Digital signature with a subliminal channel

L. Harn
G. Gong

Indexing terms: Covert channel, Digital signature, Subliminal channel

Abstract: A subliminal channel is a covert communication channel to send a message to an authorised receiver; this message cannot be discovered by any unauthorised receiver. There are some applications that can take advantage of this by hiding secret messages in this subliminal channel. 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. Simmons had found that El Gamal-type digital signature schemes can be easily used to establish a subliminal channel owing to their low information rate. Simmons had also found that in all broadband subliminal channels devised thus far the receiver needs to know the transmitter's secret signing key; subliminal channels that do not require the transmitter to entrust its secret key to the subliminal receiver are generally narrowband. This limits the practical usefulness of the subliminal channel. The paper shows how to construct a digital signature scheme with a broadband subliminal channel that does not require the subliminal receiver to share the transmitter's secret signing key. The subliminal channel can be constructed in either p-channel or q-channel, where p and q are two large primes as used in the RSA scheme. To any outsider, forging a legitimate signature requires solving both the factoring problem and the discrete logarithm problem. Implementation of the signature scheme based on the Lucas function is proposed to achieve greater efficiency.

1 Introduction

The security of El Gamal's signature scheme [1] is based on solving the discrete logarithm problem. Assume that the El Gamal scheme requires β bits of security against forgery and α bits are used to communicate a signature. Since $\alpha > \beta$, α–β bits are potentially available for subliminal communication. Simmons [2] defined that if the subliminal channel uses all, or nearly all, of the α–β bits, it is said to be broadband; otherwise it is said to be narrowband.

The digital signature on a passport can be used by customs agents to authenticate the passport holder. The message in the subliminal channel can also tell customs agents that the passport holder is a known terrorist, smuggler, etc. The digital signature on a driver's license can be used by shop tellers to verify the bearer's identity. The message in the subliminal channel can also tell law enforcement agents the bearer's driving record, traffic violation history, etc. The digital signature on a credit card can be used by any commercial company to verify the customer's identity. The message in the subliminal channel can also tell verifiers the customer's credit limit, payment history, etc. Thus, there are many potential applications which can benefit from the subliminal channel.

Simmons [3] described several narrowband subliminal channels that do not require the subliminal receiver to share the transmitter's secret signing key. In Eurocrypt '93, Simmons [2] describes a broadband subliminal channel that requires the subliminal receiver to share the transmitter's secret signing key. This requirement limits the practical usefulness of the subliminal channel. Due to this requirement, the customs agent requires to know the secret signing key of the passport agency, the law enforcement agent requires to know the secret signing key of the driver's license bureau, the shop teller requires to know the secret signing key of the credit card issuer. In other words, the subliminal receiver shares the same capability with the transmitter. In general, this requirement cannot be accepted for most applications. There are three entities with different knowledge in these applications. The signature signer knows all secrets. The subliminal receivers know a partial secret to recover subliminal messages; but they cannot forge any signature. The outsiders know only the public key of the signer to verify any signature.

In this paper, we show how to construct a digital signature scheme with a broadband subliminal channel that does not require the subliminal receiver to share the transmitter's secret signing key. The subliminal channel can be constructed in either p-channel or q-channel, where p and q are two large primes as used in the RSA scheme. To any outsider, forging a legitimate signature requires to solve both the factoring problem and the discrete logarithm problem. Thus, this signature scheme is more secure in comparison with most schemes in that the security relies on just one cryptographic assumption. We also discuss variations of this scheme to improve security as well as efficiency.

2 Proposed digital signature scheme with broadband subliminal channel

Assume that there are two 'disjoint' subliminal channels, p-channel and q-channel, in the signature

IEE Proceedings online no. 19971511
Paper first received 19th September 1996

The authors are with the Department of Computer Networking, University of Missouri – Kansas City, Kansas City, MO 64110

scheme. We call them disjoint channels because we assume that each subliminal receiver can only belong to one of these two channels and receivers in these two channels do not exchange secrets with each other. The signature signer needs to select four large primes p, q, p' and q', where $p = 2p' + 1$ and $q = 2q' + 1$, and two secret keys x_p and x_q and $x_q \in [1, q - 1]$, where x_p and x_q are even integers, for these two disjoint subliminal channels. The signer needs to compute $n = pq$ and to select a public parameter $\alpha \in [1, n - 1]$ with order $(p - 1)(q - 1)$ in mod n operation. The public key used to verify any signature is y which is the common solution that satisfies both equations $y_p = y \bmod p$ and $y_q = y \bmod q$, where $y_p = \alpha^{x_p} \bmod p$ and $y_q = \alpha^{x_q} \bmod q$. We denote y as $y = CRT(y_p$ and $y_q; p, q)$ (i.e., CRT stands for the Chinese remainder theorem). The signer also needs to compute a secret signing key $x = CRT(x_p, x_q; \phi(p), \phi(q))$, where $\phi(p) = 2p'$ and $\phi(q) = 2q'$. Since $\gcd(\phi(p), \phi(q)) = 2$, by restricting x_p and x_q to even integers one can guarantee that there are two solutions of $CRT(x_p, x_q; \phi(p), \phi(q))$; one can always select the smaller one as the secret signing key x. Since each subliminal receiver needs to know either p or q to discover the subliminal message, these two secret primes cannot be kept secret from subliminal receivers. Although each subliminal receiver knows how to factor n, this information is not revealed to any outsider.

Secret key for the signer: (p, q, x_p, x_q, x)

Secret key for the q-channel receiver: (p, x_p)

Secret key for the q-channel receiver: (q, x_q)

Public key for outsider: (α, n, y)

Signature generation: For the sake of simplicity, we assume that the signer wants to sign m, where m is the one-way hash result of a meaningful message. We assume that there are two subliminal messages, $m_p \in [1, p - 1]$ and $m_q \in [1, q - 1]$, where m_p and m_q are even integers (i.e. the least significant bit is zero), needed to be hidden in p- and q- channels, respectively. The signer needs to compute $m_{pq} = CRT(m_p, m_q; \phi(p), \phi(q))$, $r_p = \alpha^{m_p} \bmod p$ and $r_q = \alpha^{m_q} \bmod q$. Again, there are two solutions of $m_{pq} = CRT(m_p, m_q; \phi(p), \phi(q))$ and we select the smaller solution as m_{pq}. Then the signer uses the Chinese remainder theorem to compute $r = CRT(r_p, r_q; p, q)$. The signer uses the secret signing key x to solve the equation $rmx = m_{pq} + s \bmod \phi(n)$, where $\phi(n) = 4p' q' \Rightarrow s = rmx - m_{pq} \bmod \phi(n)$. The signature of m is (r, s).

Signature verification: The signature (r, s) for m can be verified using the public key (α, n, y) by checking whether $y^{rm} = r\alpha^s \bmod n$.

Theorem: If $y^{rm} = r\alpha^s \bmod n$, then (r, s) is the valid signature for m.

Proof: Since the signature (r, s) for m satisfies

$$rmx = m_{pq} + s \bmod \phi(n)$$

then

$$rmx_p = m_p + s \bmod \phi(p)$$

and

$$rmx_q = m_q + s \bmod \phi(q)$$

Thus,

$$y_p^{rm} = r_p \alpha^s \bmod p$$

and

$$y_q^{rm} = r_q \alpha^s \bmod q$$

Since $y = CRT(y_p$ and $y_q; p, q)$, and $r = CRT(r_p, r_q; p, q)$, one can obtain

$$y^{rm} = r\alpha^s \bmod n$$

Message recovery in subliminal channels: The p-channel receiver uses the secret key (p, x_p) to compute $m_p = rmx_p - s_p \bmod \phi(p)$, where $s_p = s \bmod \phi(p)$. Similarly, the q-channel receiver uses the secret key (q, x_q) to compute $\mathrm{m}_q = \mathrm{rmx}_q - s_q \bmod \phi(q)$.

Discussion:

For each subliminal-channel receiver, since p- and q-channels are disjoint and thus each receiver knows either x_p or x_q, it needs to solve the discrete logarithm problem to obtain the other secret. In our signature scheme the subliminal receiver does not have the same capability as the signer.

For any outsider, to forge a signature it needs to solve both the factoring and the discrete logarithm problems. Thus, this signature scheme is more secure in comparison with most schemes in that the security relies on just one cryptographic assumption. The security of this proposed signature scheme can be found in [4].

This proposed scheme can hide any message in subliminal channels. In addition, the message can be discovered by the subliminal receiver without computing any multiplicative inverse. In [4], there is one other variation of the El Gamal signature scheme, $(r + m)x = k + s \bmod \phi(n) \Leftrightarrow y^{r+m} = r\alpha^s \bmod n$ which can provide the same result.

In the scheme we assume that p- and q- channels are disjoint. This assumption differentiates the capability between the signer and the subliminal receivers. If it is impossible to enforce this assumption in the practical application, one may just use a single subliminal channel to hide the secret message. Thus, it is impossible for subliminal receivers to obtain both secrets x_p and x_q of these two channels simultaneously. There is one alternative approach that can cause the subliminal receiver to have difficulty in forging any signature. Instead of using p- and q- channels, we create a new subliminal channel. We call it the r-channel. The signer needs to select one more prime r. The size of this prime can be much smaller than either p or q. The secret key for the r-channel is $x_r \in [1, r - 1]$. The public key for any signature is (n, y), where $n = pqr$ and $y = CRT(y_p, y_q, y_r; p, q, r)$. The signer uses the same approach to hide message m_r in the r-channel. The subliminal receiver needs to know the secret key x_r to discover the message. Although this small prime r can be factored out easily from n, the other factoring problem is still based on the size of the product of two large primes p and q. Any outsider or subliminal receiver has to solve both the factoring problem and the discrete logarithm problem to forge any signature.

3 Modified Lucas-type signature scheme with broadband subliminal channel

Recent advanced techniques imply that the computational difficulties of solving the factoring problem in Z_n and solving the discrete logarithm in Z_p are almost the same. Thus, to maintain the minimum security level for the scheme proposed in Section 2, the size of the modulus p for the discrete logarithm problem should be determined first. Then, the size of modulus n for the factoring problem will be too large. McCurley [5] proposed the first cryptosystem based on these two assumptions. However, this design results in two disadvantages: larger key size; and longer computation time. Since the computational difficulty for solving the discrete logarithm in Zp^2 is much harder than that in Z_p [6] it is possible to reduce the difference between security levels if we build our scheme based on solving the discrete logarithm in Zp^2 and solving the factoring problem in Z_n. This approach can maintain the efficiency of the implementation. Since Lucas-type cryptosystems can incorporate the factoring problem in Z_n and the discrete logarithm problem in Zp^2 together in an efficient way, we suggest modifying the signature scheme to one based on the Lucas function.

A Lucas sequence can be represented as $\mathbf{V} = \{V_k\}_{k \geq 0}$ which elements are given by

$$V_k = \xi V_{k-1} - V_{k-2}, \quad n \geq 2, \text{ in } Z_n$$

with $\xi \in Z_n$, $V_0 = 2$, and $V_1 = \xi$. A Lucas sequence in Z_n is a second-order linear recurring sequence over Z_n with the minimal polynomial $f(x) = x^2 - \xi x + 1$ and initial state $(V_0, V_1) = (2, \xi)$. Let α and α^{-1} be two roots of the minimal polynomial $f(x)$. Then $V_k(\xi) = \alpha^k + \alpha^{-k}$.

Horster *et al.* [7] proposed a Lucas-type signature scheme in 1995. As a result of their scheme the signature generation (which requires one evaluation of Lucas function) and the signature verification (which requires three evaluations of a Lucas function) are slightly less efficient than that of the original El Gamal signature scheme over GF(p). For more information on the Lucas-type signature scheme, see [7].

System setup: The signer selects four large primes, p, q, p' and q', where $p = 2p' - 1$ and $q = 2q' - 1$, and computes $n = pq$. Then select an irreducible polynomial $f(x) = x^2 - \xi x + 1$, where $f(x)$ is an irreducible polynomial over $GF(p)$ and $GF(q)$. Instead of using α as a public parameter, here the signer publishes ξ. The public key used to verify any signature is y which is the common solution that satisfies both equations $y_p = y$ mod p and $y_q = y$ mod q, where $y_p = V_{xp}(\xi)$ mod p and $y_q = V_{xq}(\xi)$ mod q. In other words, $y = CRT(y_p, y_q; p, q)$ and $x = CRT(x_p, x_q; p + 1, q + 1)$. The secret keys and public keys for the signer, subliminal receivers and outsiders are the same as in Section 2.

Signature generation: Assume that there are two subliminal messages $m_p \in [1, p]$ and $m_q \in [1, q]$ needed to be hidden in p- and q- channels, respectively. The signer needs to compute $r_p = V_{mp}(\xi)$ mod p and $r_q = V_{mq}(\xi)$ mod q. Then signer uses the Chinese remainder theorem to compute $m_{pq} = CRT(m_p, m_q; p + 1, q + 1)$ and $r = CRT(r_p, r_q; p + 1, q + 1)$. The signer uses the secret key x to solve the equation $rmx = m_{pq} + s$ mod $(p + 1)(q + 1) \Rightarrow s = rmx - m_{pq}$ mod $(p + 1)(q + 1)$.

Signature verification: The signature (r, s) for m can be verified using the public key (ξ, n, y) by checking whether $r^2 + V_{mr}^2(y) + V_s^2(\xi) = rV_{mr}(y)V_s(\xi) + 4$ mod n. The correctness of this verification can be easily checked according to Theorem 1 in [7].

Message recovery in subliminal channels: The p-channel receiver uses the secret key (p, x_p) to compute $m_p = rmx_p - s_p$ mod $(p + 1)$. Similarly, the q-channel receiver uses the secret key (q, x_q) to compute $m_q = rmx_q - s_q$ mod $(q + 1)$.

Discussion: The signature verification requires two evaluations of a Lucas function, which is one less than the scheme proposed in [7]. From [4], the following signature generation also requires just two evaluations for verification:

$$(r + m)x = k + s \bmod \phi(n)$$
$$\Leftrightarrow r^2 + V_{m+r}^2(y) + V_s^2(\xi) = rV_{m+r}(y)V_s(\xi) + 4 \bmod n$$

Breaking this system is not computationally feasible because it requires: factoring n into two large primes, and solving the discrete logarithm problem in two subgroups of Zp^2 and Zq^2. For example, if we select two large primes p and q with 614 bits each, their product is 1228-bits long. According to [6], the difficulty of solving the discrete logarithm problem in the subgroup of Zp^2, with a 614-bit prime p, is equivalent to the difficulty of factoring a 1024-bit composite integer. Thus, in this proposed scheme it is possible to reduce the difference between security levels for these two assumptions and maintain the efficiency of the implementation.

4 Conclusion

We have proposed a digital signature scheme with a broadband subliminal channel. The unique feature of the scheme is that the subliminal receiver does not require to share the sender's secret signing key. In other words, the sender does not need to completely trust the receiver. The security of the scheme is based on two different assumptions. Since the signer shares only a partial secret with the subliminal receiver, the subliminal receiver still has to solve one security problem to forge a signature. The efficiency of the basic scheme can be improved if we construct the proposed scheme on a Lucas function.

5 References

1 SIMMONS, G.J.: 'A secure subliminal channel' *in* 'Advances in Cryptology, Crypto '85', *Lect. Notes Comput. Sci.* **963**, (Springer-Verlag, 1985), pp. 33–41

2 SIMMONS, G.J.: 'Subliminal communication is easy using the DSA'. Presented at Eurocrypt '93, Lofthus, Norway, 1993

3 SIMMONS, G.J.: 'The subliminal channels in the US digital signature algorithm'. Proceedings of the 3rd symposium on *State and progress of research in cryptography*, Rome, Italy, 1993

4 HARN, L., and XU, Y.: 'On the design of generalized El Gamal-type digital signature schemes based on the discrete logarithm', *Electron. Lett.*, 1994, **30**, (24), pp. 2025–2026

5 MCCURLEY, K.S.: 'A key distribution system equivalent to factoring', *J. Cryptol.*, 1988, **1**, (2), pp. 95–106

6 BLEICHENBACHER, D., BOSMA, W., LENSTRA, A.K.: 'Some remarks on Lucas-based cryptosystems' *in* 'Advances in cryptology, Crypto '95', *Lect. Notes Comput. Sci.*, **963**, (Springer-Verlag, 1995), pp. 386–396

7 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Digital signature schemes based on Lucas functions'. Proceedings of the IFIP conference on *Communications and multimedia security*, Graz, Austria, 1995, pp. 20–21 (TC-6 and TC-11)