<table>
<thead>
<tr>
<th>Title</th>
<th>New Subliminal Channel Embedded in the ESIGN (Special Section on Information Theory and Its Applications)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Kuwakado, Hidenori / Tanaka, Hatsukazu</td>
</tr>
<tr>
<td>Citation</td>
<td>IEICE transactions on fundamentals of electronics, communications and computer sciences, E82-A(10):2167-2171</td>
</tr>
<tr>
<td>Issue date</td>
<td>1999-10-25</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Journal Article / 学術雑誌論文</td>
</tr>
<tr>
<td>Publisher</td>
<td>publisher</td>
</tr>
<tr>
<td>Rights</td>
<td>Copyright (c) 1999 IEICE</td>
</tr>
</tbody>
</table>

URL: http://www.lib.kobe-u.ac.jp/handle_kernel/90001315

PDF issue: 2022-01-15
SUMMARY The subliminal channel is one of the methods for hiding a message in other messages. Simmons has shown conjectures on the upper bound to the bandwidth of a subliminal channel. This paper proposes a new broad-band subliminal channel embedded in the ESIGN. The bandwidth of the proposed subliminal channel is wider than that of the previous one, and it exceeds the upper bound that Simmons has conjectured. Namely, we disprove the conjectures due to Simmons. We also show that it is possible to construct the subliminal channel even if the transmitter and the subliminal receiver do not have any key in common.

key words: cryptography, digital signature, subliminal channel, ESIGN

1. Introduction

Since Simmons presented the concept of subliminal channels, many subliminal channels that are embedded in digital signature schemes have been proposed [5], [6]. The purpose of subliminal channels is to hide a message in other messages. Differing from usual cryptographic communication, a transmitter can prevent the others from being aware of the existence of cryptographic communication. For example, during an on-line meeting held by many participants, a participant can talk to the specified participant in secret by using a subliminal channel.

Simmons has classified subliminal channels into two types, i.e., a broad-band subliminal channel and a narrow-band one [6]. The definitions of these subliminal channels are as follows. A broad-band subliminal channel is one such that the bandwidth does not depend on the amount of computation required to embed a message. On the other hand, a narrow-band subliminal channel is one such that the bandwidth is logarithmically limited dependent on the exponential select and reject strategy. Here, we should notice that the bandwidth means the number of bits of the embedded message. Nevertheless, the classification is not based on the bandwidth, but on the amount of computation for embedding a message. However, the bandwidth of broad-band subliminal channels is usually several hundred bits, and that of the narrow-band ones is usually a few bits.

In this paper, we distinguish keys on digital signature as follows. We call a key for verifying a signature a verifying key. A key for computing a signature is called a signing key. We call a key that an only transmitter (signer) knows a secret key. In usual digital signature schemes, the secret key is precisely identical with the signing key. However, it is not true in broad-band subliminal channels. On the other hand, in known narrow-band subliminal channels the secret key is precisely identical with the signing key.

Let us consider the bandwidth of subliminal channels embedded in digital signature schemes. When the potential bandwidth is discussed, there are two manners; the first manner is to be focused on the number of states of digital signatures, and the second manner is to be done on the amount of transmitted data and that of keys. The first manner is especially useful for discussing the potential bandwidth of a narrow-band subliminal channel, and the second manner is available only for doing the potential bandwidth of a broad-band subliminal channel.

We mention the first manner. Assume that a digital signature employs \( z \) bits of random numbers and the digital signature can take \( 2^z \) states according to used random numbers even if a message is fixed. Then, \( z \) bits are potentially available for the subliminal communication as shown in Fig. 1.

Next, using the second manner, we consider the bandwidth of broad-band subliminal channels. Since the second manner involves the amount of transmitted data and that of keys, we discuss the potential bandwidth based on the second manner in this paper. Suppose that \( \alpha \) bits are used to communicate a signature, and the digital signature scheme provides \( \beta \) bits of security against forgery. This means that the secret key is \( \beta \) bits. Then, it seems that \( \alpha - \beta \) bits are potentially avail-

![Fig. 1 Bandwidth of subliminal channels.](image-url)
able for the broad-band subliminal channel [6]. On the bandwidth of subliminal channels, Simmons has conjectured as follows [6].

Conjecture 1: The upper bound to the bandwidth of a broad-band (work independent) subliminal channel is just the difference between the information content of the signer’s signing key, and the uncertainty about the signer’s 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.

Let the signing key be $\gamma$ bits. The difference between the number of bits of signing keys and that of the uncertainty about signing keys to a subliminal receiver is $\gamma - \beta$ bits. The conjecture 1 suggests that the upper bound to the bandwidth of a broad-band subliminal channel is $\gamma - \beta$ bits. In fact, this conjecture is true for all previous broad-band subliminal channels. A typical example of such subliminal channels is given in Sect. 2. In previous broad-band subliminal channels, it is well-known that the upper bound to the bandwidth is much less than the potential bandwidth, that is, we have $\alpha - \beta > \gamma - \beta$. Figure 2 shows the relationship between the upper bound to the bandwidth and the potential bandwidth in previous broad-band subliminal channels.

The ESIGN is one of the digital signature schemes based on the difficulty of factorization [4]. The broad-band subliminal channel embedded in the ESIGN has been proposed [5]. This paper proposes a new broad-band subliminal channel embedded in the ESIGN. The advantages of the proposed subliminal channel are the followings; (i) the bandwidth exceeds the upper bound, that is, we disprove the conjectures stated above, (ii) the transmitter does not reveal any signing key to the subliminal receiver.

The organization of this paper is as follows. Sect. 2 describes the previous subliminal channel embedded in the ESIGN. In Sect. 3, we describe the proposed subliminal channel, and discuss the indistinguishability of the proposed subliminal channel. By comparing with the previous subliminal channel, the advantages of the proposed one are concretely presented. Moreover, we mention modifications of the proposed subliminal channel. Section 4 is conclusions of this paper.

In this paper, we suppose that forging a signature in the ESIGN is equivalent to factoring the modulus. In order to distinguish the ESIGN with the subliminal channel [5], the ESIGN described in [4], which does not have the subliminal channel, is called the ordinary ESIGN. We also denote the number of bits of a non-negative integer $x$ by $\#x$.

2. Previous Subliminal Channel

We describe the previous subliminal channel embedded in the ESIGN [5]. Let $p$, $q$, and $r$ be three large primes ($p > q > r$), $n$ be of the form $n = p^2qr$. Verifying keys are $n$ and $k$ ($> 3$), and signing keys are $p$, $q$, and $r$. However, the transmitter has to give $r$ to the subliminal receiver, i.e., they have $r$ in common.

For an overt message $m$ and a covert message $m^* (< r)$, the transmitter generates the signature of $m$ as follows. Choosing a random value $c$, the transmitter computes $x$ as

$$x = m^* + cr.$$  

Then, the signature $s$ is given as

$$s = x + \left( \frac{w}{k^2} \mod p \right) pqr,$$

where $w$ is the least integer that is larger than $(h(m) - x^k \mod n)/(pqr)$, and $h$ is a public hash function.

 Receivers, including the subliminal receiver, accept $m$ as a valid message if and only if

$$h(m) \leq s^k \mod n < h(m) + O(n^{\frac{1}{2}}).$$

Moreover, since the subliminal receiver knows $r$, the subliminal receiver can obtain the covert message $m^*$ as

$$m^* = s \mod r.$$  

We observe that this is the broad-band subliminal channel, and the subliminal receiver cannot forge the signature. The signature $s$ is $\#(p^2qr)$ bits. In order to forge the signature, it is necessary to know $q$ and $r$. It follows that the signing keys is $\#q + \#r$ bits. We note that $p$ is not the essential signing key because it can be easily computed as $\sqrt{n/(qr)}$ if $q$ and $r$ are known. Since the transmitter reveals $r$ to the subliminal receiver, the secret key is only $q$. We observe that $\#q$ bits are used to provide for the security and the potential bandwidth of
the subliminal channel is \( \#(p^2q) - q \) bits. According to the conjectures, the upper bound to the bandwidth of this subliminal channel is \( \#r \) bits. In fact, the bandwidth of the subliminal channel is \( \#r \) bits, which is less than the potential bandwidth.

3. Proposed Subliminal Channel

In this section, we propose a new broad-band subliminal channel such that the subliminal receiver does not know the signing key of the transmitter.

3.1 Protocol

Let \( p \) and \( q \) be two large primes \((p > q)\), \( n \) be of the form \( n = p^2q \). Verifying keys are \( n \) and \( k \) \((k > 3)\) satisfying \( \gcd(k, \lambda(n)) = 1 \) where \( \lambda(n) = \text{lcm}(p(p-1), q-1) \). We discuss the case of \( \gcd(k, \lambda(n)) \neq 1 \) in the later part of this subsection. Secret keys are \( p \) and \( q \). In order to communicate subliminally, the transmitter and the subliminal receiver have a common key \( u \), which is not related to \( p \) and \( q \). They also know an encryption algorithm \( E \), its decryption algorithm \( D \), and the number of bits of a random prefix, denoted by \( \ell \), that is concatenated with a covert message. We assume that a ciphertext by \( E \) is \( \#(pq) - 1 \) bits, and the ciphertext can be uniquely decrypted with \( D \).

A covert message is denoted by \( m^* \), and its number of bits is \( \#(pq) - 1 - \ell \) bits. The signature of an overt message \( m \) is computed as follows. After selecting an \( \ell \)-bit random prefix \( v \), the transmitter encrypts \( v||m^* \) as

\[
d = E(v||m^*, u),
\]

where \( \| \) means concatenation. We remark that the method that a random prefix is concatenated with a covert message is one example. On the alternative method, refer to [3]. The signature \( s \) is the \( k \)-th root of \( h(m) + d \) in \( Z_n \), that is,

\[
s = (h(m) + d)^{k^{-1}} \mod n,
\]

where \( k^{-1} \) is the integer satisfying

\[
k^{-1} \equiv 1 \pmod{\lambda(n)}. \]

Similar to the ordinary ESIGN, the overt message \( m \) is accepted as a valid message if and only if

\[
h(m) \leq s^k \mod n < h(m) + O(n^{3/4}).
\]

In addition, the subliminal receiver decrpts \( (s^k \mod n) - h(m) \) as

\[
v||m^* = D((s^k \mod n) - h(m), u).
\]

Since the subliminal receiver knows the number of bits of \( v \), the subliminal receiver can obtain the covert message \( m^* \) by removing \( v \).

Since the amount of the computation for embedding \( m^* \) does not depend on the number of bits of \( m^* \), this is the broad-band subliminal channel. Since the signature is \( s \), it is \( \#(p^2q) \) bits. In order to forge the signature, it is necessary to know \( q \). Similar to usual digital signature schemes, the secret key is precisely identical with the signing key. It should notice that \( p \) is not the essential signing key because it can be easily computed as \( \sqrt{n}/q \) if \( q \) is known. Hence, \( q \) bits are used to provide for the security, and \( \#(p^2q) - q \) bits are potentially available for the subliminal channel. In the proposed subliminal channel, \( \#(pq) - 1 - \ell \) bits are actually used as the subliminal channel. Figure 3 shows the relationship the bandwidth and the potential bandwidth in the proposed subliminal channel. On the other hand, if the conjectures stated in Sect. 1 are true, then the bandwidth of the proposed subliminal channel is 0 bits because the transmitter does not reveal the signing key. Therefore, the proposed subliminal channel is a disproof of the conjectures.

We discuss the case of \( \gcd(k, \lambda(n)) \neq 1 \). Usually, in the ordinary ESIGN the value of \( k \) is chosen as the powers of two. From the viewpoint of the efficiency, it is desirable to use the powers of two because the computation such as \( s^k \mod n \) becomes to be efficient. It seems that the value of \( k \) is not related to the security as far as \( k \) is larger than three [4]. If \( \gcd(k, \lambda(n)) \neq 1 \), then there is not always a \( k \)-th root of \( h(m) + d \) in \( Z_n \). Therefore, we must find the random prefix \( v \) such that \( h(m) + d \) has a \( k \)-th root in \( Z_n \). If \( k \) is small, then the number of trails is small. In order to decide whether a given value has a \( k \)-th root, \( O(\log_2 p^2) \) multiplications on modulo \( p^2 \) and \( O(\log_2 q) \) multiplications on modulo \( q \) are required. As a typical example, we discuss the case of \( k = 4 \). Table 1 shows the probability that a 4-th root exists in \( Z_n \). In order to find the random prefix \( v \) with a 4-th root, it is necessary to examine 4–16 random prefixes on an average.

Finally, we suggest that the transmitter and the subliminal receiver use a common-key cryptosystem in
the proposed subliminal channel. It is possible to use a public-key cryptosystem instead of the common-key cryptosystem. If the subliminal receiver presents public keys for subliminal communication, then the transmitter uses them for encrypting the covert message \( m^* \). The advantage of this method is that the transmitter and the subliminal receiver do not have any common key. Namely, it is possible to construct the subliminal channel even if they do not have any key in common.

### 3.2 Indistinguishability

Any receiver, including the subliminal receiver, can not forge a signature because they do not know the signing keys \( p \) and \( q \). We show that it is infeasible for receivers to decide whether the signature involves the covert message, that is, it is hard for receivers to distinguish the signature computed with the ordinary ESIGN from that with the method described in Sect. 3.1.

In the ordinary ESIGN, a signature \( s \) is computed as

\[
s = x + \left( \frac{w}{kx^{k-1} \mod p} \right) pq,
\]

where \( x \) is a random value less than \( \max(p, q) \), and \( w \) is the least integer that is larger than \( (h(m) - x^k \mod n)/pq \). In order to prove our proposition, we show that there exists \( x \) satisfying Eq. 3 for \( s \) computed with Eq. 2. We denote \( s \mod n \) and \( \lceil s/(pq) \rceil \) by \( \tilde{x} \) and \( \tilde{y} \), respectively, i.e., \( s = \tilde{x} + \tilde{y}pq \) and \( \tilde{x} < pq \). From Eq. 2 and the assumption on the encryption algorithm \( E \), the following inequality holds.

\[
h(m) \leq s^k \mod n \leq h(m) + (2\#(pq) - 1),
\]

that is,

\[
h(m) \leq s^k \mod n \leq h(m) + pq.
\]

Since \( s^k \mod n \) is equal to \( (\tilde{x}^k + k\tilde{x}^{k-1}\tilde{y}pq) \mod n \), we have

\[
\frac{h(m) - (\tilde{x}^k \mod n)}{pq} \leq k\tilde{x}^{k-1}\tilde{y} \mod p
\]

\[
\leq \frac{h(m) - (\tilde{x}^k \mod n)}{pq} + 1.
\]

Since the probability that \( h(m) - (\tilde{x}^k \mod n) \) is divisible by \( pq \) is negligibly small, we have the followings with overwhelming probability.

\[
\tilde{y} = \frac{\tilde{w}}{k\tilde{x}^{k-1} \mod p},
\]

where

\[
\tilde{w} = \frac{h(m) - (\tilde{x}^k \mod n)}{pq}.
\]

This means that \( s \), which is computed as Eq. 2, can be interpreted as the signature that is generated with Eq. 3 when the value of \( \tilde{x} \) is adopted as a random value \( x \).

Since \( x \) in the ordinary ESIGN is a random value, the value of \( (s^k \mod n) - h(m) \) can be considered as a pseudo-random value. Hence, the value of \( d \) which is given by Eq. 1 in the proposed subliminal channel, should have the property of a pseudo-random value. This can be achieved by using a secure encryption algorithm as \( E \). Even if a covert message \( m^* \) has some statistical characteristic, it seems that the value of \( d \) does not have such a characteristic due to the encryption algorithm. If only \( m^* \) is encrypted with such an encryption algorithm and same \( m^* \) is sent twice, the value of \( d \) becomes to be same. In order to solve such a problem, it is effective to concatenate the random prefix \( v \) with \( m^* \) as stated in Sect. 3.1. Due to the random prefix and the encryption algorithm, the value of \( d \) behaves like a pseudo-random value.

### 3.3 Comparison

We discuss the performance of the proposed subliminal channel by comparing with the previous subliminal channel in Sect. 2 and the ordinary ESIGN. In order to demonstrate the results of the comparison, we suppose that primes \( p \), \( q \), and \( r \) are 512 bits.

(i) Bandwidth: The bandwidth of the previous subliminal channel is \#r bits. On the other hand, the bandwidth of the proposed subliminal channel is \#(pq) - 1 - \( \ell \) bits. For example, let the number of bits of the random prefix, i.e., \( \ell \), be 64 bits. Then, the bandwidth of the previous subliminal channel and that of the proposed one are 512 bits and 959 bits, respectively. Namely, the bandwidth of the proposed subliminal channel is about 1.87 times as wide as that of the previous one. Although the bandwidth of the previous subliminal channel achieves about 33.3\% of the potential bandwidth, that of the proposed one achieves about 93.6\%.

(ii) Amount of revealed signing keys: In the previous subliminal channel, the transmitter must reveal \( r \) to the subliminal receiver. On the other hand, in the proposed subliminal channel the transmitter does not reveal any signing key to the subliminal receiver. Hence, the amounts of revealed signing keys are 512 bits and 0 bits in the previous subliminal channel and the proposed one, respectively.

(iii) Efficiency: We discuss the time for generating the signature that the covert message is embedded in. The dominant factor in the proposed subliminal channel is the time for computing the \( k \)-th root, i.e., Eq. 2. By using the fast exponentiation method and the Chi-
Accordingly, the time for generating the signature in the proposed subliminal channel is longer than that in the previous one. Also, since a few non-modular computations and several modular computations are required in the ordinary ESIGN, the speed for generating the signature in the ordinary ESIGN is much faster than that in the proposed subliminal channel. We see that the proposed subliminal channel is inferior to the previous subliminal channel and the ordinary ESIGN in regard to the efficiency for generating the signature. However, we emphasize that the slowness on the proposed subliminal channel is not serious in practice. For example, on the case of \( \gcd(k, \lambda(n)) = 1 \), our computer simulation shows that the time for generating the signature in the proposed subliminal channel is less than 0.5 seconds on a PC. We consider that it is possible to improve the running time because the optimization of our program is not enough.

4. Concluding Remarks

We have proposed a new broad-band subliminal channel embedded in the ESIGN. The bandwidth of the proposed subliminal channel exceeds the upper bound to the bandwidth by Simmons, and is close to the potential bandwidth. We also have shown that the transmitter and the subliminal receiver do not need to have any key in common if they use the public-key cryptosystem.

Acknowledgment

The authors would like to thank the anonymous reviewers for their useful comments.

References