Authentication codes from ε-ASU hash functions with partially secret keys

Chinese Journal of Electronics
Vol.23, No.4, Oct. 2014

Authentication Codes from ϵ-ASU Hash Functions with Partially Secret Keys*

LIU Shengli[1], TILBORG Henk van[2], WENG Jian[3] and CHEN Kefei[4]

(1. *Deptartment of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*)

(2. *Deptartment of Mathematics and Computer Science, Eindhoven University of Technology, the Netherlands*)

(3. *Department of Computer Science, Jinan University, Guangzhou 510632, China*)

(4. *School of Science, Hangzhou Normal University, Hangzhou 310036, China*)

Abstract — An authentication code can be constructed with a family of ϵ-Almost strong universal (ϵ-ASU) hash functions, with the index of hash functions as the authentication key. This paper considers the performance of authentication codes from ϵ-ASU, when the authentication key is only partially secret. We show how to apply the result to privacy amplification against active attacks in the scenario of two independent partially secret strings shared between a sender and a receiver.

Key words — Information theory, Authentication code, Privacy amplification, Unconditional security.

I. Introduction

Authentication theory was first formalized by Simmons[1], who introduced the mathematical mode of authentication in Ref.[2]. Authentication considers the scenario that a transmitter sends a message over a public communication channel to a receiver in the presence of an active opponent who can modify the message or introduce a fraudulent message over the channel. The goal of authentication is to investigate a coding method such that the receiver will detect the opponent's active attack. Authenticity can be achieved by Authentication codes (A-codes): the transmitter and receiver first agree on an authentication key k, taken from a finite set $\mathcal{K}$. Each authentication key k determines an encoding rule $E_k(\cdot)$, which encodes a piece of plaintext s, hereafter called source state, to a message $m = E_k(s)$. If $m = E_k(s) = (s, t)$ with $t = e_k(s)$, we call z the tag or the authenticator, and these codes are called Cartesian A-codes.

The active attacks by the opponent can be classified into two categories according to his cheating strategies. The first is called impersonation attack in which the opponent introduces a fraudulent message to the channel, hoping it to be accepted by the receiver. The other is called substitution attack, in which the opponent intercepts a message m and modifies it to a different message m', hoping it to be accepted by the receiver. Let P_I and P_S be the probability of a successful impersonation attack resp. substitution attack.

We study authentication codes with a partially secret key S. This partial secrecy is characterized by the fact that Eve's min-entropy about S, given her information $Z = z$, is less than the length of S. This quantity is denoted by $H_\infty(S|Z = z)$.

Definition 1 Let X be a random variable over set $\mathcal{X}$. The Shannon entropy of the random variable X is defined as $H(X) = -\sum_{x\in\mathcal{X}} \Pr[X = x] \log \Pr[X = x]$. The min-entropy of X is defined as $H_\infty(X) = -\log \max_{x\in\mathcal{X}} \Pr[X = x]$.

It is easy to prove that $0 \le H_\infty(X) \le H(X) \le \log|\mathcal{X}|$ and the equality holds when X is uniformly distributed. By $|\mathcal{X}|$, we denote the cardinality of the set $\mathcal{X}$.

Throughout this paper, we denote $\log_2(\cdot)$ by $\log(\cdot)$. Let $[a]_r$ denote a substring which is comprised of any r bits of a. We also assume that elements in $GF(q)$ has a compact expression of about $\log q$ bits.

II. Universal Hashing and A-codes

Results on A-codes are usually based on the assump-

*Manuscript Received July 2012; Accepted Apr. 2014. This work is supported by Natural Science Foundation of China (No.61170229, No.61133014, No.61272413, No.61373153), Innovation Project of Shanghai Municipal Education Commission (No.12ZZ021), Specialized Research Fund for the Doctoral Program of Higher Education (No.20110073110016, No.20134401110011), and the Open Project Program of the State Key Laboratory of MEAC (No.2013A01).

tion that the authentication key is unknown to Eve except its length. Following the terminology of A-codes, let $\mathcal{A}$ denote the set of source states, $\mathcal{H}$ be the set of encoding rules (authentication keys), and $\mathcal{B}$ be the set of authenticators.

Universal hash functions were first introduced for storage and retrieval on keys by Carter and Wegman[3]. Further study of hash function in authentication was done by Wegman and Carter[4] and Stinson in Ref.[5]. In Ref.[6], Stinson showed how to construct authentication codes from ϵ-Almost strong universal (ASU) hash functions.

For a finite set $\mathcal{H}$ of hash functions, all from $\mathcal{A}$ to $\mathcal{B}$, for $a_1, a_2 \in \mathcal{A}, a_1 \neq a_2$, define $\delta_{\mathcal{H}}(a_1, a_2)$ as the number of hash function $h \in \mathcal{H}$ such that $h(a_1) = h(a_2)$, *i.e.*, it counts the number of hash functions, for which a_1 and a_2 collide.

Definition 2 Let $\epsilon > 0$. $\mathcal{H} : \mathcal{A} \to \mathcal{B}$ is ϵ-ASU if (1) for every $a \in \mathcal{A}$ and for every $b \in \mathcal{B}$, $|\{h \in \mathcal{H} : h(a) = b\}| = |\mathcal{H}|/|\mathcal{B}|$; (2) for every $a_1, a_2 \in \mathcal{A}$ ($a_1 \neq a_2$) and for every $b_1, b_2 \in \mathcal{B}$, $|\{h \in \mathcal{H} : h(a_1) = b_1,\ h(a_2) = b_2\}| \leq \epsilon|\mathcal{H}|/|\mathcal{B}|$.

Definition 3 If $\mathcal{H}$ is ϵ-ASU with $\epsilon = 1/|\mathcal{B}|$, then $\mathcal{H}$ is called strongly universal$_2$ (SU_2 for short).

Construction 1[6] For some positive integer v, let $\mathcal{A} = \{a = (a_1, a_2, \ldots, a_v); a \in GF(q)^v\}$, $\mathcal{B} = GF(q)$. Let $\mathcal{H} = \{h_k = (h_{k,1}, h_{k,2}, \ldots, h_{k,v+1});\ h_k \in GF(q)^{v+1}\}$. Then $\mathcal{H} : \mathcal{A} \to \mathcal{B}$ defines a SU$_2$ with $h_k(a) = h_{k,1} \cdot a_1 + h_{k,2} \cdot a_2 + \ldots + h_{k,v} \cdot a_v + h_{k,v+1}$.

Construction 2 Almost the same as Construction 1, the only difference is $\mathcal{H} : \mathcal{A} \to \{0,1\}^r$, where $0 < r \leq \log(q)$, and the hash value is given by any r bits of the hash value of Construction 1, *i.e.*, $h_k(a) = [h_{k,1} \cdot a_1 + h_{k,2} \cdot a_2 + \ldots + h_{k,v} \cdot a_v + h_{k,v+1}]_r$, with $\mathcal{H} = \{h_k = (h_{k,1}, h_{k,2}, \ldots, h_{k,v+1}); h_k \in GF(q)^{v+1}\}$.

Lemma 1 The family of the hash functions $\mathcal{H} : \mathcal{A} \to \{0,1\}^r$, where $0 < r \leq \log_2(q)$, in Construction 2 is also a SU$_2$ family of hash functions.

Proof 1 Recall the SU$_2$ in Construction 1, for $h_k = (h_{k,1}, h_{k,2}, \cdots, h_{k,v}) \in \mathcal{H}$, the hash value is given by $b = h_{k,1} \cdot a_1 + h_{k,2} \cdot a_2 + \ldots + h_{k,v} \cdot a_v + h_{k,v+1}$. Hence given $((a_1, \cdots, a_v), b)$, there are $|\mathcal{H}|/|\mathcal{B}| = q^{v+1}/q = q^v$ hash functions.

Now in Construction 2, the hash value is $h_k(a) = [b]_r$. Let $\tilde{b} = [b]_r$ be fixed, then there are $q/2^r$ possible values of b corresponds to $\tilde{b}$. Therefore, there are totally $q^{v+1}/2^r = |\mathcal{H}|/|\mathcal{B}|$, where $\mathcal{B} = \{0,1\}^r$.

For the SU$_2$ in Construction 1, we know that there are q^{v-1} hash function in $\mathcal{H}$ mapping $(a_1, \cdots, a_v)$ to b and $(a'_1, \cdots, a'_v)$ to b', where $(a_1, \cdots, a_v) \neq (a'_1, \cdots, a'_v)$.

Let $\tilde{b} = [b]_r$ and $\widetilde{b'} = [b']_r$, there are $q/2^r$ possible values of b corresponds to $\tilde{b}$ and $q/2^r$ possible values of b' corresponds to $\widetilde{b'}$. Therefore, there are at most $q^{v-1} \cdot \dfrac{q}{2^r} \cdot \dfrac{q}{2^r} = \dfrac{q^{v+1}}{2^{2r}} = |\mathcal{H}|/|\mathcal{B}|^2$ functions mapping $(a_1, \cdots, a_v)$ to $\tilde{b}$ and $(a'_1, \cdots, a'_v)$ to $\widetilde{b'}$ in this construction.

Construction 3 (den Boer[7]) Let $\mathcal{A} = (GF(q))^v$. For any $a = (a_1, a_2, \ldots, a_v) \in \mathcal{A}$. Define a polynomial $a(x) = a_1 x + a_2 x^2 + \ldots + a_v x^v$. It is a mapping from $GF(q)$ to itself. Let $\mathcal{H} = \{h_k = (h_{k,1}, h_{k,2}); h_k \in GF(q)^2\}$. Then $\mathcal{H} : \mathcal{A} \to \mathcal{B}$ defines an ϵ-ASU with $\epsilon = v/q$, with $h_k(a) = h_{k,1} + a(h_{k,2}) = h_{k,1} + a_1 \cdot h_{k,2} + a_2 \cdot (h_{k,2})^2 + \ldots + a_v \cdot (h_{k,2})^v$, where $h_k = (h_{k,1}, h_{k,2}) \in \mathcal{H}$ and $a = (a_1, a_2, \ldots, a_v) \in \mathcal{A}$.

Construction 4 Almost the same as Construction 3, the only difference is that $\mathcal{B} = \{0,1\}^r$, where $0 < r \leq \log(q)$. $\mathcal{H} : \mathcal{A} \to \mathcal{B}$ evaluates the hash value by any r bits of the hash value of Construction 1, *i.e.*, $h_k(a) = [h_{k,1} + a(h_{k,2})]_r$, where $h_k = (h_{k,1}, h_{k,2}) \in \mathcal{H}$ and $a = (a_1, a_2, \ldots, a_v) \in \mathcal{A}$.

Lemma 2 The family of the hash functions $\mathcal{H} : \mathcal{A} \to \{0,1\}^r$, where $0 < r \leq \log(q)$, in Construction 4 defines an ϵ-ASU with $\epsilon = v/2^r$.

The proof is similar to that of Lemma 1. We omit it.

In Ref.[8], Stinson introduced concepts of ϵ-ASU, gave some general constructions for ϵ-ASU, and showed how to construct A-codes from ϵ-ASU. Given an ϵ-ASU: $\mathcal{H} : \mathcal{A} \to \mathcal{B}$, Let $\mathcal{A}$ be the set of source states, $\mathcal{B}$ be the set of authenticators, and each hash function $H \in \mathcal{H}$ be the encoding rule. We get an authentication code with $P_I = 1/|\mathcal{B}|$ and $P_S \leq \epsilon$, as shown in Theorem 1.

Theorem 1[8] If there exists an ϵ-ASU class of hash functions $\mathcal{H}$ from $\mathcal{A}$ to $\mathcal{B}$, then there exists an authentication code for $|\mathcal{A}|$ source states, having $|\mathcal{B}|$ authenticators and $|\mathcal{H}|$ encoding rules, such that $P_I = 1/|\mathcal{B}|$ and $P_S \leq \epsilon$.

Consequently, we have A-codes from the above four constructions, which are summarized in Table 1.

Table 1. A-codes with a totally secret authentication key

A-codes	$\lvert\mathcal{H}\rvert$	$\lvert\mathcal{A}\rvert$	$\lvert\mathcal{B}\rvert$	P_I	P_S
Const 1	q^{v+1}	q^v	q	$1/q$	$1/q$
Const 2	q^{v+1}	q^v	2^r	$1/2^r$	$1/2^r$
Const 3	q^2	q^v	q	$1/q$	v/q
Const 4	q^2	q^v	2^r	$1/2^r$	$v/2^r$

III. A-Codes with Partial Secret from ϵ-ASU

However, previous results on authentication codes are usually based on the assumption that the authentication key is totally secret to the opponent Eve.

When the opponent's entropy about K is less than $\log|\mathcal{K}|$, the length of K, the key K is only partially secret to him. Now that we characterize the uncertainty by min-entropy, we have $H_\infty(K) < \log|\mathcal{K}|$. When a side information $B = b$ is exposed to the opponent, a general upper bound on the reduction of the min-entropy of $\mathcal{K}$ is given by Ref.[9].

Lemma 3[9] Let K and B be random variables and let $s > 0$. Then with probability at least $1 - 2^{-s}$ (taken over $b \in \mathcal{B}$), we have $H_\infty(K) - H_\infty(K|B = b) \leq \log|\mathcal{B}| + s$.

The following theorem shows the performance of A-codes with only a partially secret key where this partial secrecy is characterized by the fact that Eve's uncertainty about K is less than $\log|\mathcal{K}|$, the length of K.

Theorem 2 Suppose that the authentication key K, which determines hash function H_k in an ϵ-ASU class of hash functions $\mathcal{H} : \mathcal{A} \to \mathcal{B}$, is only partially secret. Let the opponent's information about K be characterized by $H_\infty(K) \geq t\log|\mathcal{K}|$, where $0 < t < 1$. Then the corresponding A-code constructed from the ϵ-ASU has $P_I \leq \dfrac{|\mathcal{K}|^{1-t}}{|\mathcal{B}|}$, $P_S \leq \epsilon \cdot |\mathcal{K}|^{1-t}$.

Proof 2 First, we want to estimate the probability of a successful impersonation attack by Eve, *i.e.*, to determine the probability that Eve, who has partial knowledge about the authentication key K shared between Alice and Bob, can successfully guess a pair (a, b) such that $b = h_K(a), a \in \mathcal{A}, b \in \mathcal{B}$. According to the properties of $\epsilon - ASU$, given a pair (a, b), the number of encoding rules satisfying $b = H_K(a)$ is $|\mathcal{K}|/|\mathcal{B}|$.

Let $Z = z$ denote all knowledge Eve knows about K before she sees any valid pair. Let $p_i,\ 1 \leq i \leq |\mathcal{S}|$, denote the probabilities that Eve has assigned to all encoding rules. Without loss of generality, let the first $|\mathcal{K}|/|\mathcal{B}|$ encoding rules give a valid pair (a, b). Then $P_I = \sum_{i=1}^{|\mathcal{K}|/|\mathcal{B}|} p_i$.

Since $H_\infty(K|Z = z) \geq t\log|\mathcal{K}|$, we know $p_i \leq 2^{-t\log|K|}$. So $P_I = \sum_{i=1}^{|\mathcal{K}|/|\mathcal{B}|} p_i \leq \sum_{i=1}^{|\mathcal{K}|/|\mathcal{B}|} 2^{-t\log|K|} = |\mathcal{K}|/|\mathcal{B}| \cdot 2^{-t\log|K|} = |\mathcal{K}|^{1-t}/|\mathcal{B}|$.

A successful substitution attack means that the opponent has guessed a correct pair (a', b') after having seen a valid pair (a, b), where $a' \neq a, b = h_k(a)$ and $b' = h_k(a')$. The number of encoding rules that give rise to both pairs is upper bounded by $\epsilon \cdot |\mathcal{K}|/|\mathcal{B}|$ according to the definition of $\epsilon - ASU$, *i.e.*,

$$|\{k : b = h_k(a) \ \&\ b' = h_k(a')\}| \leq \epsilon \cdot |\mathcal{K}|/|\mathcal{B}| \qquad (1)$$

Given any (a, b) with $b = h_k(a)$, the probability that the opponent presents a valid pair (a', b') is as follows.

$\Pr[a \neq a', b' = h_k(a') \mid a, b = h_k(a)]$
$= \sum_{k\in\mathcal{K}} \Pr[a \neq a', b' = h_k(a') \mid a, b = h_k(a), K = k] \cdot \Pr[K = k \mid a, b = h_k(a)]$
$= \sum_{k\in\mathcal{K}} \Pr[a \neq a', b' = h_k(a'), b = h_k(a) \mid a, K = k] \cdot \Pr[K = k \mid a, b = h_k(a)]$
$\leq \sum_{k\in\mathcal{K}} \Pr[a \neq a', a, b' = h_k(a'), b = h_k(a) \mid a, K = k] \cdot 2^{-t\log|\mathcal{K}|+\log|\mathcal{B}|}$
$\leq \epsilon \cdot |\mathcal{K}|/|\mathcal{B}| \cdot 2^{-t\log|K|+\log|\mathcal{B}|} = \epsilon \cdot |\mathcal{K}|^{1-t}$. Therefore,

$$P_S = \max_{a,b,a',b'} \Pr[a \neq a', b' = h_k(a') \mid a, b = h_k(a)] = \epsilon \cdot |\mathcal{K}|^{1-t}.$$

In the proof, we use the following facts.

$$\begin{aligned}(1)\quad &\Pr[a \neq a', b' = h_k(a'), b = h_k(a) \mid a, K = k]\\ &= \Pr[a \neq a', b' = h_k(a') \mid a, b = h_k(a), K = k]\\ &\quad \cdot \Pr[b = h_k(a)|a, K = k]\end{aligned}$$

and $\Pr[b = h_k(a) \mid a, K = k] = 1$.

(2) Since the source state a is independent to the authentication key K, we have

$$\Pr[K = k \mid a, b = h_k(a)] = \Pr[K = k \mid b = h_k(a)],$$

hence $H_\infty(K \mid a, b = h_k(a)) = H_\infty(K \mid b = h_k(a))$.

(3) According to Lemma 3, we have $H_\infty(K \mid b = h_k(a)) \geq t\log|\mathcal{K}| - \log|\mathcal{B}|$. Consequently, we know $\Pr[K = k \mid a, b = h_k(a)] \leq 2^{-t\log|\mathcal{K}|+\log|\mathcal{B}|}$.

Now applying Theorem 2 to the four Constructions for A-codes from ϵ-ASU in the last section, we get the following facts.

Suppose that the opponent's uncertainty about the authentication key K satisfies $H_\infty(K) \geq t\log|\mathcal{K}|$. Now applying Theorem 2 to the four Constructions for A-codes gives Table 2.

Table 2. A-codes with a partially secret key

A-codes	$\lvert\mathcal{H}\rvert$	$\lvert\mathcal{A}\rvert$	$\lvert\mathcal{B}\rvert$	P_I	P_S
Const 1	q^{v+1}	q^v	q	$q^{-(v+1)t+v}$	$q^{-(v+1)t+v}$
Const 2	q^{v+1}	q^v	2^r	$q^{-(v+1)t+v+1}/2^r$	$q^{-(v+1)t+v+1}/2^r$
Const 3	q^2	q^v	q	q^{-2t+1}	$v \cdot q^{-2t+1}$
Const 4	q^2	q^v	2^r	$q^{2(1-t)}/2^r$	$v \cdot q^{2(1-t)}/2^r$

Table 2 has shown that there is a compromise between the number of encoding rules, the number of source states, P_I, and P_S. Now that the encoding rule (authentication key) is only partially known to the opponent, the opponent's knowledge about the encoding rules also plays a role in the compromise, as shown in Table 2. To make $P_S < 1$, we have to impose different requirements on t. For example, $t > v/(v + 1)$, $t > 1 - \dfrac{r}{(v + 1)\log q}$, $t > 1/2$ and $t > 1 - \dfrac{r}{2\log q}$ are required in Construction 1, 2, 3, 4 respectively.

IV. Application to Privacy Amplification

Privacy amplification[10] distills a shorter but highly secret string from a partially secret string. Privacy amplification can be implemented by universal hash functions[10,11]. Given a partially secret string W, the length of the distilled secret key is determined by the min-entropy of W and a parameter ε, which measures how uniform the secret key is.

More precisely, if the sender and receiver share a binary string W of length n. To implement privacy amplification, the sender randomly chooses a function g from a universal class of hash functions and sends the description of this function to the receiver over a public channel. Then both the sender and receiver computes $K = g(W)$ as their secret key. When the public channel is authentic, *i.e.*, when the opponent is only able to carry out a passive attack, the length of the final, distilled secret key is approximately determined by the min-entropy about S. If partially secrecy of W is measured with $H_\infty(W) \leq tn$ $(0 < t \leq 1)$, then the length of K can be as large as $tn + 2 - 2\log 1/\varepsilon$.

On the other hand, if the public channel is not authentic, *i.e.*, when Eve can also perform an active attack, then we can detect Eve's active attacks in the following way.

Here we consider a simple scenario: the sender and the receiver share two independent partially secret strings, S_I and S_{II}. We will use the shorter one for both authentication and distillation, and the other for distillation. Surprisingly, the independence of two partially secret strings gains a lot. According to the A-Codes from Construction 3, as long as the opponent's min-entropy about S_I (of bit-length n') is larger than $n'/2$, *i.e.*, $H_\infty(S_I|Z = z) > n'/2$, active attacks can be detected with A-Codes and privacy amplification can distill a secret key of $H_\infty(S_{II}|Z = z) + 2 - 2\log 1/\varepsilon$ bits from S_{II}.

V. Conclusion

This paper studies how to construct authentication codes with ϵ-ASU hash function, but with partially secret authentication key. Our result explicitly presents the compromise between the number of encoding rules, the number of source states, and probabilities of impersonation attack and substitution attack. This result gives an immediate application to privacy amplification against active attacks.

References

[1] G.J. Simmons, "Authentication theory/coding theory", G.R. Blakley and D. Chaum, eds., *Advances in Cryptology, Proc. Crypto'84*, New York, Vol.196, pp.411–431, 1985.

[2] G.J. Simmons, " A game theory model of digital message authentication", *Congr. Numer.*, Vol.34, pp.413–424, 1992.

[3] J.L. Carter and M.N. Wegman, "Universal classes of hash functions", *Journal of Computer and System Sciences*, Vol.18, No.2, pp.143–154, 1979.

[4] M.N. Wegman and J.L. Carter, "New hash functions and their use in authentication and set equality", *Journal of Computer and System Sciences*, Vol.22, No.3, pp.265–279, 1981.

[5] D.R. Stinson, "Combinatorial techniques for universal hashing", *Journal of Computer and System Sciences*, Vol.48, No.2, pp.337–346, 1994.

[6] D.R. Stinson, "Universal hashing and authentication codes", *Designs, Codes and Cryptography*, Vol.4, No.4, pp.369–380, 1994.

[7] B. den Boer, "A simple and key-economical unconditional authentication scheme", *Journal of Computer Security*, Vol.2, No.1, pp.65–71, 1993.

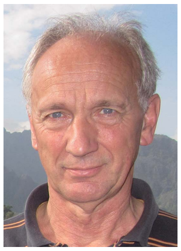
[8] D.R. Stinson, " Universal hashing and auhtentication codes", *Advances in Cryptology-CRYPTO'91*, Vol.576, pp.74–85, 1992.

[9] S. Wolf, *Information-theoretically and Computationally Secure Key Agreement in Cryptography*, *ETH Dissertation*, No.13138, ETH Zurich, 1999.

[10] C.H. Bennett, G. Brassard, C. Crépeau, *et al.*, "Generalized privacy amplification", *IEEE Trans. Inform. Theory*, Vol.41, No.6, pp.1915–1923, 1995.

[11] Y. Dodis, R. Ostrovsky, L. Reyzin, *et al.*, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", *SIAM Journal on Computing*, Vol.38, No.1, pp.97–139, 2008.

LIU Shengli is a professor at Shanghai Jiaotong University. She got her Bachelor's, Master's and Ph.D. degree from Xidian University in 1995, 1998 and 2000 respectively. From 2000 till 2002, she continued her research on cryptography and got another Ph.D. degree at Technische Universiteit Eindhoven, the Netherlands. Her research interests include public key cryptosystems and information-theoretic security. (Email: liu-sl@cssjtu.edu.cn)



TILBORG Henk van (M.S.c. 1971, Ph.D. 1976) was employed since 1972 by the Department of Mathematics and Computer Science of the Eindhoven University of Technology, the Netherlands, from 1992 to 2012 as full professor. He has written books on cryptology and coding theory and is also the editor in chief of the Encyclopedia of Cryptography and Security. He served the IEEE Information Theory Society as board member and as editor on Coding Theory. He was elected as fellow in 2000.

WENG Jian received M.S. and B.S. degrees in computer science and engineering from South China University of Technology, Guangzhou, China, in 2004 and 2000, respectively. He received the Ph.D. degree in computer science and engineering from Shanghai Jiaotong University, Shanghai, in 2008. Since 2008, he joined Jinan University at the Department of Computer Science, and is currently a professor. His research interests include key-exposure protection mechanism, provable security and pairing-based cryptography.

CHEN Kefei received the B.Sc and M.Sc degree in 1982 and 1985, respectively, from the Northwestern Telecommunications Engineering Institute, China; and the Ph.D. degree in 1994 from Justus Liebig University Giessen, Germany. From 1996 to 2012, he was a professor of the Department of Computer Science and Engineering at Shanghai Jiaotong University, he joined Hangzhou Normal University in 2013. His main research areas include classical and modern cryptography, and theory and technology of network security.