An Identity-based Mediated Signature Scheme from Bilinear Pairing

Xiangguo Cheng[1,2], Lifeng Guo[2,3], Xinmei Wang[1]
(Corresponding author: Xiangguo Cheng)

State Key Laboratory of Integrated Services Network, Xidian University[1]
Xi'an 710071, P.R.China (Email: xgcheng, xmwang@xidian.edu.cn)
Infocommm Security Department, Institute for Infocomm Research (I^2R)[2]
21 Heng Mui Keng Terrace, Singapore 119613 (Email: stuxgc, stulguo@i2r.a-star.edu.sg)
Institute of Systems Science, Academy of Mathematics and System Sciences, Chinese Academy of Sciences[3]
Graduate School of Chinese Academy of Sciences, Beijing 100080, P.R. China (Email: lfguo@amss.ac.cn)

(Received June 30, 2005; revised and accepted July 31, 2005)

Abstract

It has always been a critical issue to find efficient methods for fast revocation of a user's identity in identity (ID)-based cryptosystems. Unfortunately, none of the previous ID-based cryptography can find a practical way. Libert *et al.* and Baek *et al.* respectively propose an ID-based mediated encryption scheme based on the practical ID-based encryption scheme from bilinear pairing due to Boneh and Franklin. Both schemes provide an efficient method for immediate revocation of a user's identity. However, no ID-based mediated signature scheme from bilinear pairing has been found so far. The essential reason is that most of the previous ID-based signatures from bilinear pairing are no "good" enough to generate their mediated versions. In this paper, we first presents an ID-based signature scheme from bilinear pairing. It is secure against existential forgery under adaptively chosen message and ID attack in the random oracle model. Furthermore, it has the good property of addition, thus can be used to construct an efficient ID-based mediated signature scheme. Combining this scheme with one of the above two mediated encryption schemes yields a complete solution to the fast revocation of a user's identity in ID-based cryptosystems from bilinear pairing.

Keywords: Bilinear pairing, GDH group, ID-based mediated signature, ID-based signature

1 Introduction

The concept of an ID-based cryptosystem was first introduced by Shamir [1] in 1984. The main idea of such a cryptosystem is that each user uses his identity information such as *name*, *telephone number* or *email address* as his public key. In other words, the user's public key can be calculated directly from his identity rather than being extracted from a certificate issued by a certificate authority. ID-based cryptosystems enable any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted Private Key Generator (PKG) issues a private key corresponding to each user's identity when he first joins the network. Compared to certificate-based cryptosystems, ID-based cryptosystems have simplified key management since there is no need to maintain a great database containing a list of public keys and their respective owners. However, one inherent drawback of current ID-based cryptosystems is that they cannot provide an efficient solution to immediately revoke a user's identity. The typical way to obtain revocation of a user's identity in ID-based cryptosystems is to concatenate a validity period to an identity string. Revocation is achieved by instructing PKG to stop issuing new private keys for revoked identities. This involves the need to periodically re-issue all private keys in the system and the PKG must be online most of the time. The user's identity cannot be immediately revoked using this method.

Boneh *et al.* introduced a method for obtaining fast revocation of a user's public key privilege in RSA-based cryptosystems. They call this scheme *mediated RSA* (mRSA) [2]. The main idea behind mRSA is to introduce a special online entity, called a SEcurity Mediator (SEM) in standard RSA. To sign or decrypt a message, Alice must first obtain a message-specific token from the SEM. Without this token Alice cannot use her private key. To revoke Alice's ability to sign or decrypt, the administrator instructs the SEM to stop issuing tokens for Alice's public key. Alice's signature or decryption capabilities can therefore be revoked.

Boneh and Franklin first gave a practical ID-based encryption scheme from Weil pairing [3] in 2001. Based on this scheme, Libert and Quisquater [4], Baek and Zheng [5] respectively proposed an ID-based mediated encryption scheme using the similar method given in mRSA. Both schemes provide an efficient method to immediately revoke a user's identity. But, to our best knowledge, no ID-based mediated signature scheme from pairing has been found so far. Several ID-based signature schemes from pairing have been proposed [6, 7, 8, 9]. However, all these signatures are no "good" enough to be used to construct an efficient ID-based mediated signature scheme. To construct an efficient ID-based mediated signature scheme, we first review an ID-based signature scheme from bilinear pairing given in [11]. It is in fact a variant of the ID-based signature given by Yi [9] and is proven to be secure against existential forgery under adaptively chosen message and ID attack in the random oracle model. It is simple, efficient and has the good property of addition, thus can be used to construct an ID-based mediated signature scheme. Combining our mediated signature scheme with [4] or [5] yields an ID-based mediated cryptosystem from bilinear pairing and provides a complete solution to the fast revocation of the user's identity in ID-based cryptosystems from bilinear pairing.

The remaining sections are organized as follows. Section 2 briefly introduces some related mathematical problems. We recall the ID-based signature scheme and analyze its security in Section 3. Based on this ID-based signature scheme, we come up with an ID-based mediated signature scheme and give its security analysis in Section 4. Conclusion is drawn in the last section.

2 Preliminaries

2.1 Bilinear Pairing

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) *Bilinear:* $e(aR_1, bR_2) = e(R_1, R_2)^{ab}$ for any $a, b \in \mathbb{Z}_q$ and $R_1, R_2 \in G_1$.

2) *Non-degenerate:* There exists $R_1, R_2 \in G_1$ such that $e(R_1, R_2) \neq 1$. Which means that $e(P, P) \neq 1$ since P is the generator of the cyclic group G_1.

3) *Computable:* For all $R_1, R_2 \in G_1$, $e(R_1, R_2)$ can be computed efficiently.

2.2 Diffie-Hellman Problem

Assuming that the *Discrete Logarithm* (DL) problem in G_1 and G_2 is hard. We consider the following two problems in G_1.

1) *Computational Diffie-Hellman* (CDH) problem: Given$P, aP, bP \in G_1$ for all $a, b \in \mathbb{Z}_q^*$, compute $abP \in G_1$.

2) *Decisional Diffie-Hellman* (DDH) problem: Given $P, aP, bP, cP \in G_1$ for all $a, b, c \in \mathbb{Z}_q^*$, decide whether $c \equiv ab \bmod q$.

We call G a *Gap Diffie-Hellman* (GDH) group if DDH problem is easy while CDH problem is hard in G. The hardness of CDH problem in a group is generally considered to be dependent on the hardness of DL problem in the group. However, DDH problem becomes easy by introducing a bilinear pairing since $c \equiv ab \bmod q$ if and only if $e(aP, bP) = e(P, cP)$. That is to say, we can obtain GDH groups from bilinear pairing. Such groups can be found on super-singular elliptic curves or hyper-elliptic curves over the finite fields, and the bilinear pairing can be derived from the Weil or Tate pairing [3, 10].

Schemes in this paper can work on any GDH group. Throughout this paper, we define the system parameters in all schemes as follows: G_1, G_2, P, q and e are as described above. These system parameters can be obtained using a GDH Parameters Generator [3, 10]. Define two cryptographic hash functions: $H_1 : \{0,1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$ and $H_2 : \{0,1\}^* \rightarrow G_1$. All these parameters are denoted as $Params = \{G_1, G_2, e, q, P, H_1, H_2\}$.

3 ID-Based Signature and Its Security

3.1 ID-based Signature Scheme

Our ID-based signature scheme is based on GDH groups. It is in fact a variant of the ID-based signature scheme given by Yi [9]. the security analysis of the scheme can be found in [11]. An ID-based signature consists of *four* algorithms: system setup algorithm `Setup`, private key extraction algorithm `Extract`, signature generation algorithm `Sign` and signature verification algorithm `Verify`. They are described as follows.

1) `Setup`: Given a security parameter κ, PKG runs the GDH Parameters Generator to obtain $Params = \{G_1, G_2, e, m, P, H_1, H_2\}$. Then it picks a random number $s \in \mathbb{Z}_q^*$ as a master key and computes the system public key $P_{pub} = sP$. P_{pub} is published but s is kept secretly.

2) `Extract`: Given a user's identity ID. PKG computes $Q_{ID} = H_2(ID)$, $D_{ID} = sQ_{ID}$ and sends D_{ID} to the user via a secure channel. The user's private key is D_{ID}.

3) `Sign`: Given a message M, the signer randomly picks a number $r \in \mathbb{Z}_q^*$ and computes $R = rP$, $h = H_1(M, R)$ and $S = rP_{pub} + hD_{ID}$. The signature on message M is set to be $\sigma = (R, S)$.

4) `Verify`: Given a signature $\sigma = (R, S)$ on message M under ID, the verifier computes $h = H_1(M, R)$, $Q_{ID} = H_2(ID)$ and $T = R + hQ_{ID}$. He accepts the signature if $e(P, S) = e(P_{pub}, T)$.

Correctness of the signature:
If $\sigma = (R, S)$ is a valid signature on M under ID, then

$$\begin{aligned} e(P,S) &= e(P, rP_{pub} + hD_{ID}) = e(P, rsP + hsQ_{ID}) \\ &= e(P, s(rP + hQ_{ID})) = e(P, s(R + hQ_{ID})) \\ &= e(P, sT) = e(sP, T) = e(P_{pub}, T) \end{aligned}$$

Theorem 3.1. *The proposed ID-based signature is secure against existential forgery under adaptively chosen message and ID attack in the random oracle model with the assumption that G_1 is a GDH group.*

Proof. Two security notion models of an ID-based signature scheme are presented in [6]: *adaptively chosen message and ID attack* and *adaptively chosen message and given ID attack*. The readers can refer to [6] for more details. Note that the *adaptively chosen message and given ID attack* is in fact the security notion model of a general signature scheme.

Using the same methodology given in [6], we can easily prove that, if there exists an efficient algorithm $\mathcal{A}$ for an *adaptively chosen message and ID attack* to our scheme, then, making use of $\mathcal{A}$, we can construct an algorithm $\mathcal{B}$, with the same advantage as $\mathcal{A}$, for an *adaptively chosen message and given ID attack* to our scheme. That is to say, if our scheme is secure against *adaptively chosen message and given ID attack*, it is also secure against *adaptively chosen message and ID attack*. In the following we only need to show that our scheme is secure against *adaptively chosen message and given ID attack*.

Given an identity ID, the corresponding public-private key pair is (Q_{ID}, D_{ID}). According to the Forking Lemma in [12], if there exists an efficient algorithm $\mathcal{B}$ for an *adaptively chosen message and given ID attack* to our scheme, then there exists an efficient algorithm $\mathcal{C}$ which can produce two valid signatures (M, R, h_1, S_1) and (M, R, h_2, S_2) such that $h_1 \neq h_2$. Based on $\mathcal{C}$, an algorithm $\mathcal{F}$, which is as efficient as $\mathcal{C}$, can be constructed as follows: Let inputs to $\mathcal{F}$ be P,$P_{pub} = sP$ and $Q_{ID} = tP$ for some $t \in \mathbb{Z}_q^*$. $\mathcal{F}$ chooses a message M and runs algorithm $\mathcal{C}$ to obtain two forgeries (M, R, h_1, S_1) and (M, R, h_2, S_2) such that $h_1 \neq h_2$ and satisfy equations $e(P, S_1) = e(P_{pub}, R + h_1Q_{ID})$ and $e(P, S_2) = e(P_{pub}, R + h_2Q_{ID})$. That is, $e(P, (S_1 - S_2) - (h_1 - h_2)D_{ID}) = 1$. Since e has the property of non-degeneracy, we have $(S_1 - S_2) - (h_1 - h_2)D_{ID} = O$ and $D_{ID} = (h_1 - h_2)^{-1}(S_1 - S_2)$. It means that $\mathcal{F}$ can solve an instance of CDH problem in G_1 since $D_{ID} = sQ_{ID} = stP$.

There is no efficient algorithm for an *adaptively chosen message and given ID attack* to our scheme since G_1 is a GDH group and CDH problem in G_1 is hard. Therefore, our scheme is secure against *existential forgery under adaptively chosen message and ID attack*. □

4 ID-Based Mediated Signature and Its Security

4.1 ID-Based Mediated Signature Scheme

The main idea behind an ID-based mediated signature scheme is to introduce a trusted online party, called a Security Mediator (SEM), in a general ID-based signature scheme. A user's private key corresponding to his ID is split into two parts. One part is given to the user, and another is given to the SEM. Therefore, only with the help of the SEM, can a user generate a valid signature. As a result, an immediate revocation of a user's ID (*i.e.* a user's signing privilege) is possible by instructing the SEM not to help him any more.

Based on the aforementioned ID-based signature scheme, we come up with an ID-based mediated signature scheme. This scheme consists of three entities: *PKG*, *SEM* and *users*, there are four algorithms: `Setup`, `MeExtract`, `MeSign` and `Verify`. The PKG governs the SEM and a SEM can serve many users. Two of the algorithms, `Setup` and `Verify`, are analogous to those in original signature. The others, `MeExtract` and `MeSign`, provide the mediated signature capability. They are described as follows:

1) `Setup`: Sharing the same system parameters with underlying signature scheme. $s \in \mathbb{Z}_q^*$ is the master key and $P_{pub} = sP$ is the public key of the system, respectively.

2) `MeExtract`: Given an identity ID, PKG chooses a random number s_1 from $\mathbb{Z}_q^*$, computes $Q_{ID} = H_2(ID)$, $D_{ID}^{user} = s_1Q_{ID}$ and $D_{ID}^{sem} = (s - s_1)Q_{ID}$. D_{ID}^{user} is sent secretly to the user whose identity is ID as his private key and (D_{ID}^{sem}, ID) is sent to the SEM.

3) `MeSign`: To sign a message M, the user interacts with the SEM to do as follows:

   - The user chooses a random number $r_1 \in \mathbb{Z}_q^*$ and computes $R_1 = r_1P$. The triple (M, R_1, ID) is sent to the SEM.
   - The SEM first checks that the user's ID is not revoked. It then picks a random number r_2 from $\mathbb{Z}_q^*$ and computes $R_2 = r_2P$, $R = R_1 + R_2$, $h = H_1(M, R)$ and $S_{sem} = r_2P_{pub} + hD_{ID}^{sem}$. The pair (R, S_{sem}) is then sent back to the user.
   - After having received (R, S_{sem}), the user computes $h = H_1(M, R)$, $S_{user} = r_1P_{pub} + hD_{ID}^{user}$ and $S = S_{user} + S_{sem}$. He verifies whether $e(P, S) = e(P_{pub}, R + hQ_{ID})$ holds. If so, the signature on message M under ID is set to be $\sigma = (R, S)$.

4) `Verify`: Given a signature $\sigma = (R, S)$ on message M under ID, the verifier computes $h = H_1(M, R)$,

$Q_{ID} = H_2(ID)$ and $T = R + hQ_{ID}$. He accepts the signature if $e(P,S) = e(P_{pub}, R + hQ_{ID})$.

We note that

$$\begin{aligned} S &= S_{user} + S_{sem} \\ &= (r_1 P_{pub} + hD_{ID}^{user}) + (r_2 P_{pub} + hD_{ID}^{sem}) \\ &= (r_1 + r_2)P_{pub} + h(D_{ID}^{user} + D_{ID}^{sem}) \\ &= rP_{pub} + hD_{ID} \end{aligned}$$

where $r = r_1 + r_2$ is in fact a number in $\mathbb{Z}_q^*$ such that $R = rP$. Therefore, $\sigma = (R, S)$ is only a general ID-based signature and the verifier needs only verify it using the general `Verify` algorithm. Furthermore, the verifier need not verify whether the user's signing privilege has been revoked since the SEM does not help any user whose ID has been revoked in a signature process.

4.2 Security Analysis of the Scheme

We note that the only functionality of the SEM is to revoke a user's signing privilege. It cannot generate a valid signature of some message on behalf of its users since it does not know the private keys of the users and the users never send it their partial signatures in the signature protocol.

Suppose that an attacker is able to compromise the SEM and expose the secret key D_{ID}^{sem} corresponding to an ID. This enables the attacker to "un-revoke" previously revoked, or block possible future revocation of current valid, identities. However, the knowledge of D_{ID}^{sem} does not enable the attacker to sign messages on behalf of its users since the generation of a valid signature needs a cooperation of the SEM and the signer.

Let us consider an attacker trying to forge a user's signature on some message. Recall that the token sent by the SEM back to the user is a pair (R, S_{sem}), where $R = R_1 + R_2 = r_1P + r_2P$ and $S_{sem} = r_2P_{pub} + H_1(M,R)D_{ID}^{sem}$ are elements in G_1, respectively. We note that they are all random elements in G_1 since r_1 and r_2 are random numbers in $\mathbb{Z}_q^*$. In fact, the attacker can obtain such a pair for any message of its choice. We claim that this information is of no use to the attacker since they are all only random elements in G_1.

In the following, we will show that the proposed scheme is *unforgeable*. Note that our mediated signature can be viewed as a $(2, 2)$ threshold signature. Using the methodology indicated by R.Gennaro *et al.* in [13], we give a security notion of a mediated signature scheme as follows:

A mediated signature scheme is unforgeable if the underlying signature scheme is unforgeable and the mediated signature scheme is simulatable.

Theorem 3.1 has shown that the underlying signature scheme is *unforgeable*. In the following, we only need to prove that the proposed mediated signature scheme has the property of *simulatability*.

The adversary $\mathcal{A}$ first chooses an ID as a *target* ID. To prove the unforgeability of our scheme, we give a strong assumption that $\mathcal{A}$ has the private share D_{ID}^{user} corresponding to ID, that is, $\mathcal{A}$ has corrupted the user whose identity is ID. Its goal is to forge a signature on some message under ID without the help of the SEM.

Let `MeSign` denote the mediated signature generation protocol. The view of an adversary $\mathcal{A}$ consists of the system parameters, a message M, the system public key P_{pub}, the target ID, the private key D_{ID}^{user} of the user and the signature $\sigma = (R, S)$ of M under ID. Let $\mathtt{VIEW}_{\mathcal{A}}(\mathtt{MeSign}(D_{ID}^{use}, P_{pub}, M, ID), \sigma)$ denote all the information that $\mathcal{A}$ is able to get. To prove that the proposed scheme is simulatable, we should construct a simulator `SIM` to simulate `MeSign`. `SIM`'s inputs are the system parameters, a message M, the system public key P_{pub}, the target ID, the private share D_{ID}^{user} and the signature $\sigma = (R, S)$ of M under ID. `SIM` picks a random number $\bar{r} \in \mathbb{Z}_q^*$, computes $\bar{S}_{user} = \bar{r}P_{pub} + H_1(M,R)D_{ID}^{user}$ and $\bar{S}_{sem} = S - \bar{S}_{user}$. The SEM's partial signature on M under ID is then $(R, \bar{S}_{sem})$. Let $\mathtt{SIM}(D_{ID}^{user}, P_{pub}, ID, M, \sigma)$ denote all the information produced by the simulator. The following Lemma shows that `SIM` can simulate `MeSign`.

Lemma 4.1. $\mathtt{SIM}(D_{ID}^{user}$, P_{pub}, ID, M, $\sigma)$ *is computationally indistinguishable from* $\mathtt{VIEW}_{\mathcal{A}}(\mathtt{MeSign}(D_{ID}^{use}$, P_{pub}, M, $ID)$, $\sigma)$.

Proof. On the one hand, the partial signatures given by the user and the SEM are (R, S_{user}) and (R, S_{sem}), respectively, where $R = R_1 + R_2 = r_1P + r_2P$, $S_{user} = r_1P_{pub} + H_1(M,R)D_{ID}^{user}$ and $S_{sem} = r_2P_{pub} + H_1(M,R)D_{ID}^{sem}$, r_1 and r_2 are random numbers in $\mathbb{Z}_q^*$; On the other hand, the partial signatures in `SIM` are $(R, \bar{S}_{user})$ and $(R, \bar{S}_{sem})$, respectively, where $\bar{S}_{sem} = \bar{r}P_{pub} + H_1(M,R)D_{ID}^{user}$ and $\bar{S}_{sem} = S - \bar{S}_{user}$, $\bar{r}$ is also a random number in $\mathbb{Z}_q^*$. Note that r_1, r_2 and $\bar{r}$ have the same distribution since they are all random numbers in $\mathbb{Z}_q^*$. Therefore, S_{sem}, S_{user}, $\bar{S}_{sem}$ and $\bar{S}_{user}$ are all random elements thus have the same distribution in G_1. □

Theorem 4.1. *The proposed mediated signature scheme is unforgeable in the random oracle with the assumption that G_1 is a GDH group.*

Proof. It can be easily derived from Theorem 3.1 and Lemma 4.1. □

5 Conclusions

We proposed an ID-based mediated signature scheme, which provides an efficient method for immediate revocation of a user's identity. To obtain such a scheme, we first propose an ID-based signature scheme. Our schemes are based on the bilinear pairing. Just like other pairing based cryptosystems, our schemes are simple and efficient.

Acknowledgements

The authors would like to thank the support of the *National Grand Fundamental Research 973 Program of*

China under Grant No.G1999035803, the *National High-Tech Research and Development Plan of China* under Grant No.2002AA143021 and the *National Natural Science Foundation of China* under Grant No.60373104.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Crypto'84*, LNCS 196, pp.47-53, Springer-Verlag, 1984.

[2] D. Boneh, X. Ding, G. Tsudik, and C. Wong, "A method for fast revocation of public key certificates and security capabilities," in *Proceedings of the 10th USENIX Security Symposium*, Washington D. C., pp. 297-308, 2001.

[3] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," in *Advances in Crypto'01*, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[4] B. Libert and J.Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in *22nd Symposium on Principles of Distributed Computing (PODC 2003)*, ACM Press, pp.163-171, 2003.

[5] J. Baek and Y. Zheng, "Identity-based threshold decryption," in *Advances in PKC 2004*, LNCS 2947, pp.248-261, Springer-Verlag, 2004.

[6] C. Cha and H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *Advances in PKC 2003*, LNCS 2139, pp.18-30, Springer-Verlag, 2003.

[7] K. Paterson, "ID-based signatures from pairings on elliptic curves," *Electronics Letters*, vol. 38, no. 18, pp. 1025-1026, 2002.

[8] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proceedings of Select Areas in Cryptography, SAC 2002*, LNCS 2595, pp.310-324, Springer-Verlag, 2003.

[9] X. Yi, "An identity-based signature scheme from the Weil pairing," *IEEE Communications Letters*, vol. 7, no. 2, pp. 76-78, 2003.

[10] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil-pairing," in *Advances in Asiacrypt'01*, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

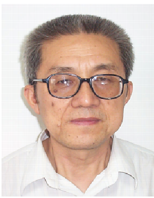
[11] X. Cheng, J. Liu, and X. Wang, "Identity-based aggregate and verifiably encrypted signatures from bilinear pairing," in *Proceedings of ICCSA 2005*, LNCS 3483, pp.1046-1054, Springer-Verlag, 2005.

[12] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp.361-396, 2000.

[13] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust threshold DDS signatures," in *Advances in Eurocrypt'96*, LNCS 1070, pp. 354-371, Springer-Verlag, 1996.

Xiangguo Cheng received his B.S. degree in Mathematics Science from Jilin University in 1992 and his M.S. degree in Applied Mathematics Science from Tongji University in 1998. He is currently a doctoral candidate under the instruction of Prof. Xinmei Wang at the State Key Laboratory of Integrated Services Network of Xidian University, P.R.China. His research interests are in the areas of information theory, Cryptography, and public key cryptosystems.

Lifeng Guo received her B.S. degree in Department of Mathematics from Yanbei Normal University, Shanxi, P.R. China in 2000 and M.S. degree in Department of Mathematics in 2003 from Shanxi University, Shanxi, P.R. China. She is currently pursuing her PhD degree in Institute of Systems Science, Academy of Mathematics and System Sciences, Chinese Academy of Sciences, Beijing, P.R. China. Her current research interests include applied cryptography and computer security.



Xinmei Wang received his B.S. degree in Communication Engineering from Xidian University in 1960. Since then he has been at Xidian University, where he is a professor of the State Key Laboratory of Integrated Services Network in Xidian University, supervisor of Ph.D. His main research interests are in information theory, error-correcting codes, digital communication and cryptography. He is the fellow of CIE and CIC and a member of IEEE Information Theory Society.