SCIS 2003 The 2003 Symposium on Cryptography and Information Security
Hamamatsu,Japan, Jan.26-29,2003
The Institute of Electronics,
Information and Communication Engineers

Exploring Signature Schemes with Subliminal Channel

Fangguo Zhang * zhfg@icu.ac.kr
Byoungcheon Lee † sultan@joongbu.ac.kr
Kwangjo Kim * kkj@icu.ac.kr

Abstract— The subliminal channel in a cryptographic protocol such as an authentication system or a signature scheme provides an additional channel from the sender to an authorized receiver and can't be read by any unauthorized receiver. In this paper, we firstly show that Hess's ID-Based signature scheme in SAC'02 can provide digital signature with the broadband and narrowband subliminal channels. Secondly, we evaluate Jan-Tseng signature schemes with subliminal channel in ICPP'99 and show that any user can change the signature, such that the subliminal message receiver cannot get the subliminal message correctly, but the verification of signature is still right.

Keywords: ID-based signature, Subliminal channel, Bilinear pairings, Cryptanalysis.

1 Introduction

A subliminal channel is a covert communication channel to send a message to an authorized receiver. This message cannot be discovered by any unauthorized receiver. In [13], Simmons invented the concept of subliminal channel in conventional digital signature schemes. The subliminal message is hidden in what looks like a normal digital signature and only authorized receiver can read it. The subliminal channel in a digital signature has several applications [17]. For example, a credit card provider can hide the card holder's credit history and credit limit in a digital signature for an issued credit card.

In 1985, Simmons [14] showed that in any digital signature scheme in which α bits are used to communicate a signature that provides β bits of security against forgery, where $\alpha > \beta$, the remaining $\alpha - \beta$ bits are potentially available for subliminal communication. In [15], Simmons defined that if the subliminal channel uses all, or nearly all, of the $\alpha - \beta$ bits, it is said to be broadband, while if it uses only a fraction of the $\alpha - \beta$ bits, it is said to be narrowband.

Beside Simmons's work, in 1997, Harn and Gong proposed two schemes that provide a digital signature with a broadband subliminal channel that does not require the subliminal receiver to share the signer's secret key. However, the length of the digital signature generated in their proposed schemes is too long, while the size of the secret keys kept by the signer and the subliminal receiver are also large. Jan and Tseng proposed two new signature schemes with subliminal channels in [6].

Recently, the bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, have been found various applications in cryptography [1, 2, 7, 12]. More precisely, they are important tools for construction of ID-based cryptographic schemes. The ID-based public key setting can be an alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. Many ID-based signature schemes have been proposed using the bilinear pairings [3, 5, 11, 12]. In these ID-based signature schemes using the bilinear pairings, Hess's scheme is not only efficient but has a security proof relative to the computational Diffie-Hellman problem. In this paper, we discuss the subliminal channel in this ID-based signature scheme. We show that Hess's ID-based signature scheme can provide a broadband subliminal channel and a narrowband subliminal channel.

In ICPP'99, Jan and Tseng proposed two new signature schemes with subliminal channels in [6]. Here we analysis Jan *et al.*'s signature schemes with subliminal channel, and we show that any user can change the signature in their signature schemes, such that the subliminal message receiver cannot get the subliminal message correctly, but the verification of signature is still right.

The rest of the paper is organized as follows: The next section explains briefly Hess's ID-based Signature Scheme from the bilinear pairings. Section 3 gives a detailed description of a broadband subliminal channel and a narrowband subliminal channel in Hess's ID-based signature scheme. In Section 4, we give a cryptanalysis of Jan *et al.*'s signature schemes with subliminal channel. Section 5 concludes this paper.

2 Hess's ID-Based Signature Scheme

In this section, we introduce Hess's ID-based signature scheme from the bilinear pairings. First of all, we give the basic concept and some properties of the bilinear pairings.

* International Research center for Information Security (IRIS), Information and Communications Univ. (ICU), 58-4 Hwaam-dong, Yusong-gu, Taejon, 305-732, Korea
† Joongbu University, San 2-25, Majon-Ri, Chuboo-Meon, Kumsan-Gun, Chungnam, 312-702, Korea

2.1 Basic Concepts on Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problems in both G_1 and G_2 are hard. Let $e : G_1 \times G_1 \to G_2$ 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 $e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$;
2. Non-degenerate: There exists $P \in G_1$ and $Q \in G_1$ such that $e(P, Q) \neq 1$;
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Suppose that G_1 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. Refer to [1, 3, 5, 18] for more details.

2.2 Hess's ID-based Signature Scheme from Pairing

Hess's ID-based signature scheme consists of following algorithms, **Setup**, **Extract**, **Signing** and **Verification**.

Let G_1 be a GDH group of prime order q. The bilinear pairing is given as $e : G_1 \times G_1 \to G_2$.

Setup: Let P be a generator of G_1. Choose a random number $s \in Z_q^*$ and set $P_{pub} = sP$. Define two cryptographic hash functions $H : \{0,1\}^* \to Z_q$ and $H_1 : \{0,1\}^* \to G_1$. The system parameters are PARAMS $= \{G_1, G_2, q, P, P_{pub}, H, H_1\}$, and s be the MASTER-KEY of TA (Trust Authority).

Extract: Given an identity ID, which implies the public key $Q_{ID} = H_1(ID)$, the algorithm returns the private key $S_{ID} = sQ_{ID}$.

The above two operations, **Setup** and **Extract** are carried out by TA. Note that TA can access to the sensitive private key S_{ID}. To avoid power abuse by TA, n trust authorities with (n, n)-threshold secret sharing scheme can be used to escrow the MASTER-KEY, as suggested in [5].

Signing: Suppose that m is the message to be signed. Let $a \in_R$ denote the uniform random selection.

- Compute $r = e(P, P)^k$, where $k \in_R Z_q^*$.
- Compute $v = H(m||r)$.
- Compute $U = vS_{ID} + kP$.

Then (U, v) is the signature of the message m.

Verification: Compute

$$r = e(U, P)e(Q_{ID}, P_{pub})^{-v}.$$

Accept the signature if and only if

$$v = H(m||r).$$

The signature consists of an element in G_1 and an element in Z_q. In practice, G_1 will be the group of points on an elliptic curve. So the size of the element in G_1 (elliptic curve group) can be reduced by a factor of 2 with compression techniques in [10].

3 Subliminal Channel in Hess's ID-based Signature Scheme

3.1 The Broadband Subliminal Channel

Before the signer sends subliminal message, he must be encoded to make mathematical sense. In this case, the signer must imbed the subliminal message, m_{sub}, as an element R_{sub} of G_1 (In practice, G_1 will be the group of points on an elliptic curve over the finite field F_p). For the imbedding message on an elliptic curve over the finite field F_p, there is no known deterministic polynomial algorithm, however there are probabilistic algorithms which have very small failure probability. About the method of imbedding, we refer to Chapt 6 of [9] and [8].

Assuming that the signer wants to sign m, the subliminal message is m_{sub}. The signer gives the secret key S_{ID} to the subliminal receiver in a confidential way.

Signing: Imbed subliminal message m_{sub} as an element R_{sub} of G_1.

- Compute $r = e(R_{sub}, P)$.
- Compute $v = H(m||r)$.
- Compute $U = vS_{ID} + R_{sub}$.

Then (U, v) is the signature of the message m.

Verification: Same as Hess's ID-based signature scheme.

Message recovery in subliminal channel: The subliminal receiver verifies the signature to make sure that the message is authentic. He then uses the secret key S_{ID} to compute $R_{sub} = U - vS_{ID}$, and decodes R_{sub}, and recovers the subliminal message m_{sub}.

Assume that the the subliminal message m_{sub} is random, after encoding, we can regard R_{sub} as a random element of G_1. So R_{sub} plays the role of kP in Hess's ID-based signature scheme. We know that Hess's ID-based signature scheme is proven to be secure against existential forgery on adaptive chosen-message attacks under the random oracle model assumption, so above ID-based signature scheme with broadband subliminal channel is secure. Obviously, the same subliminal message can't be sent twice using different signatures. If the subliminal message m_{sub} is doubly sent by two signatures (m_1, U_1, v_1) and (m_2, U_2, v_2), then $U_1 - v_1 S_{ID} = U_2 - v_2 S_{ID}$, so we have $S_{ID} = (v_1 - v_2)^{-1}(U_1 - U_2)$, *i.e.*, we can recover the secret signing key of the signer.

This channel has an obvious shortcoming. In order for the subliminal receiver to be capable of recovering the subliminal message, it is necessary for him to know the signer's secret key. This means that the subliminal receiver can forge the signer's signature. If the signer wants to use this broadband subliminal channel, he must unconditionally trust the subliminal receiver. To avoid this shortcoming, we give another subliminal channel: the narrowband subliminal channel.

3.2 The Narrowband Subliminal Channel

Simmons suggested a narrowband subliminal channel for l bits subliminal message in DSA (Digital Signature Algorithm) [16]. Like [16], we can give a narrowband subliminal channel for l bits in Hess's ID-based signature scheme. We describe it in detail as follows:

The signer chooses additionally a random number $k' \in_R Z_q^*$, computes $r' = e(P,P)^{k'}$ and sends r' to the subliminal receiver in a confidential way. We assume that the signer wants to sign m, and let m_{sub} be l bit subliminal message.

Signing:

- Compute $r = e(P,P)^{k'+m_{sub}}$.
- Compute $v = H(m||r)$.
- Compute $U = vS_{ID} + (k' + m_{sub})P$.

Then (U, v) is the signature of the message m.

Verification: Same as Hess's ID-based signature scheme.

Message recovery in subliminal channel: The subliminal receiver verifies the signature to make sure the message is authentic. He then uses his secret key r' to compute $r/r' = e(P,P)^{m_{sub}}$. Because l is bounded, the subliminal receiver can get the subliminal message m_{sub} by total search.

The size of l depends on the computational power of the subliminal receiver. Like above broadband subliminal channel, the same subliminal message can't be sent twice using different signatures too. Next, we will show that the subliminal receiver and any adversary can't forge the signature of the signer. The subliminal receiver know $r' = e(P,P)^{k'}$. He can get m_{sub}, but doesn't know k', since he must solve the discrete logarithm problem in G_2 if he wants to get k' from r'. We assume that the subliminal message is random, so $k = k' + m_{sub}$ is a random element of Z_q, the security of above signature scheme with narrowband subliminal channel is same as the original ID-based signature scheme.

4 Cryptanalysis of Jan *et al.*'s Signature Schemes with Subliminal Channel

4.1 Jan *et al.*'s Signature Schemes with Subliminal Channel

First of all we review Jan *et al.*'s Signature Schemes in brief using the same notation as [6].

Jan *et al.*'s Signature Schemes with a Broadband Subliminal Channel:

The parameters are summarized as follows:

- Public values of the signer: $(p, q, g, y, h())$, here p is a large prime number, q is a prime divisor of $p-1$ and g is a generator with the order q in $GF(p)$, $y = g^{-x_1-x_2}$, $h()$ is a one-way hash function.
- Secret keys of the signer: (x_1, x_2).
- Secret key of first-channel receiver: x_1.
- Secret key of second-channel receiver: x_2.

The signer signs the message m with two subliminal messages $m_1 \in Z_q^*$ and $m_2 \in Z_q^*$, where m_1 and m_2 are the messages hidden in the first-channel and second- channel. Then, the signer computes the signature (e, s_1, s_2) for m as follows:

$$e = h(g^{m_1} \cdot g^{m_2} \bmod p \| m),$$

$$s_1 = m_1 + e \cdot x_1 \bmod q,$$

$$s_2 = m_2 + e \cdot x_2 \bmod q.$$

Afterwards, the signer sends (e, s_1, s_2) to verifiers. Any receiver can verify the signature by checking if the following equation is equal or not.

$$e = h(g^{s_1} \cdot g^{s_2} \cdot y^e \bmod p \| m).$$

The first-channel receiver verifies the signature to make sure the message is authentic. He then uses the secret key x_1 to compute $m_1 = s_1 - e \cdot x_1 \bmod q$ and recovers the subliminal Message. Similarly, the second-channel receiver also uses the secret key x_2 to extract the subliminal message m_2.

Jan *et al.*'s Signature Schemes with a Narrowband Subliminal Channel:

The parameters are summarized as follows:

- Public values of the signer: $(p, q, g, y, h())$, here $y = g^{-x_1-x_2-x_3}$, $h()$ is a one-way hash function.
- Secret keys of the signer: (x_1, x_2, x_3).
- Secret key of first-channel receiver: x_1.

- Secret key of second-channel receiver: x_2.

The signer signs the message m with two subliminal messages $m_1 \in Z_q^*$ and $m_2 \in Z_q^*$, where m_1 and m_2 are the messages hidden in the first-channel and second- channel. Then, the signer selects a random integer $R \in Z_q^*$ computes the signature (e, s_1, s_2, s_3) for m as follows:

$$e = h(g^{m_1} \cdot g^{m_2} \cdot g^R \bmod p \| m),$$

$$s_1 = m_1 + e \cdot x_1 \bmod q,$$

$$s_2 = m_2 + e \cdot x_2 \bmod q,$$

$$s_3 = m_3 + e \cdot x_3 \bmod q.$$

Afterwards, the signer sends (e, s_1, s_2, s_3) to verifiers. Any receiver can verify the signature by checking if the following equation is equal or not.

$$e = h(g^{s_1} \cdot g^{s_2} \cdot g^{s_3} \cdot y^e \bmod p \| m).$$

The message recovery in subliminal channels is similar to the signature scheme with a broadband subliminal channel.

Jan *et al.*'s signature schemes can be implemented using the bilinear pairings, such that they can be ID-based signature. But as we will show that Jan *et al.*'s signature schemes with subliminal channel can't provide the subliminal channel correctly.

4.2 Cryptanalysis

In most applications of subliminal channel in a digital signature, the holder of message-signature pair doesn't hope that the signer can send some secret message to a special receiver through his message-signature pair. For instance, in the prisoners problem [13] or credit card application, the wardenry or the card holder doesn't hope there is some subliminal channel in their message-signature pairs. In this section, we show that in Jan *et al.*'s signature schemes with subliminal channel, any user can change the signature, such that the subliminal message receiver cannot get the subliminal message correctly and the message-signature pair still is valid.

At Jan *et al.*'s broadband scheme, a user has the signature of the signer (e, s_1, s_2) for m. If we let

$$s_1' \in_R Z_q,$$

$$s_2' = s_1 + s_2 - s_1',$$

then (e, s_1', s_2') is a valid signature for m. But from $s_i' - e \cdot x_i \bmod q$, any subliminal channel receiver cannot recover message. Similarly, at Jan *et al.*'s narrowband scheme, we let

$$s_1' \in_R Z_q, s_2' \in_R Z_q,$$

$$s_3' = s_1 + s_2 + s_3 - s_1' - s_2',$$

then (e, s_1', s_2', s_3') is a valid signature for m too, but any subliminal channel receiver cannot recover the subliminal message which they want.

At Jan *et al.*'s narrowband scheme, the user can control which receiver can recover the message correctly. For instance, the user hopes that only the first-channel receiver can recover the subliminal message correctly, then he can do as follows: for the original signature (e, s_1, s_2, s_3), let

$$s_1' = s_1, s_2' \in_R Z_q,$$

$$s_3' = s_1 + s_2 + s_3 - s_1' - s_2',$$

then (e, s_1', s_2', s_3') is a valid signature for m too, but only the first-channel receiver can recover the subliminal message correctly.

So we say that Jan *et al.*'s signature schemes with subliminal channel can't provide subliminal channel correctly.

5 Conclusion

In this paper, we studied some signature schemes with subliminal channel. We firstly show that Hess's ID-Based signature scheme can provide a broadband subliminal channel and a narrowband subliminal channel. Then we analysis Jan *et al.*'s signature schemes with subliminal channel, and we show that some dishonest users can change the signature in their signature schemes, such that the subliminal message receiver cannot get the subliminal message correctly, but the verification of signature is still right.

Recently, many ID-based signature schemes have been proposed using the bilinear pairings [3, 5, 11, 12]. But it seems that the approach used in this paper can not apply to others ID-based signature schemes using pairings. How to deal with the subliminal channel problem in others ID-based signature schemes using pairings, such as [3] and [11], is our further work.

References

[1] 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.

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing", In C. Boyd, editor, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

[3] J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, Public Key Cryptography - PKC 2003, LNCS 2139, pp.18-30, Springer-Verlag, 2003.

[4] L. Harn and G. Gong, "Digital signature with a subliminal channel", IEE Proc. Comput. Digit. Tech., Vol. 144, No. 6, pp. 387-389, 1997.

[5] F. Hess, "Efficient identity based signature schemes based on pairings", Proc. 9th Workshop on Selected Areas in Cryptography – SAC 2002, LNCS, Springer-Verlag, 2002. Available at http://www.math.tu-berlin.de/ hess/.

[6] J.K. Jan and Y.M. Tseng, "New digital signature with subliminal channels based on the discrete logarithm problem", ICPP Workshop 1999, pp.198-203.

[7] A. Joux, "A one round protocol for tripartite Diffie-Hellman", ANTS IV, LNCS 1838, pp.385-394, Springer-Verlag, 2000.

[8] N. Koblitz, "Elliptic curve cryptosystems". Mathematics of Computation, Vol. 48, No. 177, pp. 203-209, 1987.

[9] N. Koblitz, "A Course in number theory and cryptography", 2nd ed., Springer-Verlag, 1994.

[10] IEEE Std 2000-1363, "Standard specifications for public key cryptography", 2000.

[11] 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/.

[12] R. Sakai, K. Ohgishi, M. Kasahara, "Cryptosystems based on pairing", SCIS 2000-C20, Okinawa, Japan. Jan. 2000.

[13] G.J. Simmons, "The prisoner's channel and the subliminal channel", in Advances in Cryptology, Crypto' 83, pp.51-67, Plenum Press, New York and London, 1984.

[14] G.J. Simmons, "A secure subliminal channel", in Advances in Cryptology, Crypto' 85, LNCS 218, pp.33-41, Springer-Verlag, 1985.

[15] G.J. Simmons, "Subliminal communication is easy using the DSA", in Proc. EUROCYPT 93, LNCS 765, pp.218-232, Springer-Verlag, 1993.

[16] G.J.Simmons, "The subliminal channel in the U.S. Digital Signature Algorithm (DSA)", Proceedings of 3rd Symposium on State and Progress of Research in Cryptography – SPRC'93, Rome, Italy, Feb. 15–16 , pp. 35-54, 1993.

[17] G.J. Simmons, "The history of subliminal channels", IEEE Jour. on sel. Areas Comm., Vol.16, No.4, pp.452-462, 1998.

[18] 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/.