IEICE TRANSACTIONS, VOL. E 74, NO. 11 NOVEMBER 1991

PAPER

Proving Identity in Three Moves

Yuliang ZHENG†*, *Nonmember*, Tsutomu MATSUMOTO† *and* Hideki IMAI†, *Members*

SUMMARY A challenge-and-response type identification protocol consists of three moves of messages between a prover and a verifier: Move-1—The prover claims to the verifier that his/her identity is *ID*. Move-2—The verifier challenges the prover with a question related to the *ID*. Move-3—The prover responds with the answer of the question. The verifier accepts the prover iff the answer is correct. The main contribution of this paper is to show that the folklore can be made provably secure under the sole assumption of the existence of one-way functions.

1. Introduction

This paper treats the *identification problem*. The problem can be described in terms of the goals of two sides, provers and verifiers. The goal of a prover is to convince a verifier that his/her identity is indeed the identity he/she claims in such a way that the prover can't be impersonated by the verifier even after he/she proves polynomially many times to the verifier. The goal of a verifier is to accept a prover if and only if the identity of the prover is indeed the identity claimed by him/her. They achieve their goals by exchanging messages back and forth according to a pre-determined *identification protocol*. Clearly, provers' identities should be authenticated by a third party trusted both by provers and by verifiers, and the authentication by the third party should be checkable by verifiers.

In Ref. (4), Fiat and Shamir constructed an elegant identification protocol based on the (supposed) intractability of factorization. The protocol is secure as it is of zero-knowledge. Another property of the protocol is that a verifier behaves in a passive way: all messages he/she sends to a prover are just outcomes of coin flips, i.e., random strings. Fiat and Shamir used that property to transform the protocol into a secure digital signature scheme, simply by substituting a verifier with a cryptographically secure pseudo-random function[4]. Many later proposed identification protocols and signature schemes, such as those of Refs. (1), (6), (8), (10), (11) follow this line.

Manuscript received February 12, 1991.
Manuscript revised May 10, 1991.

† The authors are with the Faculty of Engineering, Yokohama National University, Yokohama-shi, 240 Japan.
* Presently, he is with the Department of Computer Science, University College, the University of New South Wales, Canberra, ACT, 2600, Australia.

Major problems with thus obtained identification protocols include:
(1) They are based on *specific* one-way functions. In particular, almost all of them are *dangerously* based on either of the following two supposed intractable problems: factorization[2],[4],[6],[8] and discrete logarithm[1],[10]. (The protocol in Ref. (11) is based on an NP-complete algebraic problem—the *permuted kernel problem*.) It seems that there is no hope of laying their bases upon an arbitrary one-way function, as they use in an essential way the *trap-doors* or *specific* (*algebraic*) *properties* of the underlying one-way functions.
(2) They are usually very *complex*, requiring many rounds of message exchanges between a prover and a verifier. (See the serial versions of Ref. (1), (2), (4), (6), (8).)

In this paper, we take the "reverse" of the above approach to obtain a simple identification protocol. The following is a bird's-eye view of our approach: Given an *arbitrary* one-way function, we first construct from the function a digital signature scheme that is secure against existential forgery under adaptive chosen message attack, then we adapt the signature scheme into a challenge-and-response type identification protocol that requires only three moves of messages between a prover and a verifier. As we have already mentioned in SUMMARY, the main idea behind the challenge-and-response type identification protocol itself is a folklore in cryptologic research society. The main contribution of this paper is to show a way of transforming the folklore into a provably secure protocol, with the weakest assumption of the existence of any one-way function.

The organization of the remaining part of the paper is as follows. In Sect. 2, we define basic concepts used later. In Sect. 3, we describe our identification protocol in detail. In Sect. 4 we prove that the protocol is secure against conspired dynamic attack. Finally, we give some remarks in Sect. 5.

2. Basic Definitions

This section gives formal definitions for secure identification protocols and digital signature schemes.

We formulate the identification problem in the following way. Denote by $\mathcal{N}$ the set of positive inte-

gers. Let $n \in \mathcal{N}$ be a security parameter which determines the overall security of an identification protocol, the number of users, etc. Consider an organization consisting of users $U_1, U_2, U_3, \cdots, U_{P(n)}$, where P is a polynomial and the computational power of all users is bounded by probabilistic polynomial time. The unique identity associated with U_i is denoted by ID_i, which could include U_i's name, address, affiliation etc. There is also a center C who is trusted by all users in the organization and hence does not conspire with any user.

The computational power of the trusted center C is bounded by probabilistic polynomial time too. One task of C is to check and authenticate each user's identity. The severeness of identity checking may vary from organization to organization. The center C considered here is allowed to be the loosest one—it authenticates a user's identity if only the user's identity differs from all identities which C has already authenticated.

Consider an identification protocol for the organization. A user who follows the identification protocol is called a *good* user, and any other user is called a *bad* user. An *impersonating adversary* A is a group of bad users in the organization who conspire with one another in order to impersonate a good user U_i. The adversary is allowed to participate as a verifier in polynomially many executions of the identification protocol with U_i or any other users as provers. Furthermore, the adversary is allowed to change dynamically by, for example, adding into it new bad users or deleting from it existing bad users. (This implies that the adversary is allowed to attack the trusted center too.) Call such a type of attack *conspired dynamic attack*. It seems that among all conceivable types of attack against an identification protocol, conspired dynamic attack is the strongest. Denote by $\Pr[A, Q(n)]$ the probability that the adversary A succeeds in convincing a good user U_k that A's identity is ID_i (i.e., in impersonating U_i), after participating as a verifier in $Q(n)$ executions of the identification protocol with U_i or any other users as provers. $\Pr[A, Q(n)]$ is computed over the sample space of coin flips that could have been made by the center C, the adversary A, the users U_i and U_k, and all other users. Informally, the identification protocol for the organization is *secure against conspired dynamic attack* if for any impersonating adversary A, the probability $\Pr[A, Q(n)]$ is negligible. More precisely,

Definition 1: An identification protocol is secure against conspired dynamic attack iff for any impersonating adversary A, for any polynomials Q_1 and Q_2, and for all sufficiently large n, $\Pr[A, Q_1(n)] < 1/Q_2(n)$.

Our protocol depends heavily on digital signature schemes. Here we introduce the notion of digital signature schemes secure against existential forgery under adaptive chosen message attack[5]. A signature scheme consists of the following six components:

(1) A security parameter n, which determines the overall security of the scheme, the lengths of messages and signatures, etc.

(2) A set $\mathcal{M}$ of messages to which the signature algorithm may be applied.

(3) A polynomial B_G which bounds the total number of signatures that can be produced with an instance of the signature scheme.

(4) A probabilistic polynomial time key generation algorithm G, which on input 1^n, chooses a pair (PK, SK) of matching public and secret keys from a *key space* $\mathcal{K}_n$ (In this paper, we assume that the size of $\mathcal{K}_n$ *is exponential in* n, and the output of G is randomly and uniformly distributed. The construction of Refs. (7), (9) satisfies the two conditions).

(5) A probabilistic polynomial time signing algorithm SA, which on input PK, SK and $m \in \mathcal{M}$, outputs the signature s of m with respect to PK.

(6) A polynomial time verifying algorithm VA, which given s, m and PK, tests whether or not s is a valid signature of m with respect to PK.

An *adaptive adversary* is a probabilistic polynomial time algorithm M that is allowed to adaptively choose messages and be supplied with signatures. Let Q be a polynomial, and denote by $\Pr[M, Q(n)]$ the probability that, after $Q(n)$ adaptive attacks, the adversary M is able to produce a valid signature for a message that we did not sign for him/her. $\Pr[M, Q(n)]$ is computed over the sample space of coin flips that the key generation algorithm G and the adversary M could have made.

Definition 2: A digital signature scheme is secure against existential forgery under adaptive chosen message attack iff for any adversary M, for any polynomials Q_1 and Q_2 and for all sufficiently large n, $\Pr[M, Q_1(n)] < 1/Q_2(n)$.

From now on, by secure digital signature schemes we always mean those schemes that are secure against existential forgery under adaptive chosen message attack. Notice that secure digital signature schemes can be obtained under the sole assumption that one-way functions exist[7],[9].

3. A 3-Move Identification Protocol

The whole identification procedure is divided into three stages:

(1) The initiation stage,

(2) The registration stage, and

(3) The identification stage.

The first stage will be completed by the trusted center only, and the second by the center too, but with the cooperation of a user. Both the first and the second stages are done once for all.

3. 1 The Initiation Stage

Assume that f is a one-way function. The trusted center constructs from f a secure digital signature scheme, by using any known construction method, such as that of Refs. (7), (9). Let G, SA and VA be the key generation, the signing and the verifying algorithms, respectively. Then the center runs with 1^n as input the algorithm G to obtain a matching pair (PK, SK) for himself. Finally, the center publishes SA, VA and PK while keeping SK in secret.

3. 2 The Registration Stage

When a user U_i wants to use the identification protocol under consideration in proving his/her identity ID_i, he/she presents ID_i to the center. After checking the validity of ID_i the center runs with 1^n as input the algorithm G to obtain a matching pair (PK_i, SK_i) for U_i. Then the center obtains the signature σ_i of $ID_i \| PK_i$ using the center's secret key SK, where $\|$ means concatenation. Finally, the center issues (PK_i, SK_i, σ_i) to U_i. Notice that it is U_i's responsibility to keep SK_i in secret. Also notice that the probability that (PK_i, SK_i) coincides with any previous output of G is negligible, since the size of the key space $\mathcal{K}_n$ is exponentially large and the output of G is randomly and uniformly distributed.

3. 3 The Identification Stage

When the user U_i wants to prove his/her identity to a user U_j, they follow the following 3-move identification protocol. See also Fig. 1.

Move-1: Preparation ($U_i \rightarrow U_j$)

U_i sends (ID_i, PK_i, σ_i) to U_j.

Move-2: Challenge ($U_i \leftarrow U_j$)

U_j checks whether or not σ_i is a valid signature of $ID_i \| PK_i$ with respect to PK. If σ_i is OK, U_j chooses a random message m_r and sends it to U_i. Otherwise U_j stops.

Move-3: Response ($U_i \rightarrow U_j$)

U_i obtains the signature s_r of the message m_r using his/her secret key SK_i, and sends the signature back to U_j. After receiving s_r, U_j tests whether or not s_r is a valid signature of m_r with respect to PK_i, and accepts the user U_i iff s_r is OK.

4. Proof of Security

This section shows that the identification protocol is indeed secure against conspired dynamic attack. Thus no (conspired) bad user(s) can impersonate a good user without being caught out.

Theorem 1: The identification protocol is secure against conspired dynamic attack.

Proof: First of all we note that the theorem should be proved for the case when the center C is the loosest one as described in Sect. 2. Such a center issues a matched public and secret keys to a user if only the user's identity differs from the identities of all previous users to whom matched public and secret keys have been issued.

Now let A be an impersonating adversary, U_i a good user, and Q_1 a polynomial. Obviously the adversary A, after participating as a verifier in $Q_1(n)$ executions of the identification protocol with U_i or any other users as provers, succeeds in convincing a good user U_k that A's identity is ID_i iff A is able to do one of the following two actions. The first action is to "impersonate" the trusted center C, and hence to impersonate *indirectly* the user U_i. And the second action is to impersonate *directly* the user U_i. The probability that A is able to do the first action is

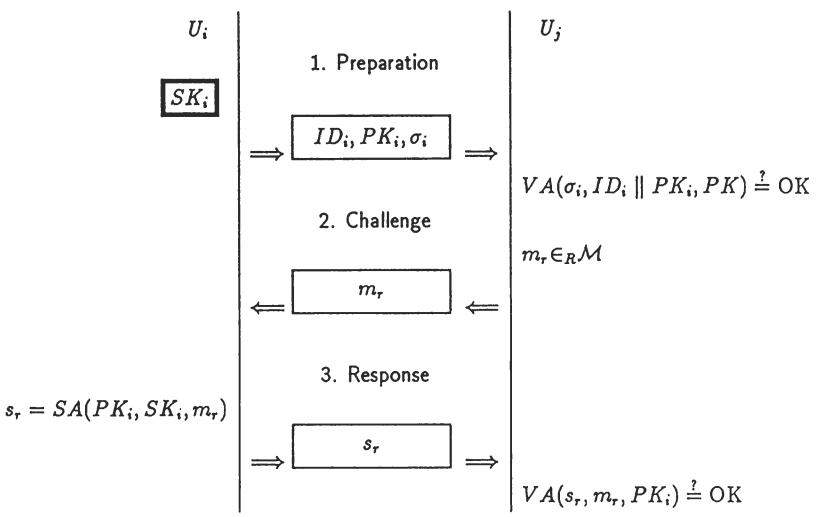


Fig. 1 A 3-Move identification protocol.

bounded by the probability that the following Event-1 occurs.

Event-1: A is able to, without knowing the secret keys SK and SK_i, find a pair $(ID_i \| PK_i', \sigma_i')$ such that $PK_i' \neq PK_i$, σ_i' is a valid signature of $ID_i \| PK_i'$ with respect to PK.

Note that A may know the whole secret key SK_i' matched with PK_i', or some partial information about SK_i', or nothing about SK_i'. The second action can be described as the following Event-2.

Event-2: A is not able to, without knowing the secret keys SK and SK_i, find a valid pair $(ID_i \| PK_i', \sigma_i')$ as described in Event-1, but is able to generate the signature s_r of a random message m_r with respect to PK_i.

Consider the bound of the probability that Event-1 occurs. Since there are only polynomially many users in the organization and the computational power of a user is bounded by probabilistic polynomial time, the computation of the adversary A can be completely simulated by a probabilistic polynomial time algorithm A_1'. Thus Event-1 can be equivalently stated as:

Event-1′: There is a probabilistic polynomial time algorithm A_1' as described above that, without knowing the secret keys SK and SK_i, finds a pair $(ID_i \| PK_i', \sigma_i')$ such that $PK_i' \neq PK_i$, σ_i' is a valid signature of $ID_i \| PK_i'$ with respect to PK.

Now let A_1'' be another probabilistic polynomial time algorithm that simulates the computation of A_1', U_i and U_k. Such an algorithm exists as A_1', U_i and U_k are all probabilistic polynomial time algorithms. Then the probability that Event-1′ occurs, hence the probability that Event-1 occurs, is less than the probability that the following Event-1″ occurs.

Event-1″: There is a probabilistic polynomial time algorithm A_1'' as described above that, without knowing the center's secret key SK, finds a pair $(ID_i \| PK_i', \sigma_i')$ such that $PK_i' \neq PK_i$, σ_i' is a valid signature of $ID_i \| PK_i'$ with respect to PK.

For Event-2, we know, by a similar analysis as above, that there is a probabilistic polynomial time algorithm A_2'' that simulates the computation of A and U_k as well as the computation of the center C except the generation of (PK_i, SK_i) for the user U_i. As a result, the probability that Event-2 occurs is less than the probability that the following Event-2″ occurs.

Event-2″: There is a probabilistic polynomial time algorithm A_2'' as described above that, without knowing the user U_i's secret key SK_i, finds the signature s_r of a random message m_r with respect to PK_i.

By definition, the signature scheme used in the identification protocol is secure against existential forgery under adaptive chosen message attack. This implies that for any polynomial Q_2 and for all sufficiently large $n \in \mathcal{N}$, both the probability that Event-1″ occurs and the probability that Event-2″ occurs are less than $1/2Q_2(n)$. Thus we have

$$\begin{aligned}\Pr[A, Q_1(n)] &\leqq \Pr[\text{Event-1}] + \Pr[\text{Event-2}] \\ &\leqq \Pr[\text{Event-1}''] + \Pr[\text{Event-2}''] \\ &\leqq 1/2Q_2(n) + 1/2Q_2(n) \\ &= 1/Q_2(n).\end{aligned}$$

This completes the proof. □

5. Concluding Remarks

The efficiency of the protocol is determined by that of the digital signature scheme. The only currently available digital signature scheme based on any one-way function is due to Naor and Yung[7], and Rompel[9]. However the scheme is not very efficient. An interesting challenge is to find a really practical signature scheme from any one-way function.

A final remark is that it is difficult, even if not impossible, to apply witness hiding protocols introduced in Ref. (3) to the identification problem formulated in this paper, simply because that it is infeasible for a probabilistic polynomial time algorithm to compute the witness of a user's identity with respect to an arbitrary one-way function.

Acknowledgements

The authors are grateful to Cerecedo Manuel for helpful comments, and to Kouichi Sakurai for fruitful discussions.

References

(1) Beth T.: "A Fiat-Shamir-like authentication protocol for the ElGamal scheme", Advances in Cryptology—EuroCrypt '88, Lecture Notes in Computer Science, **330**, Springer-Verlag, pp. 77-86 (1988).

(2) Feige U., Fiat A. and Shamir A.: "Zero knowledge proofs of identity", Journal of Cryptology, **1**, pp. 77-94 (1989).

(3) Feige U. and Shamir A.: "Witness indistinguishable and witness hiding protocols", Proceedings of the 22-nd ACM Symposium on Theory of Computing, pp. 416-426 (1990).

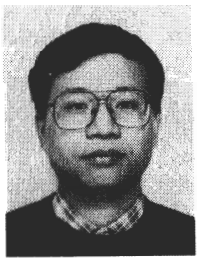
(4) Fiat A. and Shamir A.: "How to prove yourself: practical solutions of identification and signature problems", Advances in Cryptology —Crypto '86, Lecture Notes in Computer Science, **263**, Springer-Verlag, pp. 186-194 (1987).

(5) Goldwassor S., Micali S. and Rivest R.: "A digital signature scheme secure against adaptive chosen-message attacks", SIAM J. Computing, **17**, 2, pp. 281-308 (1988).

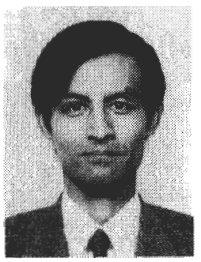
(6) Guillou L. C. and Quisquater J.-J.: "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", Advances in Cryptology—EuroCrypt '88, Lecture Notes in Computer Science, **330**, Springer-Verlag, pp. 123-128 (1988).

(7) Naor M. and Yung M.: "Universal one-way hash functions and their cryptographic applications", Proceedings of the 21-st ACM Symposium on Theory of Computing, pp. 33-43 (1989).

(8) Ohta K. and Okamoto T.: "A modification of the Fiat-Shamir scheme", Advances in Cryptology—Crypto '88, Lecture Notes in Computer Science, **403**, Springer-Verlag, pp. 232-243 (1990).
(9) Rompel J.: "One-way functions are necessary and sufficient for secure signatures", Proceedings of the 22-nd ACM Symposium on Theory of Computing, pp. 387-394 (1990).
(10) Schnorr C. P.: "Efficient identification and signatures for smart cards", Advances in Cryptology—Crypto '89, Lecture Notes in Computer Science, **435**, Springer-Verlag, pp. 239-251 (1990).
(11) Shamir A.: "An efficient identification scheme based on permuted kernels (extended abstract)", Advances in Cryptology—Crypto '89, Lecture Notes in Computer Science, **435**, Springer-Verlag, pp. 606-609 (1990).



Yuliang Zheng was born in Jiangsu, China on February 5, 1962. He received his B. S. degree in computer science from Southeastern University (formerly Nanjing Institute of Technology), Nanjing, China, in 1982, and the M. E. and Ph. D. degrees, both in electrical and computer engineering, from Yokohama National University, Yokohama, Japan, in 1988 and 1991 respectively. From 1982 to 1984 he was with the Guangzhou Research Institute for Communications, Guangzhou (Canton), China, and since February 1991 he has been with the Computer Science Department, University College, University of New South Wales, in Canberra, Australia. His current research interests include computer network security, cryptography, computational complexity theory and information theory. Dr. Zheng is a member of IEEE and IACR.



Tsutomu Matsumoto was born in Maebashi, Japan, on October 20, 1958. He received the B. E. and M. E. degrees in computer eng. both from Yokohama National University, Yokohama, Japan, in 1981 and 1983, respectively, and Ph. D. degree in electronic eng. from the University of Tokyo, Tokyo, Japan, in 1986. From 1986 to 1989, he was a Lecturer for Electrical and Computer Engineering at Yokohama National University. Since 1989, he has been an Associate Professor and is currently working in cryptography, complexity theory, computational mathematics, and their applications to information security. Dr. Matsumoto is a member of ACM, IACR, IEEE, IPSJ.

Hideki Imai was born in Shimane, Japan on May 31, 1943. He received the B. E., M. E. and Ph. D. degrees in electrical engineering from The University of Tokyo in 1966, 1968 and 1971, respectively. He is currently a Professor and a Chairman in the Division of Electrical and Computer Engineering, Yokohama National University. His current research interests include information theory, coding theory, cryptography, and their applications. He is the author of three books and coauthor of several books. Dr. Imai is a member of IEEE, IEE of Japan, IPS of Japan and ITE of Japan.