Asian Journal of Information Technology 5 (4) : 392-395, 2006


# Perfect Subliminal Channel in a Paring-Based Digital Signature

[1]Zhenyou Wang and [2]Wei Gao
[1]College of Mathematics Guangdong University of Technology,
Guangdong Guangzhou, 5 1 0 0 0 6,
[2]College of Mathematics and Econometrics, Hunan University,
Changsha, Hunan, Peoples Republic of China

**Abstract:** We show that a broad-band subliminal channel which requires the subliminal receiver hold no information about the signer's private signing key and achieves the potential bandwidth, can be easily constructed in a recently proposed paringbased signature scheme.And the existence of this subliminal channel just disproves Simmon's conjectures on the bandwidth of the subliminal channel in a digital signature. Cryptography, digital signature, subliminal channel.

**Key words:** Subliminal channel, digital signature

## INTRODUCTION

The concept of subliminal channel was invented by Simmons[1]. A subliminal channel is a covert communication channel to transmit a message which can only be recovered by the authorized receiver. The subliminal channel has many applications in real world. For example, the message in the subliminal channel embedded in the digital signature on a passport can also tell customs agents that the passport holder is known terrorist, smuggler, etc.

Simmons classified subliminal channels into two types, i.e.,a broad-band subliminal channel and a narrow-band one[1]. A broad-band subliminal channel is one such that does not depend on the amount of the computation required to embed a subliminal message. On the other hand, the narrow-band subliminal channel is one such that the bandwidth is logarithmically limited dependent on the exponential select an reject strategy. Thus, the classification is not on the bandwidth, but on the amount of the computation for embedding a subliminal message. However, the bandwidth of broad-band subliminal channels is usually several hundred bits and that of the narrowband ones is usually a few bits. In any digital signature scheme in which _ bits are used to communicate a signature that provides only _ bits of security against forgery, alteration, or transplantation of a legitimate signature from the message for which it was generated to another, where _>_, the remaining _−_ bits are potentially available for subliminal communications.

In past years, many subliminal channels in a digital signature were proposed[2-7]. Of course, the most desired subliminal channel is the broad-band (work independent) one with the bandwidth as broad as possible. On the other hand, we wish to keep the security of the signature scheme with a subliminal channel. However, it seems very difficult to achieve both broad bandwidth and the security. For example, the broad-band subliminal channel proposed in[3] has the disadvantage that the subliminal receiver shares the signing keys and so can forge the signature of any message. The broad-band subliminal channel in[5] comprising about half of the information content of the signing key and cann't resist the so-called conspiracy attack. In 1999, it was pointed out in[6] that a broad-band subliminal channel with bandwidth close to the potential one can be constructed in ESIGN without comprising the signing key, as is probably the best result on the subliminal channel.

In recent years, the so-called paring-Based cryptography has been becoming increasingly attracting[10]. And many paringbased digital signature was proposed[11-14]. However subliminal channels in such digital signatures have hardly been researched[7].

In this study, we will construct a subliminal channel with perfect properties in a recent proposed paring-Based digital signature[9]. In our scheme, the subliminal channel holds the bandwidth identical to the potential one and the key for recovering the subliminal message is independent of the signing key. So, we can claim that the proposed broad-band subliminal channel achieves the most desired property, namely the broadest bandwidth and the best security. On the other hand, we disprove Simmon's conjectures on the subliminal channel in digital signature[1] with the proposed subliminal channel as a counter example.

**Corresponding Author:** Zhenyou Wang, College of Mathematics Guangdong University of Technology, Guangdong Guangzhou, 5 1 0 0 0 6, Peoples Republic of China

The rest of the study is organized as follows: The next section presents the two conjectures of Simmons on the subliminal channel in a digital signature. Section 3 describes the sketch of the recently proposed paring-Based digital signature scheme by D. Boneh. In section 4, we give the proposed broadband subliminal channel embedded in the paring-Based digital signature and discuss its properties. The last section concludes this study.

**Simmons' conjecture:** The conjectures of Simmons[8] on the subliminal channel in a digital signature can now be stated in the following form.

**Conjecture 1:** The upper bound to the bandwidth of a broad-band (work independent) subliminal channel is just thedifference between the information content of the signers private key and the uncertainty about the signers key to a subliminal receiver.

**Conjecture 2:** The bandwidth for subliminal communications in excess of this bound is logarithmically limited, i.e. is achieved only through an exponential select and reject strategy.

The above Conjectures were disprove in[6] but it seemsthat there are too few counterexamples.

## BONEH'S PARING-BASED SIGNATURE SCHEMS

Here we present the sketch of Boneh's paring-Based signature scheme and refer the reader to[9] for more details. Let $(G_1,G_2)$ be bilinear groups where $|G_1| = |G_2| = p$ for some prime p and e: $G_1 \times G_2 \rightarrow G_T$ be the corresponding bilinear maps. As usual, $g_1$ is a generator of $G_1$ and $g_2$ a generator of $G_2$. For the moment we assume that the messages m to be signed are elements in $Z^*_P$, but the domain can be extended to all of $\{0,1\}^*$ using a collision resistant hash function H: $\{0,1\} \rightarrow Z^*_P$.

**Key generation:** Pick random $x, y \in_R Z^*_P$ and compute $u \leftarrow g_2^Y \in G_2$. The public key is $(g_1, g_2, u, v)$. The secret key is (x, y).

**Signing:** Given a secret key (x, y), $x, y \in Z^*_P$ and a message $m \in Z^*_P$, pick a random $r \in Z^*_P$ and compute $\sigma \in g_1^{1/(x+m+yr)} \in G_1$. Here $1/(x + m + yr)$ is computed modulo p. In the unlikely event that $x + m + yr = 0$ we try again with a different random r. The signature is $(\sigma, r)$.

**Verification:** Given a public key $(g_1, g_2, u, v)$, a message $m \in Z^*_P$ and a signature $(\sigma, r)$, verify that $e(\sigma, u \cdot g_2^m v_r) = e(g_1, g_2)$. If the equality holds the result is valid, otherwise, the result is invalid.

The above signature scheme is existentially unforgetable under a chosen message attack without using random oracles. The security of the scheme depends on a new complexity assumption called the Strong Diffie-Hellman assumption.

**Proposed subliminal channel:** We propose a broad-band subliminal channel such that the subliminal receiver does not know the signing key of the transmitter. The subliminal receiver and the transmitter share a semantically secure encryption scheme[16,15] with the encryption algorithm E: $Z^*_P \rightarrow Z^*_P$, the decryption algorithm D: $Z^*_P \rightarrow Z^*_P$, a key $k_{sub,d}$ for decryption and a key ksub,e for encryption. The other notations follow the above description of Boneh=s scheme. Let $m_{sub} \in Z^*_P$ denotes the subliminal message.The proposed protocol follows:

**Verification:** Given a public key $(g_1, g_2, u, v)$, a message $m \in Z^*_P$ and a signature $(\sigma, r)$, verify that $e(\sigma, u \cdot g_2^m v_r) = e(g_1, g_2)$. If the equality holds the result is valid, otherwise, the result is invalid.

The above signature scheme is existentially unforgetable under a chosen message attack without using random oracles. The security of the scheme depends on a new complexity assumption called the Strong Diffie-Hellman assumption.

**Key generation:** The transmitter picks random $x, y \in_R Z^*_P$ and compute $u \leftarrow g_2^X G_2$ and $v \leftarrow g_2^X \in G_2$. The public key is $(g_1, g_2, u, v)$. The secret key (x, y) is known is only by the transmitter.

**Encrypting the subliminal message:** The transmitter computes: $Csub = E(m_{sub}, k_{sub,e})$

**Signing:** Given a secret key (x, y), $x, y \in Z^*_P$, the transmitter generates an innocuous message $m \in Z^*_P$, sets $r = C_{sub} \in Z^*_P$ and compute $\sigma \in g_1^{1/(x+m+yr)} \in G_1$. Here $1/(x + m + yr)$ is computed modulo p. In the unlikely event that $x + m + yr = 0$ the transmitter tries again with a different random r. The innocuous message m with the signature $(\sigma, r)$ is sent out.

**Verification:** Given a public key $(g_1, g_2, u, v)$, a message $m \in Z^*_P$ and a signature $(\sigma, r)$, the ordinary receiver (the warder in the model of a subliminal model) verifies that $e(\sigma, u \cdot g_2^m \cdot v^r) = e(g_1, g_2)$. If the equality holds the result is valid, otherwise the result is invalid.

**Recovering the subliminal message:** The subliminal receiver first verifies the message as the above, then computes the subliminal message: $m_{sub} = D(r, k_{sub,d})$, here

$r = c_{sub}$. As to the above subliminal channel, we can find the following properties:

**Broad-bandness:** Since the amount of the computation for embedding the subliminal message msub does not depend on the number of bits of $m_{sub}$, this is the broad-band subliminal channel.

**Broadest bandwidth:** The signature is $(\sigma, r)$, $\sigma \in Z^*_p$ $r \in Z^*_p$ the number of the bits of the signature being $\alpha = 2\log p$, the random element being r,ó providing $\alpha$ (= log p) bits of security. So $\alpha-\beta$ (= log p) bits are potentially available for subliminal channel. And in our proposed subliminal channel, the number of the available subliminal message $m_{sub} \in Z^*_p$ is logp. So The proposed subliminal channel achieves the broadest bandwidth, namely,the entire potential bandwidth of the subliminal channel.

**Optimistic security:** The only secret information of the subliminal receiver is the key $k_{sub}$ for decrypting the encrypted subliminal message which is independent of the signing key. So if the subliminal receiver wants to forge a signature, he knows no more than the general forger commonly considered in the security model. So the digital signature with the proposed subliminal channel keeps the best security.

**Indistinguishability:** Since the encryption scheme for the subliminal message is semantically secure[15,16], it is infeasible for the outer verifier, such as the party of warder in the subliminal channel model, to decide whether the signature involves the covert message, that is, it is hard for the verifier not the subliminal receiver to distinguish the signature computed with the ordinary Boneh's scheme from that with subliminal channel.

**Efficiency:** Since the only additional work for embedding a subliminal channel, compared with the ordinary digital signature, is the procedures of encryption of decryption, as is the least necessary procedure to get the confidentiality of the subliminal message, we can say the proposed subliminal channel is most efficient.

According to the above items, it seems that the proposed subliminal channel holds many properties greatly better than the previous ones. For example, the subliminal channel in DSA[3] comprises the entire signing key. The one proposed by Harn in[5] comprises half of the signing key's information content and suffers the conspiracy attacks, the one proposed in[6] holds less efficiency and doesn't achieve the entire potential subliminal bandwidth, etc.

Additionally, we already disproves Simmon's Conjectures on the bandwidth of the subliminal channel in a digital signature. The secret signing key (x, y) is 2 log p. The only information known by the subliminal receiver is the key ksub which is independent of the secret key (x, y), so the uncertainty about the signing key to the subliminal receiver remains unchanged. So the difference mentioned in Conjecture 1 is 0 bits. However the bandwidth of the proposed broad-band subliminal channel is log p, So Conjecture 1 is disproved. And the disproving of Conjecture 2 follows obviously.

## CONCLUSION

In the recently proposed paring-Based signature scheme, we readily construct a broad-band subliminal channel which posses perfect properties: the most desired security against the forgery of all parties but the signer (requiring the subliminal receiver to share no information about the signing key), the most desired bandwidth (achieving the entire potential subliminal bandwidth), the semantical security preventing the verifier from finding whether the subliminal channel is being used, the least work for embedding a subliminal message, etc. However, it seems very difficult for a previously proposed subliminal channel in an ordinary digital signature to attain only one of the above properties, let alone all properties together. And the proposed subliminal channel can disprove Simmon's conjectures on the bandwidth of the subliminal channel in digital signature.

## REFERENCES

1. Simmons, G.J., 1984. The prisoner's problem and the subliminal channel. Advances in Cryptology-Crypto, 83: 51-67.
2. Simmons, G.J., 1984. The subliminal channel and digital signature. Advances in Cryptology-Eurocrypt 84: 364-378.
3. Simmons, G.J., 1993. Subliminal communication is easy using the DSA. Advances in Cryptology-Eurocrypt, 93: 218-232.
4. Jan, J. and Y. Tseng, 1999. New digital signature with subliminal channels based on the discrete logarithm problem. Parallel Processing, 1999. Proceedings, Intl. Workshops, pp: 198-203.
5. Harn, L. and G. Gong, 1997. Digital signature with a subliminal channel. Computers and Digital Techniques, IEE Proceedings, 144, pp: 387-389.
6. Kuwakado, H. and H. Tanaka, 1999. New subliminal channel embedded in the ESIGN. IEICE Transactions on fundamentals of electronics, Communications and Computer Sci., 82: 2167-2171.

7. Zhang, F., B. Lee and K. Kim, 2003. Exploring signature schemes with subliminal channel, SCIS, pp: 245-250.
8. Simmons, G.J., 1998. Results concerning the bandwidth of subliminal channels. J. Selected Areas in Communications, 16: 463-473.
9. Boneh, D. and X. Boyen, 2004. Short signatures without random oracles. Advances in Cryptology-Eurocrypt, pp: 56-73.
10. Dutta, R., R. Barua and P. Sarkar, 2004. Pairing-based cryptography: A Survey. Cryptology ePrint Archive, Report 2004/064. (available at http://eprint. iacr. org/2004/064/).
11. Paterson, K.G., 2004. ID-based Signatures from Pairings on Elliptic Curves, IACR eprint, report 2002/004.(availableathttp://eprint.iacr.org/2002/004/).
12. Hess, F., 2003. Efficient identity based signature schemes based on pairings. In Proceedings of 9th Workshop on Selected Areas in Cryptography, SAC 2002, pp: 163-171.
13. Yi, X., 2003. An identity-based signature scheme from the Weil pairing. Communications Lett., 7: 76-78.
14. Cha, J.C. and J.H. Cheon, 2003. An identity-based signature from gamp Diffie-Hellman groups. Public Key Cryptography-PKC 2003, pp: 18-30.
15. Goldwasser, S. and S. Micali, 1984. Probabilistic encryption. J. Computer and System Sci. JCSS, 28: 270-99.
16. Micali, S., C. Rackoff and B. Sloan, 1988. The notion of security for probabilistic encryption. SIAM J. Computing, 17: 412-426.