Signature-Masked Authentication Using the Bilinear Pairings

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{zhfg, kkj}@icu.ac.kr

Abstract. Many cryptographic schemes based on the bilinear pairings, namely the Weil pairing and the Tate pairing, were proposed recently. In this paper, we show that from these pairing-based cryptographic primitives, signature-masked authentication schemes can be developed. In such a scheme, a legitimate user obtains a signature from a Certificate Authority, and in order to get services from a service provider, he convinces the service provider that he has the signature without transmitting the original signature to the provider. Then no adversary (including the provider), who eavesdrops over the channel between the user and the service provider, can deduce the signature from what he saw over the channel and impersonate the legitimate user to get service from the provider.

Key words Bilinear pairing, Gap Diffie-Hellman problem, Digital signature, Authentication.

1 Introduction

The MOV reduction [9] and FR reduction [6] reduce the discrete logarithm problem on some elliptic curve to the discrete logarithm problem on a small extension of the field on which the curve is defined. Both of the reductions use a bilinear pairing, namely the Weil pairing and the Tate pairing. The Weil pairing was used in the MOV reduction and the Tate pairing in the FR reduction. Recently, the bilinear pairings were found to have others applications in cryptography. Many cryptographic schemes based on the bilinear pairings were proposed, including an identity based encryption scheme [2], a short signature schem [3], identity based authenticate key agreement protocol [11, 16], self-blindable credential certificates [14], and several identity-based signature schemes [4, 8, 10, 13, 15].

In many cryptographic applications, when a user obtains a signature from a CA (Certificate Authority) and in order to get some services from a service provider, he shall convince the service provider that he has the signature without transmitting the original signature to the provider. That is to say, the signature of CA will not be sent to the service provider directly by the user, while the

service provider can be convinced that the user really knows the signature. The reasons come from the fact that the signature maybe be intercepted by an attacker or the service provider colludes some unauthorized users to frame some authorized users. This type of authentication is called signature-masked authentication, and it is widely used many systems, such as the identity authentication between Digital Set-Top-Box (DSTB) and smart card in secure Digital Video Broadcasting (DVB) service system. The previous scheme uses RSA signature and Guillou-Quisquater [7] identification scheme. In this paper, under the assumption that CA uses the pairing-based short signature scheme suggested by Boneh *et al.* [3], we propose a basic signature-masked authentication scheme using the bilinear pairings. From the point of computational cost, we propose more effective signature-masked authentication scheme.

The organization of this paper is as follows: In Section 2 we introduce some basic concepts and facts on bilinear pairing. After describing Boneh *et al.*'s pairing-based short signature scheme and identity-based encryptosystems in Section 3, we propose a basic signature-masked authentication scheme using the bilinear pairing in Section 4. In Section 5, we propose an improved signature-masked authentication scheme. We compare our two schemes with prior scheme in computation overhead, the length of key size, communication overhead, *etc.*, and conclude at the final section.

2 Basic Concepts on Bilinear Pairings

Let G be a cyclic additive group generated by P, whose order is a prime q, and V be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problems (DLP) in both G and V are hard. Let $e : G \times G \to V$ be a pairing which satisfies the following conditions:

1. Bilinear: $e(P_1+P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1+Q_2) = e(P, Q_1)e(P, Q_2)$, or $e(aP, bQ) = e(P, Q)^{ab}$;
2. Non-degenerate: There exists $P \in G$ and $Q \in G$ such that $e(P, Q) \neq 1$;
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G$.

We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps.

Suppose that G is an additive group. Now we describe four mathematical problems.

- **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.
- **Decision Diffie-Hellman Problem (DDHP):** For $a, b, c \in Z_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \bmod q$.
- **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in Z_q^*$, given P, aP, bP, compute abP.
- **Gap Diffie-Hellman Problem (GDHP):** A class of problems where DDHP is easy while CDHP is hard.

We assume through this paper that CDHP and DLP are intractable, which means there is no polynomial time algorithm to solve CDHP or DLP with non-negligible probability. When the DDHP is easy but the CDHP is hard on the group G, we call G a *Gap Diffie-Hellman* (*GDH*) *group*. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear parings can be derived from the Weil or Tate pairing $e : G \times G \to V$. Our schemes of this paper can be built on any GDH group.

In practice, G will be the point group on an elliptic curve or the Jocobian group of a hyperelliptic curve over finite field, and V will denote a subgroup of the multiplicative group of a finite field.

3 Cryptographic Primitives

3.1 Pairing-Based Short Signature Scheme

Assuming that CA uses Boneh *et al.*'s pairing-based short signature scheme [3]. Now we are ready to introduce the signature scheme which is based on the bilinear pairings.

Key generation:
Secret key: a random number s chosen from Z_q^*, we note: $s \in_R Z_q^*$;
Public key: $(G, V, q, P, P_{pub}, H_1)$, here $P_{pub} = sP$, $H_1 : \{0,1\}^* \to G$.
Signing:
A message $M \in \{0,1\}^*$, $P_M = H_1(M) \in G$, $S_M = sP_M = (\sigma, \mu)$.
The signature of M is σ.
Verification:

1. Given the public key: $(G, V, q, P, P_{pub}, H_1)$, a message M, and a signature σ, find $S = (\sigma, \mu') \in G$ from σ. If there is no such a point, reject the signature.
2. Compute $u \leftarrow e(P, S)$ and $v \leftarrow e(P_{pub}, H_1(M))$.
3. If either $u = v$ or $u^{-1} = v$, accept the signature, otherwise reject.

This scheme is proven to be secure against existential forgery on adaptive chosen-message attacks under the standard assumption in [3].

3.2 ID-Based Encryption Scheme

This scheme due to Boneh and Franklin [2]. Let P be a generator of G. Remember that G is a group of prime order q and the bilinear pairing is given by $e : G \times G \to V$. Define two cryptographic hash functions $H : \{0,1\}^* \to Z_q$, and $H_1 : \{0,1\}^* \to G$.

- **Setup:** KGC chooses a random number $s \in Z_q^*$ and set $P_{pub} = sP$. The center publishes the system parameters $params = \{G, V, q, P, P_{pub}, H, H_1\}$, and keep s as the **master-key**, which is only known by itself.

- **Private key extraction:** A user submits his identity information ID to KGC. KGC computes the user's public key as $Q_{ID} = H_1(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his private key.
- **Encryption:** Let m denote the message to be encrypted. Compute $U = rP$ where r is a random element of Z_q. Then compute $V = m \oplus H(e(rQ_{ID}, P_{pub}))$. Out the ciphertext (U, V).
- **Decryption:** Compute $V \oplus H(e(S_{ID}, U)) = m$.

4 A Basic Signature-Masked Authentication Scheme

We consider the following situation: a user with identity ID wants to receive some services from a *Service Provider*. There is also a *Trusted Third Party*, say TTP, who issues credential certificates to the qualified users (in this sense, we can also call TTP as CA). Only after the service provider is convinced that a user possesses the corresponding credentials issued by TTP, the user can appreciate its services. Such a system is called a *credential system*. The basic requirement for a credential system is *non-transferability*. The system should prevent several users from sharing one credential certificate. A more complicated credential system also requires anonymity and unlinkablility (hence called a credential pseudonymous system, see [5] [14] for more details). Here we will talk about how to implement a basic credential system with the known identity-based cryptosystems.

The TTP or CA sets up the system parameters for Boneh *et al.*'s pairing-based short signature scheme [3] and ID-based public key infrastructure from the bilinear pairing [2, 4, 8, 15]. The whole system still works on a GDH group G.

When a user applies for a credential (*e.g.*, a driving license) or wants to get some services from a service provider, he has to firstly prove to the service provider that he is qualified (*e.g.*, he has passed the driving examination.) or he has a credential certificate. Then the service provider provides the service to the user. It works as follows. First the user sends his identity information ID to TTP. The identity information includes the user's identity number, and may also contain some extra attributes like the expiration date of the service that he is applying for. After TTP gets ID, TTP signs the message ID with his master key s using the signature scheme described in Section 3.1, *i.e.*, $Q_{ID} = H_1(ID)$, $S_{ID} = s \cdot Q_{ID}$. It feeds the corresponding signature S_{ID} of ID back to the user or store it into user's tamper-resistant device. Then (ID, S_{ID}) is the credential certificate.

To ensure the non-transferability, we assume that a tamper-resistant device is available to all users. With this device, the sensitive information S_{ID} can only be used, but not retrieved. Then the user cannot share the credential with other users. On the other hand, the user has to prove the service provider that he owns the credential. But he won't show the credential to the service provider for two reasons: the first reason is that the channel between the user and the provider is not safe. Anyone who eavesdrops over the channel will see the message exchanged

over the channel. The second reason is that he does not trust the provider, who probably sells the user's credential to other parties. The transaction between the user and the provider can be carried as follows:

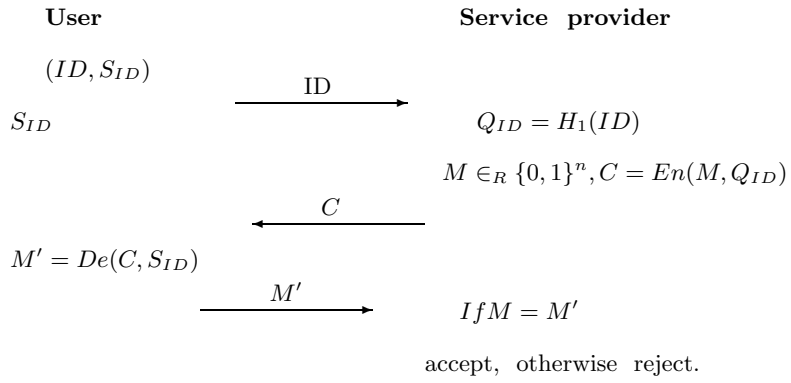

Fig. 1. Proof of possessing the Smart card to the service provider

- The user sends his ID to the provider.
- Using ID as the user's public key, the provider randomly chooses a message M, encrypts it with ID, and gets the ciphertext C. Here $En()$ is the encrypt process of identity-based encryption scheme described in Section 3.2. The provider sends C as a challenge to the user.
- From the credential, the user obtains his private key S_{ID}, which is a element of G. He decrypts C with his private key S_{ID} and recovers a message M'. The message M' is sent by the user as the response to the challenge C.
- The provider checks if $M = M'$. Only when $M = M'$, the service provider is convinced that the user has the proper credential and provides services to him.

The above credential system is based on the signature scheme and identity-based encryption scheme. The linkage between two schemes is that the signing process in the signature scheme can be regarded as the extract process in the encryption scheme. A simple analysis to the above scheme is as follows:

Security:

- The signature scheme is provably secure against existential forgery on adaptive chosen-message attacks under the standard assumptions, so is the process of issuing credentials from TTP.
- During the user's proof of possessing the proper credential to the service provider, the identity-based encryption scheme is used, which is secure against chosen-ciphertext attack under the random oracle model. That means that no polynomially bounded adversary can respond to the service provider's challenge C with correct answer M with non-negligible

probability, even if he can query the oracle some ciphertext $C_1, C_2, \ldots$ and get the corresponding plaintext $M_1, M_2, \ldots$. Recall that the successful probability of the adversary is related to the length of M. This also implies an adversary, who eavesdrops over the channel and sees the communications between the user and the service provider, can't impersonate the user to receive services from the provider.

Communication overhead:

- In the **issuing** process, the communication between the user and the TTP is the identity information ID, which depends on the context of the applications, and the corresponding credential information S_{ID}, which is an element of G.
- During the **proof** process, the communication between the user and the service provider includes the identity information ID, a challenge C consisting of a point over G and $2n$ bits, and a response M' of n bits.

In fact, if TTP signs the message ID with his master key s using the BLS signature scheme, then any ID-based signature scheme [10] [4] [8] can construct a signature-masked authentication scheme. In all those scheme, the user must compute the pairing. We note that the computation of the pairing is the most time-consuming. Although there has been many papers discussing the complexity of pairings and how to speed up the pairing computation [1], the computation of the pairing is more time-consuming. The above analysis of the proof in Fig.1 shows that the user has a heavy burden of computing, which implies the impracticality of the above credential system in the case that the device on behalf of the user has limited memory and computing power(for example, smart card). In the next section, we will proposed an improved signature-masked authentication scheme which the user need not to compute the pairing.

5 An Improved Signature-Masked Authentication Scheme

TTP issuies the signature to the user and stores it in the user's smart card.

Below we present a new scheme to deal with the case of unequal computing power between the user and the service provider, as shown in Fig.2. We denote the user by his smart card.

The verification of the service provider is justified by the following equation

$$\begin{aligned} & e(C, P) \\ &= e(H(A)S_{ID} + a^2R, P) \\ &= e(H(A)S_{ID}, P)e(aR, aP) \\ &= e(H(A)Q_{ID}, sP)e(aP, aP)^r \\ &= e(Q_{ID}, P_{pub})^{H(A)}e(A, A)^r \end{aligned}$$

Security:

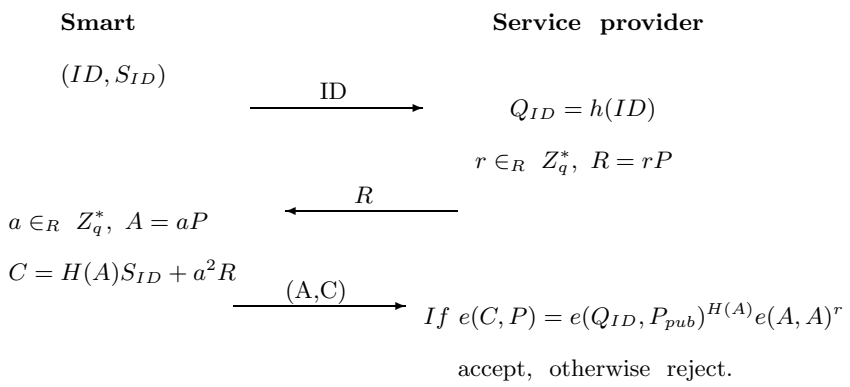

Fig. 2. Proof of possessing the Smart card to the service provider

- Suppose that an adversary is able to give a correct response (A', C') with respect to the provider's challenge R', where $A' = a'P$ (he knows the value of a') and $C' = H(A')S_{ID} + a'^2R'$. Then he knows the user's secret information by $S_{ID} = (C' - a'^2R')H(A)^{-1}$. The point is that given the information (A, C) that he sees from the channel, he cannot get S_{ID} unless he can guess a form $A = aP$, which is the hard discrete logarithm problem or he can obtain a^2R from A and R, this is CDHP.
- The service provider can't know S_{ID}. The provider given the challenge R and received the response (A, C). Since a was randomly chosen by smart card, the provider does not know a and a^2R, so he can not know S_{ID}. If the provider wants to find out the S_{ID} using $e(S_{ID}, H(A)P) = e(A, A)^r e(-C, P)$, then he must can solve CDHP: given aP, bP, let $v = e(aP, bP)$, solve X from $v = e(X, P)$, but we assume that CDHP is intractable.

Communication overhead:

- The communication between smart card and service provider includes the ID information, the challenge R, and the response (A, C). Recall that R, A and C are elements of the group G.

6 Comparision

The existing Scheme of signature-masked authentication is Guillou- Quisquater authentication scheme (GQ scheme). This scheme applies protocols of zero-knowledge proof based on RSA signature, and it was used at the authentication between the smart card and the DSTB such as EP-DVB (European Project for digital video broadcasting). About GQ scheme, the reader can refer to [7] for details.

We denote Scheme I our basic scheme and Scheme II the improved scheme. Assuming that Boneh *et al.*'s short signature scheme in our schemes using the GDH group derived from the curve $E/F_{3^{97}}$ defined by $y^2 = x^3 - x + 1$, which has 923-bit discrete-log security and the modulus n for GQ scheme is 1024-bit. We

limit the message space is $\{0,1\}^{160}$ in our schemes and the size of ID is 30-bit in all schemes.

We compare our signature-masked authentication schemes with GQ scheme in computation overhead, the length of key size and communication overhead, etc., the result are listed at Table 1 (we ignore the operation of hash in all schemes). We denote **Pa** the pairing operation, **Sm** the scalar multiplication on $E/\ F_{p^l}$, **Ex** the exponentiation over $F_{p^{l\alpha}}$ and **M** the modular exponentiation of RSA.

	Scheme I	*Scheme II*	*GQ*
Underlying problem	*GDHP*	*GDHP*	*RSA*
Public key size(bits)	625	625	2048
Private key size(bits)	151	151	1024
Signature size(bits)	154	154	1024
Communication overhead(bits)	658	954	3102
Used EC point compress	505	495	
Computation overhead(User)	$1Pa$	$3Sm$	$2M$
Computation overhead(Provider)	$1Sm + 1Pa + 1Ex$	$1Sm + 3Pa + 2Ex$	$2M$

Table 1. Comparison of our schemes and GQ scheme

From Table 1, it is easy to see that our improved scheme is very effective for user (smart card).

7 Conclusion

In this paper, we proposed two signature-masked authentication schemes based on known pairing cryptosystems. These schemes can be used in a simple credential system, where a user proves to a service provider that he has the corresponding credential certificate to get services. Based on the signature scheme from the Weil pairing and the identity-based encryption scheme, we proposed a basic signature-masked authentication scheme which applies to the case that both the user and the service provider have good computation resources. The other improved signature-masked authentication scheme was presented for the case that the user has limited computational power.

References

1. P.S.L.M. Barreto, H.Y. Kim, B.Lynn, and M.Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
2. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto'2001, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
3. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology-Asciacrypt'2001, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

4. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Cryptology ePrint Archive, Report 2002/018, available at http://eprint.iacr.org/2002/018/.
5. J. Camenisch and A. Lysyanskaya, *An efficient system for non-transferable anonymous credentials with optional anonymity revocation*, Advances in Cryptology-Eurocrypt'2001, LNCS 2045, pp. 93-118, Springer-Verlag, 2001.
6. G. Frey and H.Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation, 62, pp.865-874, 1994.
7. L.Guillou and J.Quisquater, *A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory*, Advances in Cryptology-Eurocrypt'1988, LNCS 330, pp. 123-128, Springer-Verlag, 1989.
8. F. Hess, *Exponent group signature schemes and efficient identity based signatureschemes based on pairings*, Cryptology ePrint Archive, Report 2002/012, available at http://eprint.iacr.org/2002/012/.
9. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transaction on Information Theory, 39: 1639-1646, 1993.
10. K.G. Paterson, *ID-based signatures from pairings on elliptic curves*, Cryptology ePrint Archive, Report 2002/004, available at http://eprint.iacr.org/2002/004/.
11. N.P. Smart, *An identity based authenticated key agreement protocol based on the Weil pairing*,Electron. Lett., 38, (13), pp. 630-632, 2002.
12. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, In W. Bosma, editor, ANTS IV, LNCS 1838, pp385-394,Springer-Verlag, 2000.
13. R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystems based on pairing*, SCIC 2000-C20, Jan. 2000. Okinawa, Japan.
14. E. R. Verheul, *Self-blindable credential certificates from the Weil pairing*, Advances in Cryptology-Asciacrypt'2001, LNCS 2248, pp. 533-551, Springer-Verlag, 2001.
15. F. Zhang and K. Kim, *ID-Based Blind Signature and Ring Signature from Pairings*, To appear in Cryptology-Asciacrypt'2002.
16. F. Zhang, S. Liu and K. Kim, *ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings*, Cryptology ePrint Archive, Report 2002/122, available at http://eprint.iacr.org/2002/122/.