コンピュータセキュリティ 14－4
(2001. 7. 25)

情報量的安全性に基づく署名方式の構成法について

四方順司* 花岡悟一郎* Yuliang ZHENG† 今井秀樹*

*東京大学生産技術研究所,
153-8505 東京都目黒区駒場 4-6-1
E-mail: {shikata, hanaoka}@imailab.iis.u-tokyo.ac.jp, imai@iis.u-tokyo.ac.jp
†School of Network Computing, Monash University,
McMahons Road, Frankston, Melbourne, VIC 3199, Australia.
E-mail: yuliang.zheng@infotech.monash.edu.au

概要: 最近、著者らは情報量的安全性に基づく署名方式に対しての最も強いと思われる安全性の概念を提案した。本稿では、この安全性の定義をみたすような署名の具体的な構成法を提案する。

キーワード: ディジタル署名, 情報量的安全性に基づく署名方式

Construction Methods for Unconditionally Secure Signature Schemes

Junji SHIKATA* Goichiro HANAOKA* Yuliang ZHENG† Hideki IMAI*

*Institute of Industrial Science, University of Tokyo,
4-6-1 Komaba, Meguro-ku, Tokyo, 153-8505 Japan.
E-mail: {shikata, hanaoka}@imailab.iis.u-tokyo.ac.jp, imai@iis.u-tokyo.ac.jp
†School of Network Computing, Monash University,
McMahons Road, Frankston, Melbourne, VIC 3199, Australia.
E-mail: yuliang.zheng@infotech.monash.edu.au

Abstract: Recently, the authors estabished the strong security notions of unconditionally secure signature schemes. In this paper, we propose construction methods for signature schemes which are provably secure in terms of the strong security notions of unconditionally secure signature schemes.

key words: digital signature scheme, unconditionally secure signature scheme

1 Introduction

Since the discovery of public-key cryptography [11], many significant researches have been reported on digital signature schemes [26][12]. Althogh it is shown in [11] that the trapdoor function paradigm allows to create digital signature schemes in the public-key setting, a number of technical problems arise if digital signatures are implemented using trapdoor functions as suggested in [11]. Thus it is important to have a formal notion of what a secure digital signature scheme is, and to propose a digital signature scheme which is proven to be secure under the formal notion. Current standard security notion was established by Goldwasser, Micali and Rivest [16], and the first digital signature scheme proven to be secure against a very general attack, so-called adaptively chosen message attack has been proposed in [16]. After that, many provable secure digital signature schemes have been proposed so far [3][29][8][14][1].

On the other hand, unconditinally secure signature schemes and authentication codes have been extensively studied so far. The first unconditionally secure signature was proposed by Chaum and Roijakkers [6]. Also, there have been many attempts to modify conventional unconditionally secure authentication codes [15] [37] with the aim of enhancing the codes with extra security-properties, which are close to that of signature schemes. Major extensions of conventional authentication codes include so-called A^2-codes [38] [39] [21] [22] [20], A^3-codes [4] [9] [40] [19] [20] [41] and multi-receiver authentication codes (with dynamic senders) [10] [30] [31] [32] [20]. Recently, the first unconditionally secure signature scheme that admits provably secure transfer of signatures has proposed in [17]. However, all these schemes are proved to be secure against some specific attacks, and some cryptographers may have a question: Is there no attack other than these attacks?;or, is security notion under consideration fully resonable for more general attacks?

Recently, the authors establish the strong security notions of unconditionally secure signature schemes by taking into account the security notions of digital signatures based on public-key cryptography and some desirable requirements for signature schemes in unconditional security setting. However, the problem is whether we can find construction methods for signature schemes that satisfy the strong notions.

In this paper, we actually propose construction methods for signature schemes which are provably secure in terms of the strong security notions of unconditionally secure signature schemes.

2 Security notions of unconditionally secure signature schemes

In [35], the strong security notion of unconditionally secure signature schemes was established. In this section, we describe the model and the security definition which are introduced in [35].

2.1 The model

Definition 1 [35] A signature scheme Π consists of ($\mathcal{U}$, TA, $\mathcal{M}$, $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{A}$, Gen, Sig, Ver):

1. **Notation:**
   - $\mathcal{U} := \{S, V_1, V_2, \ldots, V_n\}$ is a finite set of users, where S is a signer and others $V_i (1 \leq i \leq n)$ are verifiers,
   - TA is a trusted authority,
   - $\mathcal{M} = \{\mathcal{M}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible messages. Here, k is a security parameter and $\mathcal{M}_k \subset \{0,1\}^{l_M(k)}$, where $l_M(k)$ is a polynomial of k,
   - $\mathcal{X} = \{\mathcal{X}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible signing-keys. Here, k is a security parameter and $\mathcal{X}_k \subset \{0,1\}^{l_X(k)}$, where $l_X(k)$ is a polynomial of k,
   - $\mathcal{Y} = \{\mathcal{Y}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible verification-keys. Here, k is a security parameter and $\mathcal{Y}_k \subset \{0,1\}^{l_Y(k)}$, where $l_Y(k)$ is a polynomial of k,
   - $\mathcal{A} = \{\mathcal{A}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible signatures. Here, k is a security parameter and $\mathcal{A}_k \subset \{0,1\}^{l_A(k)}$, where $l_A(k)$ is a polynomial of k,
   - Gen is a key generation algorithm which outputs a signing-key and verification-keys,
   - $Sig : \mathcal{X} \times \mathcal{M} \longrightarrow \mathcal{A}$ is a signing-algorithm,
   - $Ver : \mathcal{M} \times \mathcal{A} \times \mathcal{Y} \longrightarrow \{true, false\}$ is a verification-algorithm.
2. **Key Generation and Distribution by TA:** The TA generates a *signing-key* $x \in \mathcal{X}$ for the signer S, and a *verification-key* $y_{V_i} \in \mathcal{Y}$ for each verifier V_i using the key generation algorithm Gen. Here Gen is a probabilistic algorithm which produce, on input 1^k, where k is a security parameter, keys $(x, y_{V_1}, y_{V_2}, \ldots, y_{V_n})$ of matching signing and verfying keys, where $x \in X_k$ and $y_{V_i} \in Y_k$ for $1 \leq i \leq n$. Then, TA transmits the signing-key x to the signer S and the verification-key y_{V_i} to the verifier V_i via a secure channel. After delivering these keys, the TA may erase the keys $(x, y_{V_1}, y_{V_2}, \ldots, y_{V_n})$ from his memory. The signer keeps secret his signing-key, and each verifier keeps secret his verification-key.
3. **Signature Generation:** For a message $m \in M_k$, the signer S generates a signature $a = Sig(x, m) \in A_k$ by using the signing-key in conjunction with the signing-algorithm. The pair (m, a) is regarded as a signed message. Here, we assume that the signing-algorithm is a deterministic algorithm, but in general it might be a randomized algorithm. If it

is deterministic, for a message m and a signing-key x, the signature $a := Sig(x, m)$ is uniquely determined, while in the case of a randomized algorithm many different signatures can be produced for the same message.

4. **Signature Verification:** On receiving (m, a) from the signer S, a verifier V_j checks whether a is valid by using his verification-key $y_{V_j} \in Y_k$. More precisely, V_j accepts (m, a) as a valid, signed message if and only if $Ver(m, a, y_{V_j}) = true$. Here, we assume that the verification-algorithm is a deterministic algorithm.

Let ψ and ψ' be the number up to which the signer is allowed to generate signatures and the number up to which each verifier is allowed to check received signatures, respectively, and let ω be the number of possible colluders among users. Let $\mathcal{W} := \{W \subset \mathcal{U} | \ |W| \leq \omega\}$. Each element of $\mathcal{W}$ represents a group of possibly collusive users. For a set $\mathcal{T}$ and a non-negative integer t, let $\wp_t^{\mathcal{T}} := \{T \subset \mathcal{T} \mid |T| \leq t\}$ be the family of all subsets of $\mathcal{T}$ whose cardinality are less than or equal to t. Of course, the empty set $\emptyset$ is also contained in $\wp_t^{\mathcal{T}}$.

With notations above, we introduce the security notions in unconditionally secure signature schemes in the sequel.

2.2 Strong security notions

In this subsection, we introduce the security definition described in [35]. To begin with, the most powerful security notion in [35] can be briefly described as follows:

Definition 2 (strong security notion) [35] Let Π be a signature scheme along with the above model. Then, Π is called *secure* if the following requirements are satisfied: it is difficult for an adversary to succeed in *existential acceptance forgery* for any verifier under *adaptive chosen-message and chosen-signature-reaction attack*. Here, the notions of *existential acceptance forgery* and *adaptive chosen-message and chosen-signature-reaction attack* are described as follows: Let V be a verifier. Then,

- existential acceptance forgery: An adversary is able to make a pair of message and signature, that a signer has not legally created and will be accepted by V, but the adversary has little or no control over the signed message which is accepted; and
- adaptive chosen-message and chosen-signature-reaction attack: An adversary is allowed to use the signer as an oracle; the adversary may request signatures of messages which depend on the signer's signing key and he may request signatures of messages which depend on previously obtained signatures or messages. Thus, at any time the adversary can choose some messages that the signer will sign for him, where the messages are chosen except for the target message. In addition, the adversary is allowed to use the verifier V as an oracle; the adversary may request the result whether a pair of message and signature will be accepted by V which depends on the V's verification-key and he may request the result whether a pair of message and signature which depends on previously obtained verification-results. Thus, at any time the adversary can choose some pairs of messages and signatures, where these pairs are chosen except for a target pair of message and signature, and obtain the results whether these pairs are accepted or not by V.

In the sequel, we formally define the above security notions along with our signature model. First, we define *exponentially negligible functions* in order to strictly describe *small probability*. After that we will introduce the security definition with this notation.

Definition 3 (exponentially negligible function) Let $\epsilon(k)$ be a function defined over the positive integers $k \in \boldsymbol{N}$ that takes positive real numbers. Then, $\epsilon(k)$ is called *exponentially negligible* if there exists an integer k_0 and some constant c such that $\epsilon(k) < \frac{c}{2^k}$ for all $k \geq k_0$.

Definition 4 (strong security) [35] Let k be a security parameter and $\epsilon(k)$ an exponentially negligible function. For simplicity, we denote the exponentially negligible function $\epsilon(k)$ by ϵ.

1)

$$P_1^{strong} := \max_{V_j} \max_{x} \max_{(m,a)} \Pr(V_j \text{ accepts } (m,a)) \leq \epsilon, \quad (1)$$

where V_j runs over $\mathcal{U} - \{S\}$, x runs over $\mathcal{X}_k$ and (m, a) runs over $\mathcal{M}_k \times \mathcal{A}_k$ satisfying $a \neq Sig(x, m)$.

2) For $W \in \mathcal{W}$ such that $V_j, S \notin W$, we define $P_2^{strong}(V_j, W)$ as

$$P_2^{strong}(V_j, W) := \max_{y_W} \max_{M_1 = \{(m,a)\} \in \wp_{\psi}^{\mathcal{M}_k \times \mathcal{A}_k}} \max_{M_2 = \{(m',a')\} \in \wp_{\psi'-1}^{\mathcal{M}_k \times \mathcal{A}_k}} \max_{(m'',a'')} \Pr(V_j \text{ accepts } (m'', a'') \mid y_W, M_1, M_2, \{Ver(m', a', y_{V_j})\}_{(m',a') \in M_2})$$

where M_1 is taken over $\wp_{\psi}^{\mathcal{M}_k \times \mathcal{A}_k}$ such that any element of M_1 is a valid signed message; M_2 is taken over $\wp_{\psi'-1}^{\mathcal{M}_k \times \mathcal{A}_k}$; and (m'', a'') runs over $\mathcal{M}_k \times \mathcal{A}_k$ such that $(m'', a'') \notin M_1$ and $(m'', a'') \notin M_2$. Note that the condition $(m'', a'') \notin M_1$ implies the cases: $m'' \neq m$; or $m'' = m$ and $a'' \neq a$ for $(m, a) \in M_1$. Similarly, we note that $(m'', a'') \notin M_2$ implies the cases: $m'' \neq m'$; or $m'' = m'$ and $a'' \neq a'$ for $(m', a') \in M_2$. Then, we define

$$P_2^{strong} := \max_{V_j, W} P_2^{strong}(V_j, W),$$

and we require

$$P_2^{strong} \leq \epsilon. \quad (2)$$

3) For $W \in \mathcal{W}$ such that $V_j \notin W$ and $S \in W$, we define $P_3^{strong}(V_j, W)$ as

$$P_3^{strong}(V_j, W) := \max_x \max_{y_{W-\{S\}}} \max_{M=\{(m,a)\} \in \wp_{\psi'-1}^{\mathcal{M}_k \times \mathcal{A}_k}} \max_{(m',a')} \Pr(V_j \text{ accepts } (m',a') \mid x, y_{W-\{S\}}, M, \{Ver(m,a,y_{V_j})\}_{(m,a)\in M})$$

where $M = \{(m,a)\}$ is taken over $\wp_{\psi'-1}^{\mathcal{M}_k \times \mathcal{A}_k}$ such that any element of M is invalid; and $(m',a') \in \mathcal{M}_k \times \mathcal{A}_k$ runs over invalid signed messages such that $(m',a') \notin M$. We define

$$P_3^{strong} := \max_{V_j, W} P_3^{strong}(V_j, W).$$

Then, we require

$$P_3^{strong} \leq \epsilon. \quad (3)$$

If a signature scheme Π satisfies the formulae (1), (2) and (3), Π is called $(n, \omega, \psi, \psi', \epsilon)$-*secure*.

3 Construction

In this section we propose a construction method for signature schemes which are secure in terms of our strong security notions. In the following, we propose a construction of key generation algorithm, *Gen*, signing algorithm, *Sig*, and verification algorithm, *Ver* along with our signature model (see Section 2.1). In the sequel, we use the notations introduced in Section 2.

- **Key Generation Algorithm**: The key generation algorithm, *Gen*, which, on input 1^k, picks a k-bit prime power q, constructs a finite field $\boldsymbol{F}_q$ with q elements. It also uniformly at random $2n$ elements $v_1^{(1)}, v_1^{(2)}, v_2^{(1)}, v_2^{(2)}, \ldots, v_n^{(1)}, v_n^{(2)}$ in ${\boldsymbol{F}_q}^{\omega+\psi'-1}$ for verifiers $V_1, V_2, \ldots, V_n$, respectively, and constructs two polynomials $F_d(Y_1, Y_2, \ldots, Y_{\omega+\psi'-1}, Z)$ $(d = 1, 2)$ over $\boldsymbol{F}_q$ with $\omega + \psi'$ variables $Y_1, Y_2, \ldots, Y_{\omega+\psi'-1}, Z$ as follows:

$$F_d(Y_1, \ldots, Y_{\omega+\psi'-1}, Z) = \sum_{i=1}^{\omega+\psi'-1} \sum_{j=0}^{\psi} a_{ij}^{(d)} Y_i Z^j + \sum_{j=0}^{\psi} a_{0j}^{(d)} Z^j \ (d = 1, 2),$$

where the coefficients $a_{ij}^{(d)}$ are chosen uniformly at random from $\boldsymbol{F}_q$. Then, a signing key for the signer S is $x := (F_1(Y_1, \ldots, Y_{\omega+\psi'-1}, Z), F_2(Y_1, \ldots, Y_{\omega+\psi'-1}, Z))$ and a verification-key for the verifier V_i is $y_{V_i} := (v_i^{(1)}, v_i^{(2)}, F_1(v_i^{(1)}, Z), F_2(v_i^{(2)}, Z))$ for $i = 1, 2, \ldots, n$. The algorithm *Gen* returns $(\boldsymbol{F}_q, x, y_1, y_2, \ldots, y_n)$.

In the sequel, we assume that $\mathcal{M}_k \subset \boldsymbol{F}_q$.

- **Signing Algorithm**: The signing algorithm, *Sig*, which, on input, the signing-key $x = (F_1(Y_1, \ldots, Y_{\omega+\psi'-1}, Z), F_2(Y_1, \ldots, Y_{\omega+\psi'-1}, Z))$ and a message $m (\in \boldsymbol{F}_q)$, returns a signature $a := (F_1(Y_1, \ldots, Y_{\omega+\psi'-1}, m), F_2(Y_1, \ldots, Y_{\omega+\psi'-1}, m))$.
- **Verification Algorithm**: The verification algorithm, *Ver*, which, on input (m, a, y_{V_i}), where $a = (F_1(Y_1, \ldots, Y_{\omega+\psi'-1}, m), F_2(Y_1, \ldots, Y_{\omega+\psi'-1}, m))$ and $y_{V_i} = (v_i^{(1)}, v_i^{(2)}, F_1(v_i^{(1)}, Z), F_2(v_i^{(2)}, Z))$, computes evaluation values $r_1^{(1)}, r_1^{(2)}, r_2^{(1)}, r_2^{(2)}$ as follows:

$$r_1^{(d)} := (F_d(Y_1, \ldots, Y_{\omega+\psi'-1}, m))|_{(Y_1,\ldots,Y_{\omega+\psi'-1})=v_i^{(d)}}$$

$$r_2^{(d)} := F_d(v_i^{(d)}, Z)|_{Z=m} \quad (d = 1, 2).$$

Then, *Ver* returns *true* if $r_1^{(d)} = r_2^{(d)}$ $(d = 1, 2)$, and *false* otherwise.

The following theorem proves the security of the above construction in terms of our strong security notions.

Theorem 1 *The above construction results in* $(n, \omega, \psi, \psi', \frac{1}{q})$-*secure signature schemes.*

The above construction method can be modified slightly, resulting in yet another $(n, \omega, \psi, \psi', \frac{1}{q})$-secure signature scheme.

Theorem 2 *In the above construction of the key generation algorithm, the following modification leads to* $(n, \omega, \psi, \psi', \frac{1}{q})$-*secure signature scheme: For* $d = 1, 2$, *instead of choosing randomly,* n *elements* $v_1^{(d)}, \ldots, v_n^{(d)} \in {\boldsymbol{F}_q}^{\omega+\psi'-1}$ *are chosen such that for any* $\omega + 1$ *vectors*

$$v_{i_1}^{(d)} = (v_{1,i_1}^{(d)}, \ldots, v_{\omega+\psi'-1,i_1}^{(d)}), \ldots,$$
$$v_{i_{\omega+1}}^{(d)} = (v_{1,i_{\omega+1}}^{(d)}, \ldots, v_{\omega+\psi'-1,i_{\omega+1}}^{(d)}),$$

the $\omega + 1$ *new vectors* $(1, v_{1,i_1}^{(d)}, \ldots, v_{\omega+\psi'-1,i_1}^{(d)}), \ldots, (1, v_{1,i_{\omega+1}}^{(d)}, \ldots, v_{\omega+\psi'-1,i_{\omega+1}}^{(d)})$ *are linearly independent.*

4 Some remarks

The signature model which we introduced in the previous paper [35] deals with *signature schemes with appendix*, and the strong security notion was established based on this signature model. However, we can easily modify this model so that we obtain the model of *signature schemes with non-appendix (signature schemes with message recovery)*, which is often discussed in the context of public-key based signature schemes [3] [1] [24] [25], and that we can establish the strong security notion for the model, as well.

In this paper, we have proposed construction methods, using multivariate polynomials over finite fields, for the model of signature schemes with appendix in terms of the strong security notion. It would also be possible to propose construction methods, using finite geometery, for the model of signature schemes with non-appendix (signature schemes with message recovery) in terms of the strong security notion (cf. [34]). The detailed will be presented in a full paper [36].

5 Conclusion

Recently, the authors estabished the strong security notions of unconditionally secure signature schemes [35]. In this paper, we have proposed construction methods for signature schemes which are provably secure in terms of the strong security notions of unconditionally secure signature schemes.

References

[1] M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm", Advances in Cryptology - ASIACRYPT'99, Lecture Notes in Computer Science, vol.1716, pp.378-389, Springer-Verlag, 1999.

[2] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols", Proc. of the First ACM Conference on Computer and Communications Security, ACM Press, pp. 1993.

[3] M. Bellare and P. Rogaway, "The exact security of digital signatures - How to sign with RSA and Rabin", Proc. of Eurocrypt'96, LNCS 1070, Springer-Verlag, 1996.

[4] E. F. Brickell and D. R. Stinson, "Authentication codes with multiple arbiters," Proc. of Eurocrypt'88, LNCS 330, Springer-Verlag, pp.51-55, 1988.

[5] D. Chaum and H. van Antwerpen, "Undeniable signatures", Proc. of Crypto'89, Springer-verlag, pp. 212-216, 1990.

[6] D. Chaum and S. Roijakkers, "Unconditionally secure digital signatures," Proc. of CRYPTO'90, LNCS 537, Springer-Verlag, pp.206-215, 1990.

[7] D. Chaum, E. Heijst and B. Pfitzmann, "Cryptographically strong undeniable signatures, unconditionally secure for the signer," Proc. of CRYPTO'91, LNCS 576, Springer-Verlag, pp.470-484, 1991.

[8] R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption", Proc. of the 6th ACM Conference in Computer and Communication Security, 1999.

[9] Y. Desmedt and M. Yung, "Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attack," Proc. of CRYPTO'90, LNCS 537, Springer-Verlag, pp.177-188, 1990.

[10] Y. Desmedt, Y. Frankel and M. Yung, "Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback," Proc. of IEEE Infocom'92, pp.2045-2054, 1992.

[11] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory 22, 6, pp. 644-654, 1976.

[12] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. on Inform. Theory, IT-31, 4, pp.469-472, 1985.

[13] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," Proc. of CRYPTO'86, LNCS 263, Springer-Verlag, pp.186-194, 1986.

[14] R. Gennaro, S. Halevi, and T. Rabin "Secure hash-and-sign signatures without the random oracle", Advances in Cryptology - EOROCRYPT'99, Lecture Notes in Computer Science, vol.1592, pp.123-139, Springer-Verlag, 1999.

[15] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, "Codes which detect deception," Bell System Technical Journal, 53, pp.405-425, 1974.

[16] S. Goldwasser, S. Micali and R. Rivest, "A degital signature scheme secure against adaptive chosen message attacks", SIAM J. Comput. 17, 2, pp. 281-308, 1988.

[17] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Unconditionally secure digital signature schemes admitting transferability", preprint, Proc. of ASIACRYPT 2000, LNCS 1976, Springer-Verlag, 2000.

[18] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Unconditionally secure digital signature schemes admitting transferability", a full paper of [17], 2001.

[19] T. Johansson, "Lower bounds on the probability of deception in authentication with arbitration", IEEE Trans. Inform. Theory, IT-40, 5, pp.1573-1585, 1994.

[20] T. Johansson, "Further results on asymmetric authentication schemes," Information and Computation, 151, pp.100-133, 1999.

[21] K. Kurosawa, "New bound on authentication code with arbitration," Proc. of CRYPTO'94, LNCS 839, Springer-Verlag, pp.140-149, 1994.

[22] K. Kurosawa and S. Obana, "Combinatorial bounds for authentication codes with arbitration," Proc. of Eurocrypt'95, LNCS 921, Springer-Verlag, pp.289-300, 1995.

[23] K. Kurosawa and S. Obana, "Characterization of (k, n) multi-receiver authentication", Proc. of Information, Security and Privacy, ACISP'97, LNCS 1270, Springer-Verlag, pp.204-215, 1997.

[24] K. Nyberg and R. Rueppel, "A new signature scheme based on the DSA giving message recovery", 1st ACM Conference on Computer and Communications Security, pp.58-61, ACM Press, 1993.

[25] K. Nyberg and R. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", Designs, Codes and Cryptography, 7 (1996), pp.61-81.

[26] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," Communication of the ACM, vol.21, no.2, pp.120-126, 1978.

[27] J. Rompel, "One-way functions are necessary and sufficient for secure signature", Proc. of STOC, pp. 387-394, 1990.

[28] B. Pfitzmann, "Sorting out signature schemes", Proc. of the First ACM Conference on Computer and Communications Security, ACM Press, pp.74-86, 1993.

[29] D. Pointcheval and J. Stern, "Secirity proofs for signature schemes", Proc. of Eorocrypt'96, LNCS 1070, Springer-Verlag, 1996.

[30] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," Proc. of Eurocrypt'98, LNCS 1403, pp.527-541, 1998.

[31] R. Safavi-Naini and H. Wang, "Broadcast authentication in group communication," Proc. of Asiacrypt'99, LNCS 1716, Springer-Verlag, pp.399-411, 1999.

[32] R. Safavi-Naini and H. Wang, "Multireceiver authentication codes: models, bounds, constructions and extensions," Information and Computation, 151, pp.148-172, 1999.

[33] R. Safavi-Naini and H. Wang, "A^3-codes under collusion attacks" Proc. of Asiacrypt'99, LNCS 1716, Springer-Verlag, pp.390-398, 1999.

[34] J.Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Further results on unconditionally secure signature schemes with transferability", Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS 2001), Oiso, Japan, January 23-26, 2001.

[35] J.Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Security notions of unconditionally secure signature schemes", Technical Report of IEICE, ISEC, May, 2001.

[36] J.Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Security notions of unconditionally secure signature schemes", a full paper, in preparation.

[37] G. J. Simmons, "Authentication theory/coding theory," Proc. of CRYPTO'84, LNCS 196, Springer-Verlag, pp.411-431, 1984.

[38] G. J. Simmons, "Message authentication with arbitration of transmitter/ receiver disputes," Proc. of Eurocyrpt'87, Springer-Verlag, pp.151-165, 1987.

[39] G. J. Simmons, "A Cartesian construction for unconditionally secure authentication codes that permit arbitration," Journal of Cryptology, 2, pp.77-104, 1990.

[40] R. Taylor, "Near optimal unconditionally secure authentication," Proc. of Eurocyrpt'94, LNCS 950, Springer-Verlag, pp.244-253, 1994.

[41] Y. Wang and R. Safavi-Naini, "A^3-codes under collusion attacks," Proc. of Asiacrypt'99, LNCS 1716, Springer-Verlag, pp.390-398, 1999.