ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.4, April 2007, pp.1007−1014
DOI: 10.1360/jos181007

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

Forking 引理与一类基于身份签名体制的安全性证明*

顾纯祥[1+]， 祝跃飞[1]， 潘晓豫[2]

[1](信息工程大学 信息工程学院 网络工程系,河南 郑州 450002)
[2](河南省生产力促进中心,河南 郑州 450008)

Forking Lemma and the Security Proofs for a Class of ID-Based Signatures

GU Chun-Xiang[1+], ZHU Yue-Fei[1], PAN Xiao-Yu[2]

[1](Department of Network Engineering, Information Engineering College, Information Engineering University, Zhengzhou 450002, China)
[2](He'nan Productivity Promotion Center, Zhengzhou 450008, China)
+ Corresponding author: Phn: +86-371-63530540, E-mail: gcxiang5209@yahoo.com.cn

Gu CX, Zhu YF, Pan XY. Forking lemma and the security proofs for a class of ID-based signatures. *Journal of Software*, 2007,18(4):1007−1014. http://www.jos.org.cn/1000-9825/18/1007.htm

Abstract: This paper offers arguments for the provable security of a class of ID-based signature schemes called ID-based generic signature schemes in the random oracle model. The theoretical result can be viewed as an extension of the Forking Lemma due to Pointcheval and Stern for ID-based signature schemes, and can help to understand and simplify the security proofs of previous work such as Cha-Cheon's scheme, Hess's scheme-1, Cheon-Kim-Yoon's scheme, and so on.
Key words: ID-based signature; Forking lemma; provable security; existential forgery

摘 要: 在随机谕示模型下,研究一类基于身份的签名体制(称为基于身份的一般签名体制)的安全性.所得理论成果可以被看作 Pointcheval 和 Stern 提出的 Forking 引理在基于身份签名体制研究领域的扩展,有助于理解和简化一些现有的基于身份签名体制的安全性证明,如 Cha-Cheon 的体制、Hess 的体制 1 及 Cheon-Kim-Yoon 的体制等.
关键词: 基于身份的签名;Forking 引理;可证安全;存在性伪造
中图法分类号: TP309 文献标识码: A

1 Introduction

ID-based public key cryptography (ID-PKC) is a paradigm proposed by Shamir[1] in 1984 to simplify key management procedures of traditional certificate-based PKI. In ID-PKC, an entity's public key is derived directly from certain aspects of its identity, such as an IP address belonging to a network host, or an e-mail address associated with a user. Private keys are generated for entities by a trusted third party called a private key generator (PKG). The direct derivation of public keys in ID-PKC eliminates the need for certificates and some of the

* Supported by the National Natural Science Foundation of China under Grant Nos.90204015, 60473021 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035804 (国家重点基础研究发展规划(973))

Received 2005-08-26; Accepted 2005-11-09

problems associated with them.

In 2001, the first entire practical and secure ID-based encryption scheme was presented by Boneh and Franklin[2]. Since then, a rapid development of ID-PKC has taken place. Using bilinear pairings, many identity based primitives based on pairings were proposed: digital signatures[3−6], authenticated key exchange, non-interactive key agreement, blind and ring signatures, signcryption, and so on. ID-Based public key cryptography has become a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required.

Evaluating the "security" is a sticking point for the construction of new cryptographic scheme. Provable security based on complexity theory provides an efficient way for providing the convincing evidences of security. However, provable security standard model often is at the cost of an important loss in terms of efficiency[7]. In 1993, Bellare and Rogaway[8] provided the so-called "*random oracle model*" to help security proofs. In this model, concrete cryptographic objects, such as hash functions, are identified with ideal random objects. Since then, security proof in random oracle model becomes very popular for the security arguments of cryptographic scheme.

The general security notion for standard signature schemes is *existential unforgeable secure under adaptively chosen-message attacks* (EUF-ACMA)[7,9]. In 2000, Pointcheval and Stern[10] offered some security arguments for standard signature schemes in the random oracle model, and provided the famous Forking Lemma for *generic signature schemes*. An appropriate extension of EUF-ACMA for ID-based setting exists in Ref.[3], where the security notion of an ID-based signature scheme is defined to be *existential unforgeable secure under adaptively chosen message and ID attacks* (EUF-ACMIA). Recently, Bellare, *et al*.[11] provided security proofs for a class of ID-based signature schemes that can be constructed from a special kind of signature schemes called convertible signature schemes.

Inspired by Pointcheval's results, this paper presents security arguments for a class of ID-based signature schemes which we call *ID-based generic signature schemes* (ID-GSSs) in the random oracle model. The rest of this paper is organized as follows. In Section 2, we recall some preliminary work. In Section 3, we define a special kind of ID-based signature schemes as ID-GSSs, and construct a conversion from an ID-GSS to a generic signature scheme. In Section 4, we offer security arguments for ID-GSSs in the random oracle model. As an example, we show that Hess's scheme-1[4] can be easily proved to be secure with our theory in Section 5. Finally, we end the paper with a brief conclusion.

2 Preliminaries

2.1 Digital signature schemes and forking lemma

Definition 1. A digital signature scheme is defined by a triple of polynomial-time algorithms[10]:

- *Kgen*: On input 1^k, where k is the security parameter, the randomized key generation algorithm returns a pair (pk,sk) of matching public and secret keys.
- *Sign*: On input secret key sk and a message m, the possibly randomized signing algorithm returns a signature σ.
- *Verify*: On input public key pk, m and a signature σ, the deterministic verification algorithm tests whether σ is a valid signature for m corresponding pk.

The advantage in existentially forging of an adversary F, given access to a signing oracle $S(.)$ and a hash oracle $H(.)$, is defined as

$$Adv_F(k)=\Pr\left[\begin{matrix}(pk,sk)\leftarrow KGen(1^k),\ (m,\sigma)\leftarrow A^{S(.),H(.)}(pk):\\ Verify((m,\sigma),pk)=1,\ (m,\sigma)\notin S_{list}\end{matrix}\right].$$

where S_{list} is the query and answer list coming from $S(.)$ during the attack. The probability is taken over the coin tosses of the algorithms, of the oracles, and of the forger.

Definition 2. A digital signature scheme $\{KGen,Sign,Verify\}$ is said to be EUF-ACMA, if for any adversary F, $Adv_F(k)$ is negligible.

Pointcheval and Stern presented a notion of *generic signature scheme* which, given the input message m, produces a triple (σ_1,h,σ_2), where σ_1 randomly takes its values in a large set, h is the hash value of (m,σ_1) and σ_2 only depends on σ_1, the message m and h. Each signature is independent of the previous ones. They provided the famous Forking Lemma:

Lemma 1 [**Forking Lemma**][**10**]. In the random oracle mode, for a generic signature scheme, let F be a Turing machine whose input only consists of public data. Assume that F can produce a valid signature (m,σ_1,h,σ_2) within a time bound T by un-negligible probability $\varepsilon\geq 10(n_s+1)(n_h+n_s)/q$, where n_h and n_s are the number of queries that F can ask to the random oracle and the signing oracle respectively. If the triples (σ_1,h,σ_2) can be simulated without knowing the secret key, with an indistinguishable distribution probability, then there is another machine which has control over the machine obtained form F replacing the signing oracle by simulation and produces two valid signatures (m,σ_1,h,σ_2) and $(m,\sigma_1,h',\sigma_2')$ such that $h\neq h'$ in the expected time less than $120686\cdot n_h\cdot T/\varepsilon$.

2.2 Bilinear pairings

Let $(G_1,+)$,$(G_2,\cdot)$ be two cyclic groups of order q, $\hat{e}:G_1\times G_1\to G_2$ be a map with the following properties:

1. Bilinear: $P,Q\in G_1$, $\alpha,\beta\in Z_q$, $\hat{e}(\alpha P,\beta Q)=\hat{e}(P,Q)^{\alpha\beta}$;
2. Non-degenerate: If P is a generator of G_1, then $\hat{e}(P,P)$ is a generator of G_2;
3. Computable: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for any $P,Q\in G_1$.

Such an bilinear map is called an *admissible bilinear pairing*[2]. The Weil pairings and the Tate pairings of elliptic curves can be used to construct efficient admissible bilinear pairings.

Definition 3. Let P be a generator of G_1. The computation Diffie-Hellman problem (CDHP) is to compute abP for any given $P,aP,bP\in G_1$., where $a,b\in Z_q$. An algorithm F solves CDHP with the probability ε, if

$$\Pr[F(P,aP,bP)=abP]\geq\varepsilon.$$

where the probability is over the random choice of generator $P\in G_1$, the random choice of $a,b\in Z_q$, and random coins consumed by F.

No probabilistic polynomial time algorithm is known to solve CDHP with a non-negligible advantage so far. The hardness seems to be a reasonable assumption for the security proofs of cryptographic schemes.

3 ID-Based Generic Signature Schemes

Definition 4. An ID-based signature scheme consists of four polynomial-time algorithms[3]:

- *Setup*: The parameters generation algorithm takes as input a security parameter $k\in N$ (given as 1^k) and returns a master key s and system parameters Ω. This algorithm is performed by PKG. PKG publishes Ω while keeping s secretly.
- *Extract*: The private key generation algorithm takes as input an identity $ID\in\{0,1\}^*$ and extracts the secret key D_{ID}. This algorithm is performed by PKG. PKG gives D_{ID} to the user by a secure channel.
- *Sign*: The signing algorithm takes as input a private key D_{ID} and a message m and outputs a signature δ.
- *Verify*: The verification algorithm takes as input an identity ID, a message m and a signature δ, and outputs 0 or 1. The later implies δ is a valid signature.

An ID-based digital signature scheme is said to be EUF-ACMIA, if for any polynomial-time adversary F, the advantage defined by

$$Adv_F(k)=\Pr\begin{bmatrix}\Omega\leftarrow Setup(1^k), & (ID,m,\delta)\leftarrow F^{S(.),E(.)}(para): \\ verify((m,\delta),ID)=1, & (ID,m,\delta)\notin S_{list},(ID,.)\notin E_{list}\end{bmatrix}$$

is negligible, where S_{list} and E_{list} are the query and answer lists coming from Sign oracle S(.) and Extract oracle E(.) respectively during the attack. In the random oracle model, the attackers also have the ability to query to the random oracles. The probability is taken over the coin tosses of the algorithms of the oracles and of the forger.

Many existed ID-based signature schemes that are constructed with bilinear pairings, such as Ref.[3−5], have the same **Setup** and **Extract** algorithms as follows:

- *Setup*: Take as input a security parameter $k\in N$, and returns a master key s and system parameters $\Omega=\{G_1,G_2,q,\hat{e},P,P_{pub},H_1,H_2\}$, where $(G_1,+),(G_2,\cdot)$ are cyclic groups of order q, $\hat{e}:G_1\times G_1\rightarrow G_2$ is an admissible bilinear map, $H_1:\{0,1\}^*\rightarrow G_1^*$ and H_2 are hash functions.
- *Extract*: Take as input an identity $ID\in\{0,1\}^*$, computes $Q_{\mathrm{ID}}=H_1(ID)$,$D_{\mathrm{ID}}=sQ_{\mathrm{ID}}$, and lets D_{ID} be the user's secret key.

Generally speaking, the user's public key for verification is in fact $Q_{\mathrm{ID}}=H_1(ID)$. Hence, we may sometimes use *Verify*$(Q_{\mathrm{ID}},m,\delta)$ and $(Q_{\mathrm{ID}},m,\delta)$ instead of *Verify*(ID,m,δ) and (ID,m,δ) respectively.

In this paper, we consider a special kind of ID-based signature schemes, which given input a message m, produce triples (σ_1,h,σ_2), where σ_1 randomly takes its values in a large set, h is the hash value of (m,σ_1) and σ_2 only depends on σ_1 and h for a fixed private key D_{ID}. Each signature is independent of the previous ones. That is, we assume that no σ_1 can appear with probability greater than $2/2^k$, where k is the security parameter. We call this kind of pairing-based schemes as *ID-based generic signature schemes* (ID-GSSs).

Let Σ={*Setup*,*Extract*,*Sign*,*Verify*} be a standard ID-based signature scheme, we can construct an ordinary signature scheme Γ={*KGen*,*Sign*′,*Verify*′} as following:

Construction

- *KGen*: On input 1^k, set $(s,\Omega)\leftarrow Setup(1^k)$, pick randomly $ID\in\{0,1\}^*$, compute $Q=H_1(ID)$, $D=sQ$, and return D as private key and (Ω,Q) as public key.
- *Sign*′: On input private key D and a message m, set Ω as the system parameters, compute and output $\delta=Sign(D,m)$.
- *Verify*′: On input public key (Ω,Q), a message m and a signature δ, set Ω as the system parameters, compute and output *Verify*(Q,m,δ).

Here, we say that Γ is a signature scheme constructed from Σ.

Lemma 2. If a standard ID-based signature scheme Σ is an ID-GSS, then the signature scheme constructed from Σ is a generic signature scheme.

Proof: Let Γ={*KGen*,*Sign*′,*Verify*′} be the ordinary signature scheme constructed from Σ. For a key pair $((\Omega,Q),D)$ generated by *KGen*(1^k), given the input m, the signing algorithm of Γ produces a signature δ which is the same as that produced by the ID-based signing algorithm of Σ with the system parameters being Ω and user's identity being ID. Σ is an ID-GSS. Hence δ is a triple (σ_1,h,σ_2), where σ_1 randomly takes its values in a large set, h is the hash value of (m,σ_1) and σ_2 only depends on σ_1, the message m and h. Each signature is independent of the previous ones. That is, Γ is a generic signature scheme.

4 Provable Security of ID-Based Generic Signature Schemes

In this section, we extend the results on the security of generic signature schemes to ID-GSSs. Let

Σ={*Setup*,*Extract*,*Sign*,*Verify*} be an ID-GSS, Γ={*KGen*,*Sign*′,*Verify*′} be the generic signature scheme that is constructed from Σ.

Lemma 3. In the random oracle model, assume that there is an adversary F_0 whose input only consists of public data, and can produce a valid signature $(ID,m,\sigma_1,h,\sigma_2)$ of Σ, within a time bound T by un-negligible probability ε. We denote by n_{h1}, n_s and n_E the number of queries that F_0 can ask to the oracles $H_1(.)$, *Sign*(.) and *Extract*(.) respectively. Then there is another adversary F_1 who can produce a valid signature of Γ, within the expected time $T+(n_{h1}+n_s+n_E)t_1+n_st_2$ with the un-negligible probability ε/n_{h1}, where t_1 denotes a scalar multiplication in $(G_1,+)$ and t_2 denotes a signing operation.

Proof: Without any loss of generality, we may assume that for any *ID*, F_0 queries $H_1(.)$ with *ID* before *ID* is used as (part of) an input of any query to $H_2(.)$, *Extract*(.) and *Sign*(.). From F_0, we can construct a probabilistic algorithm F_1 as follows:

1. A challenger $\mathcal{C}$ runs $((\Omega,Q),D)\leftarrow KGen(1^k)$, where $\Omega=\{G_1,G_2,q,\hat{e},P_{pub},H_1,H_2\}$, and gives (Ω,Q) to F_1.
2. F_1 picks u, $1\le u\le n_{h1}$ and $x_i\in Z_q$ $i=1,2,\ldots,n_{h1}$ randomly.
3. F_1 runs F_0 with input Ω. During the execution, F_1 emulates F_0's oracles as follows:
   - $H_1(.)$: For input *ID*, F_1 checks if $H_1(ID)$ is defined. If not, he defines
   - $H_1(ID)=\begin{cases}Q, & i=u\\ x_iP, & i\ne u\end{cases}$**,** and sets $ID_i\leftarrow ID$, $i\leftarrow i+1$. F_1 returns $H_1(ID)$ to F_0.
   - $H_2(.)$: For input (m,σ_1), F_1 checks if $H_2(m,\sigma_1)$ is defined. If not, F_1 picks $c\in Z_q$ randomly, sets $H_2(m,\sigma_1)=c$. F_1 returns $H_2(m,\sigma_1)$ to F_0.
   - *Extract*(.): For input ID_i, if $i=u$, then abort. Otherwise, F_1 lets $D_i=x_iP_{pub}$ be the reply to F_0.
   - *Sign*(.): For ID_i and message m, if $i\ne u$, F_1 computes $D_i=x_iP_{pub}$, $(\sigma_1,h,\sigma_2)=Sign(D_i,m)$. Otherwise, F_1 requests to his own signing oracle *Sign*′(.) with input m and gets (σ_1,h,σ_2). F_1 replies to F_0 with (σ_1,h,σ_2).
4. If F_0's output is $(ID_i,m^*,\sigma_1^*,h^*,\sigma_2^*)$ satisfying: $Verify(ID_i,m^*,\sigma_1^*,h^*,\sigma_2^*)=1$, and $i=u$, F_1 can get a forgery $(m^*,\sigma_1^*,h^*,\sigma_2^*)$ of Γ corresponding to (Ω,Q).

F_1's running time is roughly the same as F_0's running time plus the time taken to respond to F_0's oracle queries. If we neglect operations other than signing and scalar multiplication in $(G_1,+)$, the total running time is bounded by $T+(n_{h1}+n_s+n_E)t_1+n_st_2$. Because u is chosen randomly, F_1 can output a forgery corresponding to (Ω,Q) of Γ with probability ε/n_{h1}.

Theorem 1. In the random oracle mode, let F_0 be an adversary whose input only consists of public data, and can produce a valid signature $(ID,m,\sigma_1,h,\sigma_2)$ of Σ within a time bound T by the un-negligible probability $\varepsilon\ge 10n_{h1}(n_s+1)(n_{h2}+n_s)/q$, where n_{h1}, n_{h2}, n_s and n_E are the number of queries that F_0 can ask to the oracles $H_1(.)$, $H_2(.)$, *Sign*(.) and *Extract*(.) respectively. If the triples (σ_1,h,σ_2) can be simulated without knowing the secret key with an indistinguishable distribution probability, then there is another machine F_1, given $Q\in G_1^*$, which can produce two valid signatures (m,σ_1,h,σ_2) and $(m,\sigma_1,h',\sigma_2')$ of Γ for public key (Ω,Q), such that $h\ne h'$ in the expected time less than $120686\cdot n_{h1}\cdot n_{h2}(T+(n_{h1}+n_s+n_E)t_1+n_st_2)/\varepsilon$, where t_1 denotes a scalar multiplication in $(G_1,+)$ and t_2 denotes a signing operation.

Proof: With Lemma 3, from F_0, we can construct an adversary F_1, given (Ω,Q), which can produce a valid signatures (m,σ_1,h,σ_2) of Γ within the expected time $T+(n_{h1}+n_s+n_E)t_1+n_st_2$ with the un-negligible probability ε/n_{h1}. With Lemma 1, there is a machine F_2 which has control over the machine obtained from F_1 replacing interaction with the signer by simulation, and can produce two valid signatures (m,σ_1,h,σ_2) and $(m,\sigma_1,h',\sigma_2')$ such that $h\ne h'$ in the expected time less than $120686\cdot n_{h1}\cdot n_{h2}(T+(n_{h1}+n_s+n_E)t_1+n_st_2)/\varepsilon$.

5 Applications

As an example, we show that Hess's scheme-1[4] can be proved to be secure with our theorem. The scheme consists of four algorithms:

- *Setup*: Takes as input a security parameter $k\in N$, output a master key s and system parameters $\Omega=\{G_1,G_2,q,\hat{e},P,P_{pub},H_1,H_2\}$, where $(G_1,+)$, $(G_2,\cdot)$ are cyclic groups of order q, $\hat{e}:G_1\times G_1\rightarrow G_2$ is an admissible bilinear map, H_1:$\{0,1\}^*\rightarrow G_1^*$ and H_2: $\{0,1\}^*\times G_2\rightarrow Z_q^*$ are hash functions.
- *Extract*: Takes as input an identity $ID\in\{0,1\}^*$, compute $Q_{\mathrm{ID}}=H_1(ID)$, $D_{\mathrm{ID}}=sQ_{\mathrm{ID}}$, and let D_{ID} be the user's secret key.
- *Sign*: For input secret key D_{ID} and a message m, select $t\in t\in Z_q^*$ randomly, compute $r=\hat{e}(P,P)^t$, $c=H_2(m,r)$, $U=c\cdot D_{\mathrm{ID}}+t\cdot P$, and output (r,c,U).
- *Verify*: For input of an identity ID, a message m and a signature (r,c,U), the verifier computes $c=H_2(m,r)$, and checks whether $r=\hat{e}(U,P)\hat{e}(H_1(ID),P_{pub})^{-c}$.

Obviously, Hess's scheme-1 is an ID-GSS. We now prove that the triples (r,c,U) can be simulated without the knowledge of the signer's secret key.

Lemma 4. Given $(G_1,G_2,q,\hat{e},P,P_{pub}=sP,H_1,H_2)$ and an identity ID, $Q=H_1(ID)$, $D=sQ$, the following distributions are the same.

$$\delta=\left\{(r,c,U)\left|\begin{array}{l}t\in_R Z_q^{\ *}\\ c\in_R Z_q\\ r=\hat{e}(P,P)^t\\ U=cD+tP\end{array}\right.\right\}\text{ and }\delta'=\left\{(r,c,U)\left|\begin{array}{l}U'\in_R G_1\\ c\in_R Z_q\\ U=U'\\ r=\hat{e}(U,P)\hat{e}(Q,P_{pub})^{-c}\\ r\neq 1\end{array}\right.\right\}.$$

Proof: First we choose a triple (α,β,γ) from the set of the signatures: Let $\alpha\in G_2^*$, $\beta\in Z_q$, $\gamma\in G_1$ such that $\alpha=\hat{e}(\gamma,P)\hat{e}(Q,P_{pub})^{-\beta}\neq 1$. We then compute the probability of appearance of this triple, following each distribution of probabilities:

$$\Pr_{\delta}[(r,c,U)=(\alpha,\beta,\gamma)]=\Pr_{t\neq 0}\begin{bmatrix}\hat{e}(P,P)^t=\alpha\\ c=\beta\\ c\cdot D+t\cdot P=\gamma\end{bmatrix}=\frac{1}{q(q-1)},$$

$$\Pr_{\delta'}[(r,c,U)=(\alpha,\beta,\gamma)]=\Pr_{r\neq 1}\begin{bmatrix}\alpha=r=\hat{e}(U',P)\hat{e}(Q,P_{pub})^{-c}\\ c=\beta\\ U=U'=\gamma\end{bmatrix}=\frac{1}{q(q-1)}.$$

That is, we can construct a simulator M, which produces triples (r,c,U) with an identical distribution from those produced by the signer as follows:

- Simulator M: For input $(G_1,G_2,q,\hat{e},P,P_{pub}=sP,H_1,H_2)$, $H_1(ID)$ and a message m, randomly choose $U'\in G_1$, $c\in Z_q$, and set $U=U'$ and $r=\hat{e}(U,P)(\hat{e}(H_1(ID),P_{pub}))^{-c}$. In the (unlikely) situation where $r=1$, we discard the results and restart the simulation. Then it returns the triple (r,c,U).

Theorem 2. In the random oracle mode, let F_0 be an adversary who performs, within a time bound T, an existential forgery against the Hess's scheme-1, with probability $\varepsilon\geq 10n_{h1}(n_s+1)(n_{h2}+n_s)/q$, where n_{h1}, n_{h2}, n_s and n_E are the number of queries that F_0 can ask to the oracles $H_1(.)$, $H_2(.)$, *Sign*(.) and *Extract*(.) respectively. Then the computational Diffie-Hellman problem in G_1 can be solved within the expected time less than $120686\cdot n_{h1}\cdot n_{h2}(T+(n_{h1}+n_s+n_E)t_1+n_st_2)/\varepsilon$, where t_1 denotes a scalar multiplication in $(G_1,+)$ and t_2 denotes a signing operation.

Proof: From Lemma 4, we can see that a valid signature of Hess's scheme-1 (r,c,U) can be simulated without knowing the secret key, with an indistinguishable distribution probability. With Theorem 1, using adversary F_0, we can construct another adversary F_1, given $Q \in G_1^*$, and produce two valid signatures (m,r,c,U) and (m,r,c',U') such that $c \neq c'$ in expected time less than $120686 \cdot n_{h1} \cdot n_{h2}(T+(n_{h1}+n_s+n_E)t_1+n_st_2)/\varepsilon$.

From the adversary F_1, we can construct a probabilistic algorithm F_2 such that F_2 computes abP on input of any given $P, aP, bP \in G_1^*$ as follows:

1. A challenger C runs $Setup(1^k)$ to generate system parameters $\Omega = (G_1, G_2, q, \hat{e}, P, P_{pub}, H_1, H_2)$ and gives F_2 with $P, aP, bP \in G_1^*$.
2. F_2 sets $P_{pub}=aP$, and $\overline{\Omega} = (G_1, G_2, q, \hat{e}, P, aP, H_1, H_2)$.
3. F_2 runs F_1 with input $(\overline{\Omega}, bP)$ until F_1 outputs two valid signatures (m,r,c,U) and (m,r,c',U') such that $c \neq c'$.
4. F_2 can compute and output abP as follows:

$$\xi=(c-c')^{-1} \bmod q,\ abP=\xi(U-U').$$

Analogical results can be obtained for many such schemes, such as Cha-Cheon's scheme[3], Cheon-Kim-Yoon's scheme[5], and so on.

In fact, the reduction efficiency of our proof is roughly the same as that of the proofs proposed by the authors in the original papers[3−5]. For instance, in Ref.[4], the authors proved that CDHP can be solved in the expected time $c \cdot n_{h1} \cdot n_{h2}T/\varepsilon$ if there is an ACMA adversary making an existential forgery with probability $\varepsilon \geq a \cdot n_{h1} \cdot n_{h2}n_s/q$ in the random oracle model, where $a,c \in Z^{\geq 1}$ are constants. However, the security proof in Ref.[4] seems long and too abstruse.

6 Conclusion

This paper successfully extends the Forking Lemma for ID-based signature schemes. Using the result of this paper, a large class of ID-based signature schemes, which we called *ID-based generic digital signature schemes*, can be proved to be secure easily in the random oracle model.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Advances in Cryptology—CRYPTO'84. LNCS 196, Berlin, Heidelberg, New York: Springer-Verlag, 1984. 47−53.

[2] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, eds. Advances in Cryptology—CRYPTO 2001. LNCS 2139, Berlin, Heidelberg, New York: Springer-Verlag, 2001. 213−229.

[3] Cha JC, Cheon JH. An identity-based signature from gap Diffie-Hellman groups. In: Public Key Cryptography—PKC 2003. LNCS 2567, Berlin, Heidelberg, New York: Springer-Verlag, 2003. 18−30.

[4] Hess, F. Efficient identity based signature schemes based on pairings. In: Selected Areas in Cryptography the 9th Annual Int'l Workshop, SAC 2002. LNCS 2595, Berlin, Heidelberg, New York: Springer-Verlag, 2003. 310−324.

[5] Yoon HJ, Cheon JH, Kim Y. Batch verifications with ID-based signatures. In: Information Security and Cryptology—ICISC 2004. LNCS 3506, Berlin, Heidelberg, New York: Springer-Verlag, 2005. 233−248.

[6] Paterson KG. ID-Based signatures from pairings on elliptic curves. Electronics Letters, 2002,38(18):1025−1026. http://eprint.iacr/org/2002/004

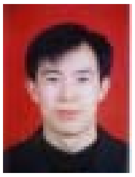
[7] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen message attacks. SIAM Journal of Computing, 1988,17(2):281−308.

[8] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st CCCS. New York: ACM Press, 1993. 62−73.

[9] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. In: Proc. of the STOC'98. ACM Press, 1998. 209−218.

[10] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000,13(3):361−369.

[11] Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes. In: Proc. of the Eurocrypt 2004. LNCS 3027, Berlin, Heidelberg, New York: Springer-Verlag, 2004. 268−286.



GU Chun-Xiang was born in 1976. He is a Ph.D. candidate at the Information Engineering University. His research areas are cryptography and information security.

ZHU Yue-fei was born in 1962. He is a professor and doctoral supervisor at the Information Engineering University and a CCF senior member. His research areas are cryptography and information security.

PAN Xiao-Yu was born in 1977. Her research area is information engineering.

****

全国教育游戏与虚拟现实学术会议(**EGVR 2007**)

征文通知

2007 年 8 月 19~21 日，大连

主办：中国图象图形学会虚拟现实专业委员会、中国教育技术协会信息技术教育专业委员会

承办：辽宁师范大学

协办：大连民族学院、中国系统仿真学会数字娱乐仿真专业委员会、浙江大学数字娱乐与动画研究中心、南京师范大学教育游戏研究中心、中国传媒大学数字技术与艺术研发中心

全国教育游戏与虚拟现实学术会议(EGVR 2007)将于 2007 年 8 月 19 日至 21 日在大连举行，它是虚拟现实、图形学、教育与游戏产业最新研究成果与产品的交流平台，是将于 2007 年在香港举行的“电子学习与数字娱乐国际会议”(Edutainment) 的姐妹会议。本次大会的内容包括学术报告、专题研讨、最新成果和应用系统演示，并邀请国内外著名专家到会作特邀报告。会议录用论文将结集出版，优秀论文将推荐到《计算机辅助设计与图形学学报》、《中国图象图形学报》、《系统仿真学报》等国内一级学报与核心期刊发表。热诚欢迎一切从事图形学、虚拟现实、教育技术以及游戏产业界的专家、学者和专业技术人员踊跃投稿。

EGVR 2007 会议的议题包括：图形学、虚拟现实、游戏设计与开发、游戏引擎开发与定制、游戏中的人工智能与人工生命、游戏中的物理学、游戏渲染与动画、虚拟人物与 Agent、在线游戏/移动游戏/视频游戏、编故事和故事叙述、游戏中的情感交互、E-learning 标准平台与工具、学习资源管理、体验型学习、教育与远程课堂、协同学习环境、移动学习与协同学习、教育中的虚拟现实技术、动画技术在教学中的应用、增强现实与混合现实在教学中的应用、教育游戏在教育教学中的应用等。

征文要求：(1) 论文未被其它会议、期刊录用或发表，中文撰写；(2) 要求电子投稿 (Word 版本)；(3) 论文包含题目、中英文摘要、正文、参考文献等，正式格式见录用通知；(4) 务必写清论文联系人的姓名、单位、通信地址、联系电话及 E-mail。

重要日期：征稿截止：2007 年 05 月 15 日 (最后收到日期)
录用日期：2007 年 06 月 15 日 (最后发出日期)
最终稿件：2007 年 06 月 20 日 (最后收到日期)

投稿邮箱：egvr2007@lnnu.edu.cn

更多详情请登陆网站了解：http://www.egvr2007.lnnu.edu.cn