical description. Indeed, there is *no point* in keeping secret an SID that can *only* be used by the (unique legitimate) person with matching physical ID! Of course, this public-key identification system is nothing new: according to Simmons [23], it corresponds to the very first practical use of the concepts of public-key cryptography revealed in the open literature [17].

The above paragraph should be taken with a grain of salt. Although the public-key system is conceptually simpler than the Feige–Fiat–Shamir scheme (it hinges on the classic notion of digital signature rather than the fancier notion of zero-knowledge), it would be *less efficient* if the same level of safety were desired. The reason is that this would require the use of a digital signature scheme that is "not existentially forgeable under an adaptive chosen-message attack" [15], and known instances of such schemes are not very practical. Nevertheless, if one is willing to reduce theoretical safety slightly, Rabin's signature scheme [18] (or its Guillou–Quisquater–Simmons variant [3]) could be used. In that case, signature verification would involve a single modular squaring, which would be vastly more efficient than the Feige–Fiat–Shamir scheme, in addition to being conceptually simpler. Moreover, impersonators could not make use of the known weaknesses of Rabin's signature scheme (such as the chosen-text attack) short of a biotechnological revolution (such as creating an individual whose physical description is the square of a chosen number!).

An even simpler public-file-based identification system is possible if each individual has a unique physical description that can be checked accurately and cannot be deceived, *and* if the integrity of the authority-maintained public file can be guaranteed. For each individual that it wishes to register, the authority measures his physical description and creates an entry in the public file certifying the name (and perhaps other relevant information) of whoever measures up to this given

description. Whenever A wishes to prove his identity, he simply says: "Hi! I am A." In order to verify this claim, it is sufficient to look up the ID of A in the public file and compare it with the claimer's physical description. Note that the public file need not be encrypted nor signed (as long as its integrity can be guaranteed, which may perhaps be achieved in practice through digital signatures). For more ideas on this concept, and for means to protect the individual's privacy, read [6].

5. Conclusions

We conclude that the idea [20], [11], [21], [12], [9], [10] of using zero-knowledge protocols for identification purposes is very nice. However, in order to benefit from the marvelous properties of zero-knowledge protocols, a careful implementation is absolutely necessary.

An important aspect of this paper is that it demonstrates a difference between mathematically secure systems and implemented secure systems. A system (or a mathematical part of a system, e.g., a protocol) can be mathematically proven secure, although it is completely insecure when inappropriately implemented. Finally, we conclude that more research is necessary in order to define conditions for secure implementations and in order to obtain mathematical proofs for these conditions.

Observe that as yet nobody has given a formal definition for identification (e.g., none is in [10]). Our paper clearly demonstrates that the formal definition of proof of knowledge is insufficient for this purpose. Hence, no system has ever formally been proven to be a secure identification system.

Acknowledgements

We are grateful to Shimon Even and Louis Guillou for pointing out the analogy between the middleperson attack and the chessmaster scenario (see the end of Subsection 2.1). We also thank Ernie Brickell and the anonymous referees for the considerable time they have spent on this paper.

References

[1] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater, "Aspects and Importance of Secure Implementations of Identification Systems," Manuscript M209, Philips Research Laboratory, Brussels, May 1987; revision available from the authors.

[2] T. Beth and Y. Desmedt, "Identification tokens—or: Solving the chess grandmaster problem," *Proceedings of Crypto '90*, Santa Barbara, California, August 1990, Lecture Notes in Computer Science, Springer-Verlag, Berlin, to appear.

[3] G. Brassard, "How to improve signature schemes," *Proceedings of Eurocrypt '89*, Houthalen, Belgium, April 1989, Lecture Notes in Computer Science, Vol. 434, Springer-Verlag, Berlin, pp. 16–22.

[4] M. V. D. Burmester and Y. G. Desmedt, "Remarks on the soundness of proofs," *Electronics Letters*, **25**(22) (1989), 1509–1511.

[5] J. H. Conway, *On Numbers and Games*, Academic Press, London, 1976.

[6] Y. Desmedt, "Major security problems with the 'unforgeable' (Feige-)Fiat-Shamir proofs of identity and how to overcome them," *Proceedings of Securicom 88*, Paris, March 1988, pp. 147–159.
[7] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the Fiat–Shamir passport protocol," *Proceedings of Crypto '87*, Santa Barbara, California, August 1987, Lecture Notes in Computer Science, Vol. 293, Springer-Verlag, Berlin, pp. 21–39.
[8] Y. Desmedt and J.-J. Quisquater, "Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?)," *Proceedings of Crypto '86*, Santa Barbara, California, August 1986, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, Berlin, pp. 111–117.
[9] U. Feige, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," *Proceedings of 19th ACM Symposium on Theory of Computing*, New York, May 1987, pp. 210–217.
[10] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, **1**(2) (1988), 77–94.
[11] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," *Proceedings of Crypto '86*, Santa Barbara, California, August 1986, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, Berlin, pp. 186–194.
[12] A. Fiat and A. Shamir, "Unforgeable proofs of identity," *Proceedings of Securicom 87*, Paris, March 1987, pp. 147–153.
[13] J. Gleick, "A new approach to protecting secrets is discovered," *New York Times*, pp. C1 and C3, February 18, 1987.
[14] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, **18** (1989), 186–208.
[15] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, **17**(2) (1988), 77–94.
[16] B. W. Lampson, "A note on the confinement problem," *Communications of the ACM*, **16**(10) (1973), 613–615.
[17] P. D. Merillat, "Secure stand-along positive personnel identity verification system (SSA-PPIV)," Technical Report SAND79-0070, Sandia National Laboratories, March 1979.
[18] M. O. Rabin, "Digital signatures and public-key functions as intractable as factorization," Technical Report MIT/LCS/TR-212, Massachusetts Institute of Technology, 1979.
[19] J. Saltzer, "On digital signatures," *ACM Operating Systems Review*, **12**(2) (1978), 12–14.
[20] A. Shamir, "Interactive identification", Presented at the Workshop on Algorithms, Randomness and Complexity, Centre International de Rencontres Mathématiques (CIRM), Luminy, Marseille, March 1986.
[21] A. Shamir, "The search for provably secure identification schemes," *Proceedings of the International Congress of Mathematicians, ICM 86*, Berkeley, California, August 1986, pp. 1488–1495.
[22] G. J. Simmons, "The prisoners' problem and the subliminal channel," *Proceedings of Crypto '83*, Santa Barbara, California, August 1983, Plenum, New York, pp. 51–67.
[23] G. J. Simmons, "A system for verifying user identity and authorization at the point-of-sale or access," *Cryptologia*, **8**(1) (1984), 1–21.
[24] *Webster's Third New International Dictionary of the English Language (Unabridged)*, Merriam, Springfield, Massachusetts, 1971.
[25] R. Zelazny, *Unicorn Variations*, The Amber Corporation, 1982, reprinted by Avon Books, New York, 1987.