Josai Mathematical Monographs
vol. 8 (2015), pp. 115-133

Information-Theoretically Secure Blind Authentication Codes without Verifier's Secret Keys *

Noriyasu TAKEI, Yohei WATANABE and Junji SHIKATA

Abstract. In modern cryptography, information-theoretic security is formalized by means of some probability (e.g., success probability of adversary's guessing) or some information-theoretic measure (e.g., Shannon entropy), and the study on cryptographic protocols with information-theoretic security is one of effective applications of the probability theory, statistics, and information theory. In this paper, we study the blind authentication code (BA-code), a kind of information-theoretically secure authentication protocols, in which verifier's secret keys are not required. For realizing it, we utilize a unidirectional low-bandwidth auxiliary channel which is called a *manual channel*. Specifically, in this paper we propose a model, a security definition, and a construction of BA-codes in the manual channel model. Furthermore, we consider BA-codes in other models, i.e., the noisy channel model and the bounded storage model, in which no verifier's secret key is required.

1. Introduction

1.1. Background and Related Works

In modern cryptography, there are two kinds of security settings, *computational security* and *information-theoretic security* (a.k.a. *unconditional security*). The former is based on the assumption of difficulty of computationally hard problems such as the integer factoring problem or the discrete logarithm problem in finite fields or elliptic curves. On the other hand, in general, the latter is formalized by means of some information-theoretic measure (e.g., Shannon entropy) or some probability (e.g., success probability of adversary's guessing), and it intends to represent the security which is guaranteed against the adversary having unlimited (i.e., infinite) computational resources. In particular, the security of information-theoretically secure authentication protocols, which are dealt with in this paper, is formalized and analyzed by success probability of the best strategy of adversary's attacks. In this sense, the study on cryptographic protocols with information-theoretic security is one of effective applications of the probability theory, statistics, and information theory.

The blind signature scheme is first introduced by Chaum [**2**]. Blind signature schemes allow a user to obtain a valid signature for a message from a signer such

* The material in this paper was presented in part at the 3rd International Symposium on Engineering, Energy and Environment (3rd ISEEE), Bangkok, Thailand, November, 2013.

that the message is kept secret for the signer. Therefore, it achieves to protect user's privacy, and can be used for electronic voting and electronic cash schemes. In [**10**], Pointcheval and Stern proposed the first provably secure blind signature schemes by assuming ideal hash functions, which is often called the random oracles. Furthermore, Juels et al. [**6**] first proposed blind signature schemes without the random oracles. In the information-theoretic security setting, Hara et al. [**5**] first studied information-theoretically secure blind signature schemes.

On the other hand, Pinkas [**9**] first mentioned the idea of a blind message authentication code (blind MAC), which is specific to the shared key (secret key) setting, whereas blind signature schemes are specific to the public key setting. Hara et al. [**4**] also proposed blind MAC in the information-theoretic security setting, which is called the *blind authentication code* (BA-code for short). The model of BA-codes is similar to that of information-theoretically secure blind signature schemes [**5**] except that BA-codes are designed such that only a single verifier can check the validity of an authenticated message.

In [**13**], Vaudenay formalized a realistic communication model for message authentication, in which the sender and the receiver having no shared secret are connected by both a bidirectional insecure channel and a unidirectional low-bandwidth auxiliary channel. The low-bandwidth auxiliary channel enables the sender to *manually* authenticate one short string to the receiver. In the channel, the adversary cannot modify the short string, however, he can still read it, delay it, and remove it. In [**8**], Naor et al. formally showed that authentication codes (A-codes for short) could be constructed in this model without any secret information. They refer to the auxiliary channel as the *manual channel*, and to this communication model as the *manual channel model* (MCM for short). In recent years, the MCM is becoming popular in real-world scenarios, for example, in a scenario where a person connects a new DVD player to his home wireless network: Having him read a short string on the display of the DVD player and type it on a PC's keyboard constitutes a manual authentication channel from the DVD player to the PC. This model is also suited to connect the two devices in a wireless network such as Wireless USB and Bluetooth.

1.2. Our Contribution

In information-theoretically secure cryptographic protocols including BA-codes [**4**] and blind signature schemes [**5**], all entities enrolled in the protocols need to have secret keys, in general. For realizing it, it is often assumed that there is a trusted authority which generates secret keys of entities and securely distributes the keys to corresponding entities. This model is often called *a trusted initializer model* (TI model for short) [**11**]. However, the smaller the number of entities who need secret keys in the protocol becomes, the more practical the cryptographic protocol becomes, since generating and distributing secret keys in a secure way is not an easy task in general. On the other hand, as mentioned above, we can realize

A-codes without any shared secret information (i.e., without the presence of TI) in the MCM.

The goal of this paper is to study BA-codes in which the number of entities who need secret keys is less than that of the BA-codes in the TI model [**4**]. Specifically, based on the idea of A-codes in the MCM, we study BA-codes in which a verifier can check the validity of any authenticated message without his secret key by using A-codes in the MCM. Since a verifier needs no secret key, it enables a user to arbitrarily select a verifier during the protocol, i.e., not necessary to determine a verifier before the protocol starts. This property is useful in real-world applications. For example, we consider electronic cash as application of BA-codes in the MCM. In that case, the user is a customer, the signer is a bank, and a verifier is a store. Then, a customer can select a store at any time in which he will use the electronic cash authenticated by the bank, and this situation is more convenient for customers in the real world.

In this paper, we propose a model and a security definition of BA-codes in the MCM. In addition, we provide a construction of BA-codes in the MCM, and we show our construction satisfies our security definition. Furthermore, we consider its extension: Based on the idea of our construction, we can obtain a generic construction of BA-codes from any unconditionally secure commitment scheme and any A-code with no secret keys in a certain model, i.e., A-codes in the manual channel model (MCM), A-codes in the noisy channel model (NCM) [**14**], and A-codes in the bounded storage model (BSM) [**7**].

The rest of this paper is organized as follows. In Section 2, we survey authentication protocols with information-theoretic security: A-codes and BA-codes in the TI model, A-codes in the MCM. In Section 3, we propose a model, a security definition, and a construction of BA-codes in the MCM. Furthermore, we consider several extension of our results. Finally, in Section 4, we give concluding remarks of the paper.

2. Information-Theoretically Secure Authentication Protocols

In this section, we survey information-theoretically secure authentication protocols. In the following, we assume the trusted initializer model (TI model) [**11**] for each protocol, if not otherwise mentioned.

2.1. Authentication Code

Authenticity (or integrity) is one of the fundamental and important cryptographic functions, and authentication/signature schemes are usually used for providing this function. In particular, an authentication code (A-code for short) is the traditional authentication scheme with information-theoretic security. The A-code was originally proposed by Gilbert, McWilliams and Sloan [**3**], and later developed by Simmons [**12**].

In A-codes, there are three entities, a sender S, a receiver R and a trusted initializer TI. A-codes are executed as follows. TI generates and distributes secret keys on behalf of S and R. The sender S generates an authenticator for a message by using his secret key. In the model of A-codes (and all authentication protocols dealt with in this paper), a pair of messages and authenticators is regarded as an authenticated message. Then, S sends the authenticated message to the receiver R over an insecure channel. Then, R checks the validity of the authenticated message by using his secret key. The formal model of A-codes is given as follows.

DEFINITION 1 (A-CODE). *An authentication code (A-code for short) Φ involves three entities, TI, S and R, and consists of a three-tuple of algorithms (Gen, Auth, Ver) with three finite sets, M, Σ and E, where all of algorithms except Gen are deterministic. Φ is executed with three phases as follows.*

- ***Notation.***
    - *Entities: TI is a trusted initializer, S is a sender, and R is a receiver.*
    - *Sets: M is a set of possible messages, Σ is a set of possible authenticators, and E is a set of possible secret keys.*
    - *Algorithms: Gen is a key generation algorithm which takes a security parameter as input and outputs secret keys for S and R. Auth: $M \times E \rightarrow \Sigma$ is an authentication algorithm and Ver: $M \times \Sigma \times E \rightarrow \{true, false\}$ is a verification algorithm.*

1. ***Key Generation and Distribution by TI.*** *TI generates a secret key $e \in E$ for S and R by using Gen. After distributing the key to S and R over secure channels, respectively, TI deletes the key from his memory. Each of S and R keeps his own secret key secret.*

2. ***Authenticator Generation.*** *S generates an authenticator $\sigma := Auth(m, e) \in \Sigma$ for $m \in M$ by using his secret key e. Then, S sends the authenticated message (m, σ) to R over an insecure channel.*

3. ***Verification.*** *On receiving (m, σ) from S, R checks the validity of (m, σ) by using his secret key e. More precisely, if $Ver(e, (m, \sigma)) = true$ then R accepts (m, σ) as valid, and rejects it otherwise.*

In the above definition, we require correctness, i.e., for all possible $e \in E$ and $m \in M$, it holds that $Ver(e, (m, Auth(m, e))) = true$.

In A-codes, for simplicity we assume the one-time model where it is allowed for the sender to generate an authenticator and to transmit an authenticated message only once; and the receiver is allowed to verify an authenticated message at most one time.

The security of A-codes is defined as the security against the following two types of attacks.

1) Impersonation attack: An adversary tries to impersonate the sender S by inserting an authenticated message into the channel between S and R, and he expects that it will be accepted as valid by R.

2) Substitution attack: An adversary tries to replace an authenticated message generated by S with a fraudulent authenticated message, and he expects that it will be accepted as valid by R.

In the impersonation attack, the computationally unbounded adversary selects a message with his best strategy such that the probability that it is accepted as valid by R becomes to be maximum; and in the substitution attack, the computationally unbounded adversary selects a fraudulent authenticated message with his best strategy such that it is accepted as valid by R becomes to be maximum. Therefore, the security formalization is given in such a way that the success probability that R accepts a fraudulent authenticated message created by the adversary is small enough. More precisely, the security of A-codes is formally given as follows.

Definition 2 (Security). *Let Φ be an A-code. Then, Φ is said to be ϵ-secure, if* $\max\{P_{\Phi,I}, P_{\Phi,S}\} \leq \epsilon$*, where $P_{\Phi,I}$ and $P_{\Phi,S}$ are defined as follows.*

1) ***Impersonation attack:*** *The adversary tries to generate a fraudulent authenticated message (m, σ) that will be accepted by the receiver R. The success probability of this attack denoted by $P_{\Phi,I}$ is defined as*

$$P_{\Phi,I} := \max_{(m,\sigma)} \Pr(R \text{ accepts } (m,\sigma)),$$

where the the probability is over random choices of Gen, and the maximum is taken over all possible authenticated messages $(m, \sigma) \in M \times \Sigma$.

2) ***Substitution attack:*** *The adversary can observe a transmitted authenticated message (m, σ) which is correctly generated by the sender S, and then tries to generate a fraudulent authenticated message (m', σ') with $(m', \sigma') \neq (m, \sigma)$ that will be accepted by the receiver R. The success probability of this attack denoted by $P_{\Phi,S}$ is defined as*

$$P_{\Phi,S} := \max_{(m,\sigma)} \max_{(m',\sigma') \neq (m,\sigma)} \Pr(R \text{ accepts } (m', \sigma') \mid (m, \sigma)),$$

where the probability is over random choices of Gen, and the maximum is taken over all possible authenticated messages $(m, \sigma), (m', \sigma') \in M \times \Sigma$ with $(m, \sigma) \neq (m', \sigma')$.

It is well known that we can construct an A-code by using algebraic structures as follows.

1. **Gen.** For a security parameter 1^{μ}, it selects a prime power q with bit length μ and constructs the finite field with q elements, and it is denoted by $GF(q)$. Then, it chooses a and b, uniformly at random from $GF(q)$. Then, it outputs $e := (a, b)$. In the following, we assume that all elements are encoded as elements in $GF(q)$.
2. **Auth.** For a message m and a sender's secret key e, it computes $\sigma := am + b$, and then outputs the authenticator σ.
3. **Ver.** For an authenticator σ and a receiver's secret key e, it outputs *true* if $\sigma = am + b$ holds, and otherwise outputs *false*.

In the above construction, it is easily seen that, for all possible $e \in E$ and $m \in M$, $Ver(e, (m, Auth(m, e))) = true$. The security of the above construction follows from the following proposition.

PROPOSITION 3. *The above construction of A-codes is $\frac{1}{q}$-secure.*

2.2. Authentication Code in the Manual Channel Model

Information-theoretically secure cryptographic protocols such as A-codes usually require secret information held by all entities enrolled in the protocols. By assuming the manual channel, Naor et al. [8] showed that A-codes could be constructed without any secret information. The manual channel is a unidirectional low-bandwidth auxiliary channel, and only a very short message can be *authentically* transmitted by the channel. In other words, the adversary cannot insert or modify a short string over the manual channel, however, he may still read it, delay it, or remove it in the manual channel. The manual channel model (MCM for short) [8] assumes that there are bidirectional insecure channels between a sender and a receiver and only one manual channel from the sender to the receiver. Formally, the model of A-codes in the MCM is defined as follows.

DEFINITION 4 (A-CODE IN THE MCM). A *k-round authentication code in the manual channel model (k-round A-code in the MCM)* Ω involves two entities, S and R, and consists of a two-tuple of algorithms (*Auth, Ver*) with four finite sets, M, T, Σ and $\tilde{\Sigma}$, where all of algorithms are deterministic. Ω is executed with two phases as follows.

- **Notation.**
  - *Entities*: S is a sender, and R is a receiver.

- *Sets*: M is a set of possible messages, Σ is a set of possible authenticators, T is a set of possible tags, and $\tilde{\Sigma}$ is a set of possible short strings.
- *Algorithms*: *Auth*: $T \times \Sigma \to \Sigma$ is an authentication algorithm, and *Ver*: $\Sigma \times \tilde{\Sigma} \to \{true, false\}$ is a verification algorithm.

1. **Authenticator Generation.** The protocol between a sender S and a receiver R consists of $(k-1)$-round interactive communications over insecure channels and only one communication from S to R over a manual channel. In the first round, S sends a message m, an authenticator σ_1 and a tag t_1 to R over the insecure channel; R sends only a tag t'_1 to S over the insecure channel. Then, both of S and R create an authenticator $\sigma_2 := Auth(t_1, \sigma_1)$. After this, in the i-th round for odd i, S sends only a tag t_i to R over the insecure channel; R sends only a tag t'_i to S over the insecure channel. And in the j-th round for even j, R sends only a tag t_j to S over the insecure channel; S sends only a tag t'_j to R over the insecure channel. Then, both of S and R inductively create an authenticator $\sigma_{i+1} := Auth(t_i, \sigma_i)$ for every $2 \leq i \leq k-1$. Finally, after $(k-1)$-round communications over the insecure channels, in the k-th round S sends a short string s to R over a manual channel.
2. **Verification.** R checks the validity of a message m by using an authenticator σ_k and a short string s. More precisely, R accepts m as valid if and only if $Ver(\sigma_k, s) = true$.

The security of A-codes in the MCM is given as follws.

Definition 5 (Security [8]). Let Ω be a k-round A-code in the MCM. Then, Ω is said to be $(n, \lambda, k, \epsilon)$-*secure*, if the following requirements are fulfiled, where n is bit length of messages, λ is the capacity of the manual channel, and ϵ is defined as follows.

1) **Correctness.** For any message m, if there is no interference by the adversary in the protocol execution, the receiver accepts m with probability at least 1/2. Furthermore, if the receiver R accepts m with probability 1, it is said that Ω meets perfect correctness.

2) **Unconditional unforgeability.** For any message m transmitted from the sender, any computationally unbounded adversary cannot replace m with a different message m' which will be accepted by the receiver R with probability larger than ϵ.

In particular, if Ω meets perfect correctness, it is said to be *perfectly* $(n, \lambda, k, \epsilon)$-*secure*.

Although the weak condition on correctness is considered in the above definition (i.e., not necessarily perfect correctness), we note that we have always considered perfect correctness in the traditional A-code. Therefore, we also consider A-codes in the MCM which satisfy perfect correctness in this paper. In addition, we note that the security of A-codes in the MCM is given as the security against the substitution attack, and that of the impersonation attack is not considered. This is because the impersonation attack cannot be successful in principle, since there is a manual channel from the sender S to the receiver R in the last transmission by which all impersonation attack is detectable.

Next, we show a construction of A-codes in the MCM proposed in [**8**]. Here, suppose that a universal hash function is given as follows: let k be an odd integer, and the universal hash function C_x is defined by $C_x(m) := \sum_{i=1}^{k} m_i x^i$. In the following, $\langle u, v \rangle$ denotes the concatenation of the strings u and v.

1. **Authentication Algorithm, Auth.** In the first round, the sender S sends a message m to the receiver R, then R receives it as an authenticator $m_R^{(1)}$. And, let an authenticator $m_S^{(1)} := m$. Furthermore, S chooses a tag $i_S^{(1)}$ and sends it to R; R receives $\hat{i}_S^{(1)}$, chooses a tag $i_R^{(1)}$ and sends it to S; S receives $\hat{i}_R^{(1)}$, and computes a authenticator $m_S^{(2)} := \langle \hat{i}_R^{(1)}, C_{i_R^{(1)}}(m_S^{(1)}) + i_S^{(1)} \rangle$; and R computes an authenticator $m_R^{(2)} := \langle i_R^{(1)}, C_{i_R^{(1)}}(m_R^{(1)}) + \hat{i}_S^{(1)} \rangle$.
   After that, in the j-th round ($2 \le j \le k-1$), S and R execute the protocol as follows.

   - If j is odd, S chooses a tag $i_S^{(j)}$ and sends it to R; R receives $\hat{i}_S^{(j)}$, chooses a tag $i_R^{(j)}$ and sends it to S; S receives $\hat{i}_R^{(j)}$, and computes a authenticator $m_S^{(j+1)} := \langle \hat{i}_R^{(j)}, C_{\hat{i}_R^{(j)}}(m_S^{(j)}) + i_S^{(j)} \rangle$; and R computes an authenticator $m_R^{(j+1)} := \langle i_R^{(j)}, C_{i_R^{(j)}}(m_R^{(j)}) + \hat{i}_S^{(j)} \rangle$.
   - If j is even, R chooses a tag $i_R^{(j)}$ and sends it to S; S receives $\hat{i}_R^{(j)}$, chooses a tag $i_S^{(j)}$ and sends it to R; R receives $\hat{i}_S^{(j)}$, and computes an authenticator $m_R^{(j+1)} := \langle \hat{i}_S^{(j)}, C_{\hat{i}_S^{(j)}}(m_R^{(j)}) + i_R^{(j)} \rangle$; S computes an authenticator $m_S^{(j+1)} := \langle i_S^{(j)}, C_{i_S^{(j)}}(m_S^{(j)}) + \hat{i}_R^{(j)} \rangle$.

   In the k-th round, S sends a short string $m_S^{(k)}$ to R over the manual channel.

2. **Verification Algorithm, Ver.** For an authenticator $m_R^{(k)}$ and a short string $m_S^{(k)}$, it outputs *true* if $m_S^{(k)} = m_R^{(k)}$, and otherwise outputs *false*.

The security of the above construction is shown as follows.

PROPOSITION 6 ([**8**]). *The above construction of A-codes in the MCM is* $(n, \lambda, k, \epsilon)$*-secure, where* $k \ge 3$ *is an odd integer,* n *is a positive interger,* $\epsilon \in (0, 1)$

is a real number, and $\lambda = 2\log\frac{1}{\epsilon} + 2\log^{(k-1)} n + O(1)$. *Here,* $\log^{(i)} x$ *is the function obtained by repeating composition of* $\log x$ *i times.*

2.3. Blind Authentication Code

We review the blind authentication code with information-theoretic security (BA-code for short), which is an information-theoretically secure authentication code with anonymity of messages, proposed by Hara et al. [4].

In BA-codes, there are four entities, a signer S, a user U, a verifier V, and a trusted initializer TI, and we assume that V is honest in the model. BA-codes are executed as follows. TI generates and distributes secret keys on behalf of S, U and V. U selects a message, generates a blinded message of the message, and then, he sends it to S. S generates an authenticator for the blinded message, and sends it back to U. Then, U creates an authenticator for the original message from the authenticator for the blinded message sent from S. In this model, a pair of the message and the authenticator is regarded as an authenticated message. Then, U checks the validity of the authenticated message. If the authenticated message is valid, U sends it to V. Then, V checks the validity of the authenticated message. The formal model of BA-codes is given as follows.

DEFINITION 7 (BA-CODE [4]). *A blind authentication code (BA-code for short)* Π *involves four entities, TI, S, U and V, and consists of a six-tuple of algorithms (Gen, Blind, Sign, Unblind, UVer, VVer) with seven finite sets,* M, M^*, Σ, Σ^*, E_S, E_U, *and* E_V, *where all of algorithms except Gen are deterministic.* Π *is executed with six phases as follows.*

- **Notation.**
  - *Entities: TI is a trusted initializer, S is a signer, U is a user, and V is a verifier.*
  - *Sets:* M *is a set of possible messages,* M^* *is a set of possible blinded messages,* Σ *is a set of possible authenticators for messages,* Σ^* *is a set of possible authenticators for blinded messages,* E_S *is a set of possible signer's secret keys,* E_U *is a set of possible user's secret keys, and* E_V *is a set of possible verifier's secret keys.*
  - *Algorithms: Gen is a key generation algorithm which takes a security parameter as input and outputs secret keys for S, U and V. Blind:* $M \times E_U \to M^*$ *is a blinding algorithm, Sign:* $M^* \times E_S \to \Sigma^*$ *is a signing algorithm, Unblind:* $\Sigma^* \times E_U \to \Sigma$ *is an unblinding algorithm, UVer:* $M \times \Sigma \times E_U \to \{true, false\}$ *is a verification algorithm for the user, VVer:* $M \times \Sigma \times E_V \to \{true, false\}$ *is a verification algorithm for the verifier.*

1. ***Key Generation and Distribution by TI.*** *TI generates secret keys $e_s \in E_S$, $e_u \in E_U$, and $e_v \in E_V$ for S, U, and V, respectively, by using Gen. After distributing these secret keys over secure channels, respectively, TI deletes them from his memory. S, U and V keep their secret keys secret, respectively.*

2. ***Blinding.*** *For a message $m \in M$, U generates a blinded message $m^* := Blind(m, e_u) \in M^*$ by using his key e_u. Then, U sends m^* to S.*

3. ***Authenticator Generation.*** *On receiving m^* from U, S generates an authenticator $\sigma^* := Sign(m^*, e_s) \in \Sigma^*$ for m^* by using his secret key e_s. Then, S sends σ^* to U.*

4. ***Unblinding.*** *On receiving an authenticator σ^* of m^* from S, U can create an authenticator $\sigma := Unblind(\sigma^*, e_u) \in \Sigma$ for the original message m by using his secret key e_u. Then, (m, σ) is regarded as an authenticated message.*

5. ***Verification by U.*** *On generating (m, σ) from (m^*, σ^*), U checks the validity of σ for m by using his secret key e_u. More precisely, if $UVer(m, \sigma, e_u) = true$ then U accepts (m, σ) as valid, and rejects it otherwise. If (m, σ) is valid, (m, σ) is regarded as a legal authenticated message, and U transmits (m, σ) to V.*

6. ***Verification by V.*** *On receiving (m, σ) from U, V checks the validity of (m, σ) by using his secret key e_v. More precisely, if $VVer(m, \sigma, e_v) = true$ then V accepts (m, σ) as valid, and rejects it otherwise.*

In the above definition, we require correctness of BA-codes, i.e., for all possible $e_u \in E_U$, $e_e \in E_S$, $e_v \in E_V$ and $m \in M$, it holds that

$$UVer(m, Unblind(Sign(Blind(m, e_u), e_s), e_u), e_u) = true,$$
$$VVer(m, Unblind(Sign(Blind(m, e_u), e_s), e_u), e_v) = true.$$

As in [4], we consider a one-time model of BA-codes where the signer is allowed to generate and transmit an authenticated message only once, and each of the user and the verifier is allowed to verify an authenticated message only once.

Next, we explain the security definition of BA-codes.

DEFINITION 8 (SECURITY [4]). *Let Π be a BA-code. Then, Π is said to be ϵ-secure, if* $\max(P_{\Pi,F}, P_{\Pi,D}, P_{\Pi,B}) \leq \epsilon$, *where $P_{\Pi,F}, P_{\Pi,D}, P_{\Pi,B}$ are defined as follows.*

1) ***Unconditional unforgeability.*** *The notion of unconditional unforgeability means that it is difficult for a dishonest user U to succeed in impersonation or substitution attacks by creating a fraudulent authenticated message. We define $P_{\Pi,F}$ as $P_{\Pi,F} := \max(P_{\Pi,F_I}, P_{\Pi,F_S})$, where P_{Π,F_I} and P_{Π,F_S} are success*

probabilities of impersonation and substitution attacks, respectively, defined below.

1-1) *In the impersonation attack, U tries to create a fraudulent authenticated message that has not been legally generated by a signer S but will be accepted by a verifier V. Success probability of the impersonation attack is defined by*

$$P_{\Pi,F_I} := \max_{e_u} \max_{(m,\sigma)} \Pr(V \textit{ accepts } (m,\sigma) \mid e_u),$$

where the probability is over random choices of Gen, and the maximum is taken over: all possible user's keys $e_u \in E_U$; and all possible authenticated messages $(m,\sigma) \in M \times \Sigma$.

1-2) *In the substitution attack, after observing a valid authenticated message created by S, U tries to create a fraudulent authenticated message that will be accepted by a verifier V. Success probability of the substitution attack is defined by*

$$P_{\Pi,F_S} := \max_{e_u} \max_{(m,\sigma)} \max_{(m^*,\sigma^*)} \max_{(m',\sigma') \neq (m,\sigma)} \Pr(V \textit{ accepts } (m',\sigma') \mid e_u, (m,\sigma), (m^*,\sigma^*)),$$

where the probability is over random choices of Gen, and the maximum is taken over: all possible user's keys $e_u \in E_U$; all possible authenticated messages $(m,\sigma), (m',\sigma') \in M \times \Sigma$ with $(m,\sigma) \neq (m',\sigma')$; and all possible pairs of blinded messages and authenticators $(m^*,\sigma^*) \in M^* \times \Sigma^*$.

2) ***Unconditional Undeniability.*** *The notion of unconditional undeniability means that it is difficult for a dishonest signer S to create an illegal authenticated message such that a user U will accept it, but a verifier V rejects it. The success probability of this attack denoted by $P_{\Pi,D}$ is defined as*

$$P_{\Pi,D} := \max_{e_s} \max_{m^*} \max_{(m,\sigma)} \Pr(U \textit{ accepts } (m,\sigma) \wedge V \textit{ rejects } (m,\sigma) \mid e_s, m^*).$$

3) ***Unconditional Blindness.*** *The notion of unconditional blindness means that it is difficult for a dishonest signer S to obtain information on the original message from its blinded message. The success probability of this attack denoted by $P_{\Pi,B}$ is defined as*

$$P_{\Pi,B} := \max_{e_s} \max_{m^*} \{ \sum_{m \in M} \mid \Pr(m|e_s, m^*) - \Pr(m) \mid \}.$$

A direct construction of BA-codes is given in [4], and we describe it as follows.

1. **Key Generation Algorithm, *Gen*:** For a security parameter 1^μ, it selects a prime power q with bit length μ, and constructs the finite field $GF(q)$ with q elements. It also chooses a polynomial $C_\alpha(z) := z + \alpha$ by picking $\alpha \in GF(q)$ uniformly at random. In addition, it chooses uniformly at random a polynomial $G(y, z) := \Sigma_{i=0}^{2} \Sigma_{j=0}^{1} g_{ij} y^i z^j \in GF(q)[y, z]$. It also selects $v_u, v_v \in GF(q)$ uniformly at random. Then, it outputs keys $e_s := G(y, z)$, $e_u := (G(v_u, z), v_u, C_\alpha(z))$ and $e_v := (G(v_v, C_\alpha(z)), v_v)$. In the following, we assume that all messages are encoded as elements in $GF(q)$.

2. **Blinding Algorithm, *Blind*:** For a message $m \in GF(q)$ and e_u, it computes $m^* := C_\alpha(m)(= m + \alpha)$, and then, outputs m^*.

3. **Signing Algorithm, *Sign*:** For a blinded message $m^* \in GF(q)$ and e_s, it computes $\beta(y) := G(y, m^*)$, and then outputs $\sigma^* := \beta(y)$.

4. **Unblinding Algorithm, *Unblind*:** Let $\sigma := \sigma^*$. Then it outputs σ.

5. **Verification Algorithm, *UVer*:** For an authenticated message (m, σ) and a user's secret key e_u, it outputs *true* if $\beta(v_u) = G(v_u, C_\alpha(m))$ holds, and otherwise outputs $false$.

6. **Verification Algorithm, *VVer*:** For an authenticated message (m, σ) and a verifier's secret key e_v, it outputs *true* if $\beta(v_v) = G(v_v, C_\alpha(m))$ holds, and otherwise outputs $false$.

It is easily seen that the above construction of BA-codes meet the correctness condition, i.e., for all possible $e_u \in E_U$, $e_e \in E_S$, $e_v \in E_V$ and $m \in M$, it holds that

$$UVer(m, Unblind(Sign(Blind(m, e_u), e_s), e_u), e_u) = true,$$
$$VVer(m, Unblind(Sign(Blind(m, e_u), e_s), e_u), e_v) = true.$$

Moreover, the security of the above construction follows from the following proposition.

PROPOSITION 9 ([4]). *The above construction of BA-codes is $\frac{2}{q}$-secure.*

3. Blind Authentication Code in the Manual Channel Model

In this section, we propose a BA-code in the MCM in which the number of entities having secret keys is smaller than that of the BA-code [4].

3.1. Model and Security Definition

We propose a model of information-theoretically secure BA-codes in the MCM. Our model is similar to that of BA-codes [4], however, a verifier does not need to have his secret key in our model. Therefore, it enables a user to arbitrarily select a verifier during the protocol (i.e., a verifier is not necessarily determined in advance). In addition, we assume that a signer does not perform the deniable attack, while it is considered in the security of BA-codes in Section 2.3. The reason is explained in Remark 12. Furthermore, we consider the one-time model of BA-codes in the MCM as well as that of BA-codes. In the following, we propose a model and a security definition of BA-codes in the MCM.

In BA-codes in the MCM, there are four entities, TI, S, U, and V, which are the same as those in Definition 7. Informally, a BA-code in the MCM is executed as follows. TI generates secret keys on behalf of S and U. After distributing these secret keys to S and U over secure channels, respectively, TI deletes the keys from his memory. Once being given a secret key from TI, for a message m, U generates a blinded message m^* by using his secret key. Then, U sends m^* to S over an insecure channel. On receiving m^* from U, S issues a receipt, and sends it back to U over an insecure channel. On receiving the receipt from S, U can select a verifier V, and he sends the message m and his secret key to V over an insecure channel. On receiving m and a user's secret key, V asks S to send his secret key and the blinded message m^* to V. On receiving a signer's secret key and m^* from S by using an A-code in the MCM, V checks the validity of the message m by using all information received from U and S. Thus, a BA-code in the MCM utilizes an A-code in the MCM as a subprotocol.

Formally, we define a BA-code in the MCM as follows.

Definition 10. *A blind authentication code in the manual channel model (BA-code in the MCM) Ψ involves four entities, TI, S, U and V, and consists of a three-tuple of algorithms (Gen, Blind, Ver) with four finite sets, M, M^*, E_S, and E_U, where all algorithms except Gen are deterministic. Ψ is executed with seven phases as follows.*

- ***Notation.***
    - *Entities: TI, S, U, and V are the same as those in Definition 7.*
    - *Sets: M, M^*, E_S, and E_U are the same as those in Definition 7.*
    - *Algorithms: Gen is the same as that in Definition 7, Blind: $M \times E_U \to M^*$ is a blinding algorithm, Ver: $M \times M^* \times E_U \times E_S \to \{true, false\}$ is a verification algorithm executed by V.*

1. ***Key Generation and Distribution by TI.*** *TI generates secret keys $e_s \in E_S$ and $e_u \in E_U$ for S and U, respectively, by using Gen. After distributing*

these secret keys to S and U over secure channels, respectively, TI deletes the keys from his memory. S and U keep their secret keys secret, respectively.

2. ***Blinding.*** *For a message $m \in M$, the user U generates a blinded message $m^* := Blind(m, e_u) \in M^*$ by using his key e_u. Then, U sends m^* to S.*

3. ***Receipt Issue by S.*** *On receiving m^* from U, the signer S issues a receipt to show that S has accepted the blinded message m^*. Then, S sends the receipt to U.*

4. ***Selecting Verifier and Data Transmission.*** *U can select a verifier V (or a verifier V may be selected in advance), and U transmits m and e_u to the verifier V.*

5. ***Transmission by the manual channel.*** *On receiving m and e_u from U, the verifier V asks the signer S to send his secret key e_s and the blinded message m^*. Then, S sends them to V by using an A-code in MCM.*

6. ***Verification by V.*** *On receiving e_s and m^* from S, the verifier V verifies the validity of m by using e_u, e_s, and m^*. More precisely, if $Ver(m, m^*, e_u, e_s) =$ true, then V accepts m as valid, and rejects it otherwise.*

In the above definition, we require the correctness condition, i.e., for all possible $e_u \in E_U$, $e_e \in E_S$ and $m \in M$, it holds that

$$Ver(m, Blind(m, e_u), e_u, e_s) = true.$$

Next, we define security of BA-codes in the MCM as follows.

DEFINITION 11. *Let Ψ be a BA-code in the MCM. Then, Ψ is said to be $(n, \lambda, k, \epsilon, \delta)$-secure, if the underlying A-code in the MCM is an unconditionally perfectly secure $(n, \lambda, k, \epsilon)$-authentication protocol and it holds that $\max\{P_{\Psi,F}, P_{\Psi,B}\} \leq \delta$, where $P_{\Psi,F}$ and $P_{\Psi,B}$ are defined as follows.*

1) ***Unconditional unforgeability.*** *The notion of unconditional unforgeability means that it is difficult for a dishonest user U to succeed in the substitution attack by creating a fraudulent message m' for a valid message m. Success probability of this attack is defined by*

$$P_{\Psi,F} := \max_{m} \max_{m' \neq m} \max_{e_u{}'} \max_{m^*} \Pr(\, Ver(m', m^*, e_u{}', e_s) = true \mid m, e_u, m^*),$$

where the probability is over random choices of Gen, and the maximum is taken over: all possible messages $m, m' \in M$ with $m \neq m'$; and all possible *user's secret keys* $e_u{}' \in E_U$ *(it is not necessarily the case with* $e_u \neq e_u{}'$*, i.e.,* $e_u = e_u{}'$ *is possible); and all possible blinded messages* $m^* \in M^*$*.*

2) ***Unconditional blindness.*** *The notion of unconditional blindness is the same as blindness in BA-codes. Success probability of this attack is defined by*

$$P_{\Psi,B} := \max_{e_s} \max_{m^*} \{ \sum_{m \in M} |\Pr(m|e_s, m^*) - \Pr(m)| \},$$

where the probability is over random choices of Gen, the summation is over all possible messages $m \in M$*, and the maximum is taken over: all possible signer's keys* $e_s \in E_S$*; and all possible blinded messages* $m^* \in M^*$*.*

REMARK 12. *In our model, we do not consider the attack by a dishonest signer against unconditional undeniability in the security definition of BA-codes (see Definition 8), since we cannot realize the security against this attack in principle, i.e., the setting of no verifier's key makes it impossible that a BA-code meets unconditional undeniablity. Actually, if a signer is dishonest, he can control all information which the user will send to a verifier. Therefore, the dishonest signer succeeds in the attack against unconditional undeniability with probability one. From an aspect of applications, there would be several situations that we can trust an authority corresponding to the signer in the real world. Our scheme can be applied in such situations.*

In addition, in our model we do not consider the impersonation attack by a dishonest user in the security definition of BA-codes (see Definition 8). The reason is essentially the same as that in the A-code in the MCM.

Note that our model of BA-codes in the MCM is simpler than that of BA-codes in the TI model in Section 2.3, since we have assumed that the signer does not perform the deniable attack in our model: By the assumption, the user does not need authenticators of a message and its corresponding blinded message to check the validity of them; and our model of BA-codes in the MCM requires only the three-tuple of algorithms, while the model of BA-codes in the TI model requires the six-tuple of algorithms.

3.2. Construction

In this section, we propose a construction of BA-codes in the MCM. The idea in our construction is to utilize the construction of commitment schemes [**1**]. Our construction of algorithms is given as follows.

1. **Key Generation Algorithm, *Gen*.** For a security parameter 1^μ, it selects a prime power q with bit length μ, and constructs the finite field $GF(q)$ with q elements. Then, it chooses a, b, x_1 uniformly at random from $GF(q)$ and

puts $y_1 = ax_1 + b$. Then, it outputs $e_u := (a, b)$ and $e_s := (x_1, y_1)$. In the following, we assume that messages are encoded as elements in $GF(q)$.

2. **Blinding Algorithm, *Blind*.** For a message m and a user's secret key e_u, it computes $m^* := m + a$, then outputs the blinded message m^*.

3. **A-code in the MCM.** In the phase of *transmission by the manual channel*, the signer transmits a verifier (m^*, e_s), where $e_s = (x_1, y_1)$, by using the perfectly $(n, \lambda, k, \epsilon)$-secure A-code in the MCM with $k = 3$ in [**8**] (see Section 2.2).

4. **Verification Algorithm, *Ver*.** For a message m, a user's secret key $e_u = (a, b)$, a signer's secret key $e_s = (x_1, y_1)$, and a blinded message m^*, it outputs *true*, if it holds that

$$m^* = m + a, \tag{1}$$

$$y_1 = ax_1 + b, \tag{2}$$

and otherwise outputs *false*.

It is easily seen that the above construction satisfies correctness, i.e., for all possible $e_u \in E_U$, $e_s \in E_S$ and $m \in M$, it holds that

$$Ver(m, m^*, e_u, e_s) = \mathit{true}.$$

The security of the above construction is shown as follows.

THEOREM 13. *The above construction is* $(n, \lambda, 3, \epsilon, \delta)$*-secure, where* $n = \lfloor 3 \log q \rfloor$, $\lambda = \left\lceil 2 \log \frac{1}{\epsilon} + \log^{(3)} n \right\rceil$, $\epsilon = \frac{12 \log q}{q}$, *and* $\delta = \frac{1}{q}$.

PROOF. In the phase of *transmission by the manual channel*, we have used the perfectly $(n, \lambda, k, \epsilon)$-secure A-code in the MCM with $k = 3$ in [**8**]. Hence, n, λ, ϵ are evaluated as the statement of the theorem.

In the following, we will evaluate δ. Our construction of BA-codes except for the subprotocol of the A-code in the MCM is based on construction of the commitment scheme in [**1**]. Furthermore, by construction, it is seen that the security of concealing and binding in the commitment scheme corresponds to the security of unconditional blindness and unconditional unforgeability of the BA-code, respectively. First, we note that the construction of the commitment scheme in [**1**] meets perfectly concealing, and hence we have $P_{\Psi,B} = 0$ in our construction (see [**1**, Theorem 4.1]). Second, we show $P_{\Psi,F} \leq \frac{1}{q}$. This fact straightforwardly follows from the security proof of binding in [**1**] (see [**1**, Theorem 4.2]). Thus, we have $\max\{P_{\Psi,F}, P_{\Psi,B}\} \leq \frac{1}{q}$. □

3.3. Extension

3.3.1 Generic construction from commitment schemes

In our construction of BA-codes in the MCM, we have used the construction of the commitment scheme in [**1**], since it meets good security condition, i.e., perfectly concealing. However, by the construction in Section 3.2, it is straightforwardly seen that *any construction* of commitment schemes can be applied in our construction, instead of the one in [**1**]. Therefore, we can obtain a generic construction of BA-codes in the MCM, starting from unconditionally secure commitment schemes and A-codes in the MCM. In this case, the security proof can be shown in a very similar way as that of Theorem 13, namely, the security of concealing and binding in the underlying commitment scheme corresponds to the security of unconditional blindness and unconditional unforgeability of the BA-code, respectively.

3.3.2 BA-codes in the noisy channel model and the bounded storage model

In this paper, we focused on the manual channel model (MCM) to realize a mechanism of BA-codes where no verifier's secret-key is required. The essential idea in our scheme lies in utilizing the A-code between the signer and the verifier with no shared secret in the phase of *transmission by the manual channel* in Definition 10. However, we note that, instead of using the A-code in the MCM in the phase, it is also possible to use the A-code with no shared secrets in the noisy channel model (NCM) [**14**] or the bounded storage model (BSM) [**7**]. Actually, by applying the key agreement in the NCM (resp., BSM) and the traditional A-code, we can construct the A-code in the NCM (resp., BSM). Therefore, we can also realize:

- BA-code in the noisy channel model (NCM); and
- BA-code in the the bounded storage model (BSM).

The proofs of security of the BA-code in the NCM and BSM can be shown by essentially the same way as that of Theorem 13.

4. Concluding Remarks

In this paper, we proposed a formal model and security formalization for BA-codes in the MCM. The advantage of our model over the traditional BA-codes [**4**] is that a verifier does not have to hold a secret key and hence a user can arbitrarily select a verifier during the protocol execution. In addition, we presented a construction of BA-codes in the MCM. Furthermore, we considered several extension: the BA-codes in the MCM could be constructed from any unconditionally secure commitment scheme and A-code in the MCM in a generic way; and that the BA-codes in the noisy channel model and the ones in the the bounded storage model could also be obtained by using the similar idea in our construction.

Although we proposed the construction of BA-codes in the MCM in this paper, it is not shown what an optimal construction of BA-codes in the MCM is, where the optimal construction means a construction satisfying the condition that the size of secret keys of the user and the signer being minimized. Therefore, it would be interesting to derive a tight lower bound on the size of the user's and the signer's secret keys, and to show an optimal construction which meets the lower bound with equality.

Acknowledgments. The authors would like to thank Tsutomu Matsumoto for helpful comments.

References

[1] C. Blundo, B. Masucci, and D. Stinson, "Constructions and bounds for unconditionally secure non-interactive commitment schemes", Designs, Codes and Cryptography, vol.26, pp. 97–110, 2002.

[2] D. Chaum, "Blind signatures for untraceable payments", Advances in Cryptology – CRYPTO '82, pp. 199–203, Springer, 1982.

[3] E.N. Gilbert, F.J. MacWilliams, and N.J.A. Sloane, "Codes which detect deception", Bell System Technical Journal, vol. 53, no. 3, pp. 405–424, 1974.

[4] Y. Hara, T. Ishiwata, J. Shikata, and T. Matsumoto, "Unconditionally Secure Blind Authentication Codes: The Model, Constructions, and Links to Commitment", Formal to Practical Security, LNCS 5458, pp. 116–137, Springer, 2009.

[5] Y. Hara, T. Seito, J. Shikata, and T. Matsumoto, "Unconditionally Secure Blind Signatures", ICITS 2007, LNCS 4883, pp. 23–43, Springer, 2009.

[6] A. Juels, A. Luby, and R. Ostrovsky, "Security of blind digital signatures,"Advances in Cryptology-CRYPTO'97, LNCS 1294, pp.150-164, 1997.

[7] U. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher,"J. Cryptology, vol.5, no.1, pp.53-66, 1992.

[8] M. Naor, G. Segev, and A. Smith, "Tight bounds for unconditional authentication protocols in the manual channel and shared key models,"IEEE Transactions on Information Theory, vol.54, no.6, pp.2408-2425, 2008.

[9] B. Pinkas, "Fair secure two-party computation,"Advances in Cryptology-EUROCRYPT 2003. LNCS 2656, pp.87-105, 2003.

[10] D. Pointcheval, and J. Stern, "Provably secure blind signature schemes,"Advances in Cryptology-ASIACRYPT'96, LNCS 1163, pp.252-265, 1996.

[11] R. Rivest, "Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer", manuscript, 1999. Available at `http://people.csail.mit.edu/rivest/Rivest-commitment.pdf`

[12] G. Simmons, "Authentication theory/coding theory,"In G.Blakley and D.Chaum, editors, Advances in Cryptology, LNCS 196, pp.411-431, 1982.

[13] S. Vaudenay, "Secure communications over insecure channels based on short authenticated strings,"Advances in Cryptology - CRYPTO 2005, LNCS 3621, pp. 309-326, 2005.

[14] A.D. Wyner, "The wire-tap channel", Bell System Technical Journal, vol. 58, pp. 1355–1387, 1975.

Noriyasu Takei

Graduate School of Environment and Information Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya, Yokohama, 240-8501, Japan
takei-noriyasu-mx@ynu.jp

Yohei Watanabe

Graduate School of Environment and Information Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya, Yokohama, 240-8501, Japan
watanabe-yohei-xs@ynu.jp

Junji Shikata

Graduate School of Environment and Information Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya, Yokohama, 240-8501, Japan
shikata@ynu.ac.jp