Short Paper

Efficient Key-Evolving Protocol for the GQ Signature[*]

CHENG-FEN LU AND SHIUHPYNG SHIEH[+]
Department of Computer Science and Information Engineering
Ta Hwa Institute of Technology
Hsinchu, 307 Taiwan
E-mail: cflu@csie.nctu.edu.tw
[+]*Department of Computer Science and Information Engineering*
National Chiao Tung University
Hsinchu, 300 Taiwan
E-mail: ssp@csie.nctu.edu.tw

Several key-evolving protocols for the Guillou-Quisquater (GQ) signature have been proposed. However, the computational loads are still high, which require the multiplication of several modular exponentiations of at least 1024-bit length. In this paper, we present a low-complexity key-evolving protocol with two additional benefits. First, it ensures the secrecy of other signing keys, even when the signing keys in some periods are compromised. Second, it provides the basic time-stamping service, which is important for legal or notary applications. Related schemes are also compared with our scheme.

Keywords: cryptography, key management, signature scheme, key-evolving protocol, GQ scheme

1. INTRODUCTION

The synchronized key-updating mechanism, or the so-called key-evolving protocol, reduces the number of re-distributions of secret keys and their exposure in public networks. In this sense, key-evolving protocols extend the lifetimes of the initial secrets. For symmetric cryptosystems, Abdalla and Bellare showed that the lifetimes of secret keys can be extended by employing proper pseudorandom functions to conduct key-updating [1]. For asymmetric cryptosystems, the recent research on forward-secure related schemes [2-9] has also shown that the lifetimes of the original cryptosystems can be extended under proper number-theoretical assumptions.

In particular, Itkis and Reyzin showed that by employing a key-evolving protocol, the original Guillou-Quisquater (GQ) signature could be made forward-secure, which

Received October 22, 2002; revised May 24, 2003; accepted June 23, 2003.
Communicated by Ja-Ling Wu.

[*] This work was done while the author was with National Chiao Tung University.

means that all signatures of previous periods are secure, even if the scheme is broken at present [5]. Furthermore, they modified the signature model and provided a key-evolving protocol, which can provide stronger security under more restricting conditions [8]. However, these two key-evolving protocols require the multiplication of several modular exponentiation operations of large numbers.

For a mobile user, such as a smart card or mobile phone owner, it is costly to support the hardware or software needed for modular exponentiation operations. To cope with this problem, a protocol design without such support is investigated here. In other words, we aim to design key-evolving protocols of low-complexity, which require no modular exponentiation operations in the process of updating the verification keys. Besides being light in terms of computation, the proposed key-evolving protocol can ensure the security of the future and past signature even if the scheme is broken at present.

This paper is organized as follows. Section 2 gives the background of the GQ signature. Section 3 extends GQ signatures to multiple periods with the key-evolving protocol. In section 4, we present security analysis of the scheme. Finally, we compare our scheme with related schemes and draw conclusions in section 5.

2. BACKGROUND

In this section, we provide the background of the GQ signature. The GQ signature scheme is a modification of the Guillou-Quisquater identification protocol [10] obtained by replacing the challenge with a one-way hash function H. The signing key s and the verification key v are related via $s^e v = 1$. The three components of the GQ signature are presented as follows.

1. Key generation: The signer generates two primes p and q ($n = pq$), and chooses a prime e as the public exponent in the RSA setting. Next, he computes $d = e^{-1}$ (mod $\phi(n)$), chooses a random number $v \in Z_n^*$, and then computes the signing key $s = (1/v)^d$ (mod n). He then publishes the verification key set $VK = (n, e, v, H)$, where H is a hash functions from $\{0, 1\}^*$ to Z_n^*. The signing key s and the system secret for the signer d are kept secret separately.
2. Signature generation: The signer chooses a random number $r \in Z_n^*$ and computes $a = H(r^e \| M)$ and $z = rs^a$. The signature pair is (a, z).
3. Signature verification: Upon receiving (a, z), the verifier computes $a' = H(z^e v^a \| M)$. He accepts the signature if $a = a'$.

In this scheme, only someone with knowledge of s can successfully forge the signature. Given arbitrary v, to compute s, the e-th root of $1/v$ is the inverse RSA problem, which is assumed to be intractable [10, 11].

3. GQ SIGNATURE VARIANT OVER MULTIPLE PERIODS

This section presents the GQ signature variant, which operates over multiple periods with the same RSA modulus. First, an efficient key-evolving protocol is presented. Then, the signature variant is compared with the original signature.

Let T denote the total number of periods. In period i, the periodic signing key s_i and verification key v_i are linked via $s_i^e v_i = 1$. The key generation algorithm is modified as follows. The signer generates two primes p and q ($n = pq$) and then chooses a prime e, the public exponent, as in the RSA setting. Next, he chooses a random number $v_0 \in Z_n^*$ and publishes the verification key set $VK = (n, e, v_0, h, H)$, where h and H are both hash functions from $\{0, 1\}^*$ to Z_n^*. H is used in the signature scheme, and h is used for the key-evolving protocol. The system secret for the signer $d = e^{-1} \pmod{\phi(n)}$ is kept secret. The key-evolving protocols for the verifiers and the signer are described as follows.

1. Key-evolving protocol for period i for verifiers:
   $VK = (n, e, v_0, h, H)$ is given to the verifiers. To compute v_i, the verifiers compute $v_j = h(v_{j-1})$ iteratively with v_0.
2. Key-evolving protocol for period i for the signer:
   To compute s_i, the signer computes $v_i = h(v_{i-1})$ and then computes $s_i = (1/v_i)^d \pmod{n}$.

The GQ signature variant is presented in Fig. 1. Compared to the original GQ signature, steps 2 and 3 are needed for key-evolving for the verifiers and signer, respectively. In each period, no matter how the periodic signing and verification keys evolve, the relation $s_i^e v_i = 1 \pmod{n}$ corresponds to the relation $s^e v = 1 \pmod{n}$ in the original GQ signature. Also, signature generation and verification in steps 4 and 5 remain unchanged.

1. Key generation: The signer generates two primes p and q ($n = pq$), and chooses a prime e as the public exponent in the RSA setting. Next, he chooses a random number $v_0 \in Z_n^*$ and publishes the verification key set $VK = (n, e, v_0, h, H)$, where h and H are both hash functions from $\{0, 1\}^*$ to Z_n^*. H is used in the signature scheme, and h is used in key-evolving. The system secret for the signer $d = e^{-1} \pmod{\phi(n)}$ is kept secret.
2. Key-evolving protocol for period i for the verifier:
   The verifier computes $v_j = h(v_{j-1})$ iteratively for j from 0 to i.
3. Key-evolving protocol for period i for the signer:
   The signer computes $v_i = h(v_{i-1})$ and then computes $s_i = (1/v_i)^d \pmod{n}$.
4. Signature generation for period i: If s_i is not available, the signer generates s_i. He chooses a random number $r \in Z_n^*$ and computes $a = H(r^e \| M)$ and $z = r(s_i)^a$. The signature for period i is (a, z, i).
5. Signature verification for period i: Upon receiving (a, z, i), the verifier updates the verification key to obtain v_i. He then computes $a' = H(z^e v_i^a \| M)$. He accepts the signature if $a = a'$.

Fig. 1. GQ signature variant for multiple periods.

4. SECURITY ANALYSIS

This section deals with security of the GQ signature variant when the system is broken during a certain period. First, two aspects of signature schemes related to different security concerns are discussed, namely, the unforgeability of signatures and the secrecy of signing keys. Next, we argue that these two aspects are equivalent in the GQ signature. Then, security analysis of the proposed scheme is presented.

Forward-security (backward-security) means that past (future) signatures are unforgeable if the present key is compromised. Forward-secrecy (backward-secrecy) ensures the secrecy of past (future) keys even if the present key is compromised. The following definitions have been proposed previously [2-5, 8, 9].

Definition 1 A signature variant is forward-secure (backward-secure) even when s_i is compromised, and any valid signature in period j, $j < i$ ($j > i$), remains unforgeable.

Definition 2 A signature variant is forward-secret (backward-secret) even when s_i is compromised, and any s_j, $j < i$ ($j > i$), remains secret.

Definition 3 A signature variant is key-independent if it is both forward-secret and backward-secret.

This concept of forward-security, which addresses the unforgeablility of signatures, was first investigated in research on forward-secure signatures [2-5]. The notion of forward-secrecy, as it addressed the secrecy of the signing key was first defined in the key exchange protocol [12]. Since it is assumed that only someone who has knowledge of the signing key can forge the GQ signature [10, 11], the conditions required for secrecy of the signing key and unforgeablility are treated as being equivalent. Therefore, the latter notion is used to evaluate the security of the scheme, which is summarized in the following proposition.

Proposition 1 The proposed signature variant is key-independent if the inverse RSA problem is intractable.

Proof: Let I denote a subset of $\{1, 2, \ldots, T\}$. Suppose the periodic singing keys s_i and $i \in I$ are compromised. Given the above compromised keys, the attacker goal in breaking forward- and backward-secrecy is to find out some other signing key s_j and $j \notin I$. Because h is seen as being the random oracle, v_j is independent of any v_i, $i \in I$. In fact, each v_j is seen as being chosen randomly from Z_n^*. In this case, the knowledge of s_i, $i \in I$ does not help someone compute $s_j \notin I$. Therefore, computing s_j from v_j is the inverse RSA problem, which is assumed to be intractable. Therefore, the proposed scheme is key-independent if the inverse RSA problem is intractable. ❑

Besides extending the lifetime of the GQ signature, this signature variant provides the basic time-stamping function, an important goal for legal applications [13]. In the following, we show that the proposed signature variant has the period-stamping function.

Definition 4 A signature variant is called period-stamping if a periodic verification key v_i is verifiable by someone with the knowledge of v_{i-1}.

Proposition 2 The proposed signature variant is a period-stamping.

Proof: In this scheme, the relation $v_i = h(v_{i-1})$ holds. ❑

5. DISCUSSION

When forward-secure signatures were originally proposed, only signing keys were updated over time, and verification keys were fixed [2, 14]. The reason for the fixed verification keys was that there was a one-to-many relationship between the verification and signing keys in the underlying signatures (the Ong-Schnorr signature [2] and Micali signature [14]). On the other hand, because the verification key was fixed, it did not provide any time-stamping function.

In contrast, this one-to-many relationship between verification and signing keys is no longer valid in the GQ signature scheme [5, 8], Okamoto-Schnorr signature [15], discrete logarithm based signatures [9], or generic signature [16]. Due to the one-to-one relationship between the verification key and signing key, both keys will be updated over time.

Therefore, these subsequent proposals [9, 16, 5, 8, 15] have to update both the signing and verification keys, either explicitly [9, 16] or implicitly [5, 8, 15].

Compared to previous schemes, our scheme requires only hash operations in the verification key-evolving stage. This avoids the need for costly hardware or software support for modular exponentiation operations. Therefore, our scheme is especially applicable to smart card or mobile phone usage of digital signature schemes.

6. CONCLUSIONS

A simple and efficient key-evolving protocol for a forward-secret, backward-secret and period-stamping variant of the GQ signature has been proposed. These features extend the lifetime of the GQ signature by using the same RSA modulus. Also, for mobile users without modular exponentiation HW/SW support, it is more practical than previous proposals.

REFERENCES

1. M. Abdalla and M. Bellare, “Increasing the lifetime of a key: a comparative analysis of the security of re-keying techniques,” in *Advances in Cryptology – ASIACRYPT 2000*, LNCS, Springer Verlag, Vol. 1976, 2000, pp. 546-559.
2. M. Bellare and S. K. Miner, “A forward-secure digital signature scheme,” in *Advances in Cryptology – CRYPTO ’99*, LNCS, Springer Verlag, Vol. 1666, 1999, pp. 431-448.

3. H. Krawczyk, “Simple forward-secure signatures from any signature scheme,” in *Proceedings of the 7th ACM Conference on Computer and Communications Security* (*CCS ’00*), S. Jajodia and P. Samarati, eds., 2000, pp. 108-115.
4. M. Abdalla and L. Reyzin, “A new forward-secure digital signature scheme,” in *Advances in Cryptolgoy – ASIACRYPT 2000*, LNCS, Springer Verlag, Vol. 1976, 2000, pp. 116-129.
5. G. Itkis and L. Reyzin, “Forward-secure signatures with optimal signing and verifying,” in *Advances in Cryptology – Crypto 2001*, LNCS, Springer Verlag, Vol. 2139, 2001, pp. 332-354.
6. W. Tzeng and Z. Tzeng, “Robust key-evolving public key encryption schemes,” Record 2001/009, Cryptology ePrint Archive, 2001.
7. Y. Dodis, J. Katz, S. Xu, and M. Yung, “Key-insulated public key cryptosystems,” in *Eurocrypt 2002*, available from IACR ePrint, 2002, pp. 65-82.
8. G. Itkis and L. Reyzin, “Intrusion-resilient signatures, or towards obsoletion of certificate revocation,” in *Crypto 2002*, available from IACR ePrint, 2002.
9. C. F. Lu and S. P. Shieh, “Secure key-evolving protocols for discrete logarithm schemes,” in *Topics in Cryptology*, CT-RSA 2002, LNCS, Springer Verlag, Vol. 2271, 2002, pp. 300-309.
10. L. C. Guillou and J. J. Quisquater, “A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory,” in *Advances in Cryptology – EUROCRYPT ’88*, LNCS, Springer Verlag, Vol. 330, 1988, pp. 123-128.
11. A. J. Menezes, P. C. van Ooschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, 1997.
12. C. G. Guenther, “An identity-based key-exchange protocol,” in A*dvances in Cryptology – EUROCRYPT ’89*, J. J. Quisquater and J. Vandewalle, eds., LNCS, Springer Verlag, Vol. 434, 1989, pp. 29-37.
13. S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *Journal of Cryptology: the Journal of the International Association for Cryptologic Research*, Vol. 3, 1991, pp. 99-111.
14. M. Abdalla and L. Reyzin, “A new forward-secure digital signature scheme,” in *Advances in Cryptology – ASIACRYPT 2000*, LNCS, Springer Verlag, Vol. 1976, 2000, pp. 116-129.
15. Y. Dodis, J. Katz, S. Xu, and M. Yung, “Strong key-insulated signature schemes,” in *Proceedings of the International Workshop on Public Key Cryptography* (*PKC 2003*), LNCS2567, 2003, pp. 130-144.
16. H. Krawczyk, “Simple forward-secure signatures from any signature scheme,” in *Proceedings of the 7th ACM Conference on Computer and Communications Security* (*CCS ’00*), 2000, pp. 108-115.

Cheng-Fen Lu (呂正棻) received her M.S. degree in Electrical and Computer Engineering Department from the University of Texas at Austin and Ph.D. degree in Department of Computer Science and Information Engineering from National Chiao Tung University in 2003. There she was with the lab of distributed system and network security, directed by Dr. Shiuh-Pyng Shieh. Also she was a NSC/DAAD exchange student at two German institutes for two years (1998-2000), including the Computer Science Department at University of Saarland and the Mathematics Department at University of Frankfurt. Currently, she is an assistant professor at the Department of Computer Science and Information Engineering, Ta Hwa Institute of Technology. Her research interests include cryptography, coding theory, and network security.

Shiuh-Pyng Shieh (謝續平) received the M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Maryland, College Park, in 1986 and 1991, respectively. He is currently a professor and the chairman of the Department of Computer Science and Information Engineering, National Chiao Tung University; the vice chairman of Chinese Cryptology & Information Security Association; director of Cisco Internetworking Technology Lab. From 1988 to 1991 he participated in the design and implementation of the B2 Secure XENIX for IBM, Federal Sector Division, Maryland, U.S.A. He is also the designer of Secure Network Protocols (SNP), a popular security shareware on the Internet. He has been consultants in the areas of network security and distributed operating systems for many institutes, such as Industrial Technology Research Institute, and National Security Bureau, Taiwan. He was on the organizing committees of numerous conferences, and is currently an editor of Journal of Computer Security, and Journal of Information Science and Engineering. Recently, he has received two outstanding research awards, honored by National Chiao Tung University and Executive Yuan of Taiwan, respectively. His research interests include internetworking, distributed systems, and network security.