Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption

Dang Nguyen Duc*, Jung Hee Cheon** and Kwangjo Kim*

*IRIS, Information and Communication University (ICU)

**Department of Mathematic, Seoul National University

Abstract

Key exposure is the most devastating attacks in any crytographic scheme. In this paper, we investigate key exposure problem in blind signature. We then present a variant of Okamoto-Guillou-Quisquater (OGQ for short) blind signature scheme guaranteeing forward secrecy. Namely, even if current secret key is revealed, forging any signature valid in the past is impossible. Our proposed scheme exhibits an efficient key updating protocol and introduces no significant communication overhead.

Key words: Key Exposure, Blind Signature, Forward Secure.

I. Introduction

Cryptography works under the assumption that a small piece of information (secret key) must be kept secret. Therefore, key exposure is the most devastating attack in all cryptographic schemes. Forward secrecy introduced by Anderson [2] is the security notion addressing key exposure problem. Intuitively speaking, forward sececy protects validity of previous usage (before key exposure) of cryptographic schemes.

Key evolution is a natural solution to prevent key exposure problem since frequently updating key makes it harder to be stolen. However, naive key evolution, *i.e.,* randomly get a new key to replace the old key, is very inefficient to guarantee forward secrecy. Specifically, in public key cryptography since if public key is randomly changed, key owner will need to register his public key again or include it in every his digital signature. Thus, in public key cryptography, we usually evolve key pair such that public key (or an essential part of public key) is not changed.

Blind signature proposed by David Chaum [1] is an interesting digital signature. It allows an user to get signature on his message from a signer without revealing the message to the signer. Blind signature has applications in electronic cash, electronic voting, etc. In this paper, we study key exposure problem in blind signature and propose a forward secure blind signature scheme. Our scheme is an variant of a provable secure blind signature scheme, namely, Okamoto-Guillou-Quisquater (OGQ for short) blind signature [3, 4, 7]. Our proposed scheme also exhibits an efficient key updating protocol and introduces no significant communication overhead.

The organization of the paper is as follows: We give several definitions in section 2. In section 3, we describe our proposed forward secure blind signature. We then analyze its security in section 4. Finally, we make the conclusion in section 5.

II. Definition

Key-evolving blind signature scheme. A

key evolving blind signature scheme has following components:

- **Setup**: This component generates system parameter as well as initial key pair for the signer, (PK, SK_1).
- **Key Update**: This component generates a new secret key for time period $t+1$, SK_{t+1} on imput secret key for time period t, SK_t.
- **Signer and User**: These two entities involve in signature issuing protocol in a given time period, say time period t. After signature issuing protocol ends, the user either output signature of the signer on his message or 'error'; the signer either output 'complete' or 'incomplete' accordingly.
- **Verification**: This procedure on input message, signature and public key of the signer, decides whether the signature is valid or not.

Security Notions. We give security notions for a key-evolving blind signature scheme with forward secrecy.

- **Blindness**: Blindness property of a blind signature scheme (with application to electronic cash) addresses anonymity of cash in real life. To satisfy blindness property, any party (especially the signer) cannot identify signature owner given that the party has all information exchanged during signature issuing protocol.
- **One-more Unforgeability**: In real life, any customer should not get more money than the bank gives him. In blind signature context, this fact was understood by Pointcheval and Stern [4]. Roughly speaking, one-more unforgeability means that user cannot get more than l signatures after l interactions with the signer.
- **Forward Secrecy**: In this paper, we focus on forward security of key-evolving protocol and blind signature. Specifically, a key-evolving protocol is forward secure if given secret key at time period t, SK_t, attacker cannot compromise any secret keys at time period j for any $j < t$. In blind signature, forward security means that even knowing the signer secret key at time peiod t, SK_t, attacker cannot forge any valid signature for any time period $j < t$.

Security Assumption. In this paper, we interest in a mathematical hard problem related to RSA cryptosystem, namely the strong RSA assumption. Firstly, we define the strong RSA problem on which the strong RSA assumption follows.

Definition 1. *Given a RSA modulus N (which is the product of large primes) and* $x \in Z_N^*$, *the RSA problem is to find* $y \in Z_N^*$ *and an integer e such that* $y^e = x$.

The strong RSA assumption states that the strong RSA problem is intractable. We also give following useful lemma regarding the strong RSA problem

Lemma 1. *Given a RSA modulus N and* $a, b \in Z_N^*$ *together with two integers* x, y *such that* $a^x = b^y$ *and* $gcd(x, y) = 1$, *one can efficiently compute* c *such that* $c^y = a$.

Lemma 1 shed a light on how to prove security of a cryptosystem in relation with the strong RSA problem. Specifically, we try derive from a forger an equation $a^x = b^y$ for some a, b, x and y. Using Lemma 1, we can then come to a solution of the strong RSA problem, thus violating the strong RSA assumption.

III. The Proposed Blind Signature Scheme with Forward Secrecy

In this section, we describe a variant of OGQ blind signature scheme guaranteeing forward secrecy. To do so, we implement a key-evolving protocol for the OGQ scheme. In one time period, our scheme works just like the OGQ scheme. We denote H as a collision-free cryptographic hash function whose domain and co-domain are $\{0,1\}^*$ and Z_*^*, respectively. We

also omit "mod N" for all computation done in $Z_{\mathcal{N}}^*$.

Setup

- *Generate two primes p' and q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are also prime. Let $\mathcal{N} = pq$ and $\phi(\mathcal{N}) = (p-1)(q-1)$.*
- *Generate a random prime e such that it is co-prime with $\phi(\mathcal{N})$.*
- *Choose a from $Z_{\mathcal{N}}^*$ of order greater than e. Also choose $r_0 \in_R Z_n^*$, $s_0 \in_R Z_{\mathcal{N}}^*$ and $e \in_R Z_{\mathcal{N}}^*$.*
- *Compute $\mathcal{V} = a^{-r_0 s_0^{-1}}$, $f_1 = a^{r_0}$, $v_1 = \mathcal{V}^2 f_1$, $\ell = 2r_0 e \div e$, $r_1 = 2r_0 e \bmod e$ and $s_1 = a^{r_0} s_0^2$.*
- *The signer's intial secret key, SK_1 is $(1, r_1, s_1, f_1, v_1)$ and the corresponding public key PK is $(\mathcal{N}, e, a, \mathcal{V})$.*

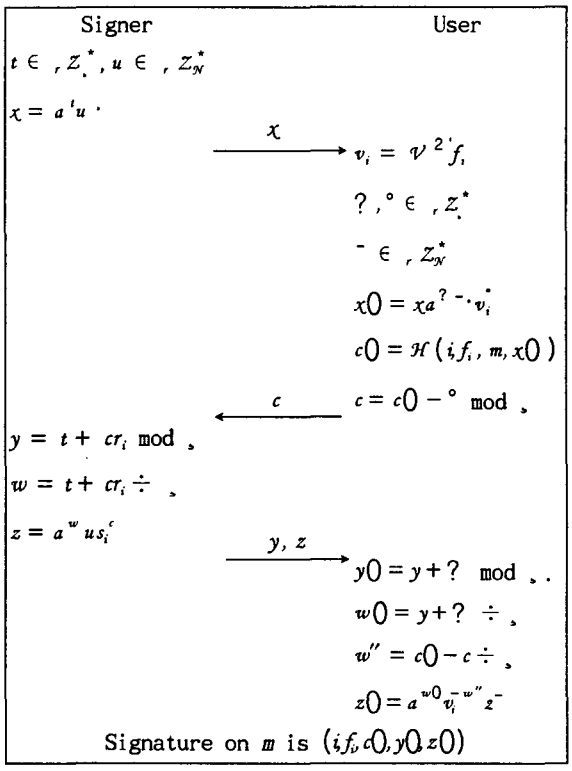
Key Update

- *Parse SK_i as (i, r_i, s_i, f_i, v_i).*
- *Choose $e \in_R Z_{\mathcal{N}}^*$.*
- *Compute $v_{i+1} = v_i^2 a^{r_i}$, $f_{i+1} = f_i^2 a^{r_i}$, $\ell = 2r_i e \div e$, $r_{i+1} = 2r_i e \bmod e$ and $s_{i+1} = a^{r_i} s_i^2$.*
- *The signer's secret key in time period $i+1$, SKi+1, is $(i+1, r_{i+1}, s_{i+1}, f_{i+1}, v_{i+1})$.*

Note that, the time period i and the corresponding f_i, v_i are not secret anyway. We assume that users, when contact with the signer, have access to those information (*e.g.* in the signer's public read-only directory).

The Signature Issuing Protocol

We describe the interactive signature issuing protocol between the signer and an user in a time period, say i.



We should emphasize that the time period index i must be enforced to be embedded into signature. Otherwise, we cannot tell in which period, a signature is issued. Furthermore, f_i is needed so that verifier can compute the verifying key $v_i = \mathcal{V}^{2^i} f_i$. One may argue that this is no better that embedding v_i into every signature so that naive key evolution (generating new key randomly) is possible. However, in blind signature, user is in charge of hashing his messages. Thus, naive key evolution cannot force user to embed correct time period index which means forward secrecy is lost.

Verification

To verify a signature $(i,f,c0,y0,z0)$ on message m (we omit the time period index on f), a verifier does the following steps:

- *Compute* $v_i = v^{2^i} f$ *and* $x00' = a^{y0} z0 v_i^{c0}$.
- *Accept the signature only if* $c0 = H(i,f,m,x00)$.

It is easy the verify the correctness of the verification procedure since we can easily show that $x00' = a^{y0} z0 v_i^{c0} = x0$.

IV.Security Analysis

We state two theorems regarding security of the proposed scheme.

Theorem 1. *The proposed scheme has blindness property.*

Proof. To prove the theorem, we should show that given any signature and any view (*i.e.*, information exchanged between the signer and user during signature issuing protocol), we can uniquely determine the blinding factors, $?, ^{-}$ and $°$. It is easily done as follows: $° = c0 - c \bmod$ $,$, $? = y0 - y \bmod ,$ and $° = z0/(a^{w0} v_i^{-w''} z)$ where w' and w'' are computed just like in signature issuing protocol. This fact prevents the signer from distinguishing signatures by using exchanged information during signature issuing protocol. To conclude, the proposed scheme satisfies blindness property.

Theorem 2. *The proposed scheme is forward secure.*

Proof. We will prove this theorem by using forking lemma proposed by Pointcheval and Stern [4]. The forking lemma states that if there exists an forger, then, with non-negligible probability, we can obtain from the forger two different signature on the same message. Specifically, suppose that we get two valid signatures $(i,f,c_1 0, y_1 0, z_1 0)$ and $(i,f,c_2 0, y_2 0, z_2 0)$ from a message m from the forger. Then, it must be the case that $a^{y0_1} z0_1 (v^{2^i} f)^{c0_1} = a^{y0_2} z0_2 (v^{2^i} f)^{c0_2}$. We expect that $v^{2^i} f = v_i$, otherwise, we try again. Since $v_i = a^{-r_i s_i^{-}}$, then we can obtain the following equation $a^{\frac{1}{2}} = 6$ for some integer 6 and $\frac{1}{2}$. Since it is very likely that $\gcd(\frac{1}{2}, ,) = 1$ (because $,$ is prime), using Lemma 1, the above equation enables us to violate the strong RSA assumption. Thus, there does not exists forger or the proposed scheme is forward secure.

V.Conclusion

We have presented the first forward secure blind signature scheme. Our proposed scheme is constructed the provably secure OGQ blind signature scheme. The key-evolving protocol in our scheme is efficient so very frequent key update (*e.g.* every 10 minutes) is possible. We believe that forward secrecy is an important feature in blind signature as it protects customers as well as the bank from loss of money (in case of electronic cash).

However, signature size is not so efficient. We should find a better key-evolving protocol to improve signature size.

Reference

[1] David Chaum, "*Blind Signatures For Untraceable Payments*", Advances in Cryptology - CRYPTO'82, Plenum Publishing, pp. 199-204, 1982.

[2] Ross Anderson, "*Two Remarks on Public Key Cryptography*", Invited Lecture, Fourth Annual Conference on Computer and Communications Security, ACM, 1997.

[3] Louis S. Guillou and Jean J. Quisquater, "*A Practical Zero-knowledge Protocol Fitted to Security Microprocessors Minimizing both*

Transmission and Memory" , Advances in Cryptology - EUROCRYPT'88, LNCS 330, Springer-Verlag, pp. 123-128, 1988.

[4]. David Pointcheval and Jacques Stern, "*Provably Secure Blind Signatures Schemes*" , Advances in Cryptology - ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp. 252-265, 1996.

[5]. Gene Itkis and Leonid Reyzin, "*Forward-Secure Signatures with Optimal Signing and Verifying*" , Advances in Cryptology - CRYPTO'01, LNCS 2139, Springer-Verlag, pp. 332-354, 2001.

[6] Mihir Bellare and Sara K. Miner, "*A Forward-Secure Digital Signature Scheme*" , Advances in Cryptology - CRYPTO'99, LNCS 1666, Springer-Verlag, pp. 431-448, 1999.

[7] Tatsuki Okamoto, "*Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes*" , Advances in Cryptology - CRYPTO'92, LNCS 740, Springer-Verlag, pp. 31-53, 1992.

[9] Ronald Crammer and Victor Shoup, "*Signature Scheme Based on the Strong RSA Assumption*" , In ACM Transactions on Information and System Security, Vol. 3, pp. 161-185, 2000.