WUJNS
Wuhan University Journal of Natural Sciences

Vol.10 No.1 2005 207-210

Article ID: 1007-1202(2005)01-0207-04

Robust Threshold Guillou-Quisquater Signature Scheme

WANG Hong[1], ZHANG Zhen-feng[2], FENG Deng-guo[1,2]

1. State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing 100039, China;

2. State Key Laboratory of Information Security (Institute of Software of Chinese Academy of Sciences), Beijing 100080, China

Abstract: The deficiencies of the first threshold Guillou-Quisquater signature scheme presented by Li-San Liu, Cheng-Kang Chu and Wen-Guey Tzeng are analysised at first, and then a new threshold Guillou-Quisquater signature scheme is presented. The new scheme is unforgeable and robust against any adaptive adversary if the base Guillou-Quisquater signature scheme is unforgeable under the chosen message attack and computing the discrete logarithm modulo a prime is hard. This scheme can also achieve optimal resilience. However, the new scheme does not need the assumption that N is the product of two safe primes. The basic signature scheme underlying the new scheme is exactly Guillou-Quisquater signature scheme, and the additional strong computation assumption introduced by the first threshold Guillou-Quisquater scheme is weaken.

Key words: veriable secret sharing; threshold cryptography; digital signature scheme; robust; secure multiparty computation

CLC number: TN 918.1; TP 309

Received date: 2004-05-31

Foundation item: Supported by the National Key Basic Research Program of China (G1999035802) and the National Natural Science Foundation of China (60373039)

Biography: WANG Hong (1972-), male, Post doctor, research direction: modern cryptography and information security. E-mail: wanghong@is.ac.cn

0 Introduction

Threshold signatures are parts of a general approach known as threshold cryptography. This approach has received considerable attention in the literature; we refer the reader to Ref. [1] for a survey of some of the work in this area.

To present fully novel threshold signature schemes and construct new threshold scheme based on well-known digital signature schemes, are hot topics in applied cryptography field. Many schemes such as threshold Elgamal-like, threshold DSS and RSA signature schems have already constructed[2-4]. In recent years, threshold signature schemes based on other widely-spreading signature schemes, e. g. Fiat-Fiege-Shamir scheme and Guillou-Quisquater scheme, are presented[5-7]. In ACNS 2003, the first threshold GQ (Guillou-Quisuater) signature scheme based on a variation of GQ scheme is given[6].

The scheme presented by Li-San Liu, Cheng-Kang Chu and Wen-Guey Tzeng (referred to LCT-TGQ scheme)[6] is very efficient, but more rigorous assumptions is additionally introduced. Thus, some limitations are resulted in. The first limitation is due to that LCT-TGQ scheme needs an assumption that N is the product of two safe primes. Known methods to jointly generate an RSA modulus cannot be easily adapted to generate a safe prime modulus. Thus, a fully distributed construction for LCT-TGQ is more difficult. Note that there may be also good reasons to avoid safe primes, other than the distributed key generation issue[2].

The second limitation is that an additional computation assumption is introduced. The key generation of basic GQ scheme is that randomly select a number $r \in Z_N^*$ as the private

key, where $Z_N^* = \{x \mid x \in Z_N, (x, N) = 1\}$. In LCT-TGQ scheme, the trusted dealer set $s = g^r \bmod N$ be the main secret and hand $s_i = g^{f(i)}$ to player P_i secretly as share. Thus, additional assumption like strong RSA assumption is needed to achieve security. This assumption is too strong and strict. Nevertheless, verifiable secret sharing technique is not easy to adapt and the trust for dealer is difficult to remove.

The third is the inaccuracy of applying (t, n) verifiable secret sharing over integers. In LCT-TGQ scheme, the basic build block is INT-JOINT-RVSS protocol, which is a variation of Pedersen unconditionally secure VSS (Verifiable Secret Sharing) over the integers[8]. However, due to the truth that each player cannot know the order of Q_N, which is exactly the range of the constant-term coefficient of $f_i(x)$, that protocol expands the range loosely to $\lfloor N/4 \rfloor - 1$. It does not fit well and has more strictness.

In this paper, a new threshold GQ signature scheme is contributed. We firstly construct several building blocks for our purpose. Then, we provide the first robust threshold version signature scheme based on original GQ scheme[9]. The scheme can withstand the limitations of LCT-TGQ scheme. Nevertheless, our threshold GQ solution maintain robustness.

Our communication model is composed of a set of n players $P_1, \cdots, P_n$ who can be modeled by polynomial-time randomized Turing machines. They are connected by a complete network of private (i. e. untappable) point-to-point channels. In addition, the players have access to a dedicated broadcast channel. The communication channels provide a partially synchronous message delivery. We assume that a polynomially bounded static or adaptive adversary can corrupt up to t of the n players in the network.

1 Building Blocks

1.1 New Revisited Pedersen VSS Protocol

The idea of the protocol is first suggested by M. Abdalla[5] and applied to robust threshold FFS scheme[7].

Initial parameters: Two large primes p and q are generated and $N = pq$. Another large prime P such that $P = xN + 1$ for some positive integer x is generated, and $g, h \in Z_p^* = \{1, 2, \cdots, P-1\}$ are two generators of order N. It is assumed that the discrete logarithm of h with respect to g is unknown to each party.

Let secret $a \in Z_N$. Let $P_1, \cdots, P_n$, be n parties, and t is the threshold. Let $L = n!$ and $L^* = L^{-1} \bmod N$.

① Shares distribution: The dealer chooses two random polynomials $f(x) = a_0 + a_1 x + \cdots + a_t x^t$ and $g(x) = b_0 + b_1 x + \cdots + b_t x^t$, where $a_0 = a$ and $a_1, \cdots, a_t; b_0, b_1, \cdots, b_t \in Z_N, a_t, b_t \neq 0$. Then secretly transmits to each party P_i his shares $s_i = f(i) \bmod N$ and $t_i = g(i) \bmod N$ respectively. The dealer also publishes $y_k = g^{a_k} h^{b_k} \bmod P$ where $k = 0, 1, 2, \cdots, t$.

② Shares verification: Each party P_i verifies its shares as: $g^{s_i} h^{t_i} \equiv \prod_{k=0}^{t} y_k^{i^k} \bmod P$. If the verification is not passed, then P_i broadcasts a complaint to the dealer. When the complaints are more than $t+1$, then dealer is disqualified. Otherwise, dealer must broadcast the correct shares satisfied with the verification equation.

③ Secret reconstruction: Each party shows its shares and verifies them with the verification equations. Let $\{s_{i_1}, \cdots, s_{i_{t+1}}\}$ is $t+1$ correct shares and $\Lambda = \{i_1, \cdots, i_{t+1}\}$. They calculate $L_i = \prod_{j \in \Lambda \setminus \{i\}} (-j)(L / \prod_{j \in \Lambda \setminus \{i\}} (i - j))$. Then the secret a can be reconstructed by interpolation: $a = \sum_{i \in \Lambda} s_i L_i L^* \bmod N$.

We denote the shares distribution of new revisited Pedersen VSS as $\mathrm{NVSS}(a, b_0)[g, h] \rightarrow (s_i, t_i)(y_0, \cdots, y_t)$. And we denote the corresponding joint-random secret sharing version as $\mathrm{JR\text{-}NVSS}(r_1, \cdots, r_n) \longleftrightarrow r$ where r_i is P_i's share for random secret $r \in_R Z_N \setminus \{0\}$.

1.2 Two Term Distributed Multiplication Protocol

Using the new VSS protocol, NVSS, in place of the protocol[10] PedVSS, we get a new two term distributed multiplication protocol for our purpose. We denote the two term distributed multiplication protocol as $\mathrm{NDM}(\{A_i\}, \{B_i\}) \longleftrightarrow (\{C_i\})$ where C_i is P_i's share for the product of secrets A and B.

1.3 Multiple Term Distributed Multiplication Protocol

Assumed K secrets $A_1, A_2, \cdots, A_K \in Z_N$ are shared securely as the protocol in section 1.1, R^k is the random companion secret of A_k:

$\mathrm{NVSS}(A_k, R^k)[g, h] \rightarrow (A_{k,i}, R_i^k)(\mathrm{EA}_0^k, \cdots, \mathrm{EA}_t^k)$,

where $A_{k,i}, R_i^k$ are the shares of party P_i, $\mathrm{EA}_0^k = g^{A_k} h^{R^k} \bmod P$, and $\mathrm{EA}_j^k = g^{a_j} h^{b_j} \bmod P$, a_j and b_j are randomly selected from Z_N, for $j \in \{1, 2, \cdots, t\}$ and $k \in \{1, 2, \cdots, K\}$.

① Each party P_i executes the following VSSs, where R_i^{22}, R_i^{kk} are the random companion secrets. $\langle\rangle$

means that the variable can be locally computed by the recievers, or it has been sent before.

$\mathrm{NVSS}(A_{1,i},R_i^1)[g,h]\rightarrow(U_{i,j}^1,R_{i,j}^1)(\langle \mathrm{VA}_{1,i}\rangle,\mathrm{EU}_{i,1}^1,\cdots,\mathrm{EU}_{i,t}^1)$

$\mathrm{NVSS}(A_{2,i},R_i^2)[g,h]\rightarrow(U_{i,j}^2,R_{i,j}^2)(\langle \mathrm{VA}_{2,i},\rangle \mathrm{EU}_{i,1}^2,\cdots,\mathrm{EU}_{i,t}^2)$

$\mathrm{NVSS}(A_{2,i},R_i^{22})[\mathrm{VA}_{1,i},h]\rightarrow(\langle U_{i,j}^2\rangle,R_{i,j}^{22})(\mathrm{EW}_{i,0}^2,\cdots,\mathrm{EW}_{i,t}^2)$

$\mathrm{NVSS}(A_{k,i},R_i^k)[g,h]\rightarrow(U_{i,j}^k,R_{i,j}^k)(\langle \mathrm{VA}_{k,i},\rangle \mathrm{EU}_{i,1}^k,\cdots,\mathrm{EU}_{i,t}^k)$

$\mathrm{NVSS}(A_{ki},R_i^{kk})[\langle \mathrm{EW}_{i,0}^{k-1}\rangle,h]$
$\rightarrow(\langle U_{i,j}^k\rangle,R_{i,j}^{kk})(\mathrm{EW}_{i,0}^k,\cdots,\mathrm{EW}_{i,t}^k)$ where $k=3,\cdots,K$

$\mathrm{NVSS}\left(\prod_{k=1}^{K}A_{k,i},R_i^1\prod_{k=2}^{K}A_{k,i}+\sum_{k=2}^{K-1}R_i^{kk}\prod_{l=k+1}^{K}A_{l,i}+R_i^{KK}\right)\cdot[g,h]\rightarrow(C_{i,j},R_{i,j})(\langle \mathrm{EW}_{i,0}^K\rangle,\mathrm{EC}_{i,1},\cdots,\mathrm{EC}_{i,t})$.

In above VSSs, $U_{i,j}^1,R_{i,j}^1,C_{i,j},R_{i,j}$ and $U_{i,j}^k,R_{i,j}^k,R_{i,j}^{kk},k\in\{2,\cdots,K\}$, are the subshares of party P_j. $\mathrm{VA}_{k,i}=g^{A_{k,i}}h^{R_i^k} \bmod P$, $k\in\{1,\cdots,K\}$, $\mathrm{EW}_{i,0}^2=(\mathrm{VA}_{1,i})^{A_{2,i}}h^{R_i^{22}} \bmod P$, $\mathrm{EW}_{i,0}^k=(\mathrm{EW}_{i,0}^{k-1})^{A_{k,i}}h^{R_i^{kk}} \bmod P$, $k\in\{3,\cdots,K\}$, and $\mathrm{EU}_{i,d}^k=g^{u_{k,d}}h^{v_{k,d}} \bmod P$, $k\in\{1,\cdots,K\}$, $\mathrm{EW}_{i,d}^2=(\mathrm{VA}_{1,i})^{w_{2,d}}h^{m_{2,d}} \bmod P$, $\mathrm{EW}_{i,d}^k=(\mathrm{EW}_{i,0}^{k-1})^{w_{k,d}}h^{m_{k,d}} \bmod P$, $k\in\{3,\cdots,K\}$, where $u_{k,d},v_{k,d},w_{k,d}$ and $m_{k,d}$ are randomly selected from Z_N for $d\in\{1,2,\cdots,t\}$. $\mathrm{EC}_{i,d}=g^{c_d}h^{z_d} \bmod P$, where c_d and z_d are randomly selected from Z_N for $d\in\{1,2,\cdots,t\}$.

② Each party P_j verifies:

$$g^{U_{i,j}^1}h^{R_{i,j}^1}\equiv \mathrm{VA}_{1,i}\prod_{l=1}^{t}\mathrm{EU}_{i,l}^{1\,j^l} \bmod P$$

$$g^{U_{i,j}^2}h^{R_{i,j}^2}\equiv \mathrm{VA}_{2,i}\prod_{l=1}^{t}\mathrm{EU}_{i,l}^{2\,j^l} \bmod P$$

$$\mathrm{VA}_{1,i}^{U_{i,j}^2}h^{R_{i,j}^{22}}\equiv \prod_{l=0}^{t}\mathrm{EW}_{i,l}^{2\,j^l} \bmod P$$

$$g^{U_{i,j}^k}h^{R_{i,j}^k}\equiv \mathrm{VA}_{k,i}\prod_{l=1}^{t}\mathrm{EU}_{i,l}^{k\,j^l} \bmod P$$

$$\mathrm{EW}_{i,0}^{k-1\,U_{i,j}^k}h^{R_{i,j}^{kk}}\equiv \prod_{l=0}^{t}\mathrm{EW}_{i,l}^{k\,j^l} \bmod P$$

where $k=3,\cdots,K$

$$g^{C_{i,j}}h^{R_{i,j}}\equiv \mathrm{EW}_{i,0}^K \bmod P$$

If verification is failed, then P_j broadcasts a complaint to P_i, and the subprotocol[10] DisQualification is performed.

③ Let I is qualified set and $\|I\|\geqslant Kt+1$. Each party P_j calculates:

$$S_j=\sum_{i\in I}\lambda_{i,I}C_{i,j} \bmod N$$

$$R_j=\sum_{i\in I}\lambda_{i,I}R_{i,j} \bmod N$$

$$\mathrm{ES}_l=\prod_{i\in I}\mathrm{EC}_{i,l}^{\lambda_{i,I}} \bmod P, l=0,\cdots,t$$

where $\mathrm{EC}_{i,0}=\mathrm{EW}_{i,0}^K$.

We denote the multiple term distributed multiplication protocol as $\mathrm{MDM}(\{A_{k,i}\},k=1,\cdots,K)\leftrightarrow(\{S_i\})$ where S_i is P_i's share for the product of secrets $A_1,A_2,\cdots,A_K$.

2 Proposed Robust Threshold GQ Signature Scheme

$\{N;P,g,h\}$ is generated as the new revisited Pedersen VSS protocol. A tuple (t,n) is selected properly. A secure hash function $H:\{0,1\}^*\rightarrow Z_N$ is chosen. The trusted center publishes $\{N;t,n;P,g,h;H(\cdot)\}$.

2.1 Key Generation

The key generation is also executed by the trusted key distribution center. Note that these steps in key generation phrase is just like the basic GQ signature scheme. It selects a secure exponent $e\in Z_N\backslash\{0\}$, $(e,(p-1)(q-1))=1$. Randomly selects a secret $a\in Z_N^*$ as the private key. It then calculates values v where $v=a^{-e} \bmod N$. Public key is v. The trusted center distributes the secret values a by running: $\mathrm{NVSS}(a,b_0)[g,h]\rightarrow(s_i,t_i)(y_0,\cdots,y_t)$. As a result, each partial signer P_i gets his share s_i for secret a.

2.2 Signature Generation

Assumed m is the message to be signed.

① All parties jointly run the protocol JR-NVSS to create a joint-random verifiable secret sharing for $r\in_R Z_N\backslash\{0\}$: $\mathrm{JR\text{-}NVSS}(r_1,\cdots,r_n)\leftrightarrow r$. The shares is $r_1,\cdots,r_n$.

② All parties run distributed multiplication protocol to securely share the product $R=r^e \bmod N$ as following:

If $n\geqslant(e+1)t+1$, then run e-term multiplication protocol: $\mathrm{MDM}(\{r_i\},k=1,\cdots,e)\leftrightarrow(\{R_i\})$.

Otherwise, if $n\geqslant 2t+1$, let public value $e=(0,\cdots,0,1,e_1,e_2,\cdots,e_{K_1-1-K_2},1)=2^{K_2}+2^{K_2+1}e_1+\cdots+2^{K_1-1}e_{K_1-1-K_2}+2^{K_1}$, $K_1-1>K_2\geqslant 0$, $e_k\in\{0,1\}$. Firstly, the protocol $\mathrm{MDM}(\{r_i\},\{r_i\})\leftrightarrow(\{r_i^{(2)}\})$ recurs K_1 times, where $r_i^{(2)}$ is ith-share for r^2, and eventually result in secure sharing $r^{2^{K_1}}$. Then noninteratively iterate the two term multiplication protocol in this order: the initial state is $\{O_i^{(0)}=r_i^{(2^{K_2})}\}$; from $k=1$ to K_1-1-K_2, if $e_k=0$, no need to do anything but resist current sharing state $\{O_i^{(k)}=O_i^{(k-1)}\}$; when $e_k=1$, perform $\mathrm{MDM}(\{O_i^{(k-1)}\},\{r_i^{(2^{K_2+k})}\})\leftrightarrow(\{O_i^{(k)}\})$, where $r_i^{(2^{K_2+k})}$ is

ith-share for internal secret $r^{2^{K_2}+k}$ and generated in former recursion phrase. Finally, all parties perform MDM($\{O_i^{K_1-1-K_2)}\}$, $\{r_i^{(2^{K_1})}\}$) $\leftrightarrow$ ($\{R_i\}$) and securely share the product $R=r^e \bmod N$.

③ Each party P_i publishes $R_i \bmod N$ and its dual share. The correctness of the published shares can be verified by every party. Now $R=r^e \bmod N$ can be interpolated by any $t+1$ correct shares.

④ Every party calculates $u=H(m \| R)$, where $\|$ denotes concatenation. Just like ②, all parties perform the multiplication protocols to distributedly share the product $a^u \bmod N$ by replacing e and r.

⑤ All parties run two term distributed multiplication protocol to create shares for the product $r \cdot a^u \bmod N$, where $a^u \bmod N$ is shared by ④. Note the shares for the final product by $\{t_i\}$.

⑥ Each party P_i publishes $t_i \bmod N$ and its dual share. The correctness of the published shares can be verified by every party. Now $s=r \cdot a^u \bmod N$ can be interpolated by any $t+1$ correct shares. The signature for m is (u,s).

3 Discussion

As discussed in Ref. [10], our distributed multiplication protocols are robust and secure. The scheme presented above can be proved secure and unforgeable by standardly constructing simulated protocols. Due to space limitation, the security analysis and proof are omitted.

Thereom 1 If the basic underlying GQ signature scheme is unforgeable under the adaptive chosen message attack, and the discrete logarithm of h with respect to g is unknown to each party, then the proposed new threshold GQ signature scheme is unforgeable and robust against the adaptive adversary who corrupts up to t players.

4 Conclusion

We propose a novel robust threshold GQ signature scheme. This is the first robust threshold version of the original GQ signature scheme.

The distributed multiplication protocols are the main techniques. Our scheme still needs the trusted dealer. However, because our scheme is exactly designed to the basic GQ scheme, the technique for fully distributed constrction of RSA signature scheme is feasibly adapted to devise a fully distributed version threshold GQ scheme without trusted dealer. We remain this problem as a further research subject.

References

[1] Desmedt Y G. Threshold Cryptography. *European Transaction on Telecommunications*, 1994, **5**(4): 449-457.

[2] Damgard I, Koprowski M. Practical Threshold RSA Signatures without a Trusted Dealer. *Proceedings of Advances in Cryptology EUROCRYPT* 2001. Berlin: Springer-Verlag Heidelberg, 2001. 152-165.

[3] Shoup V. Practical Threshold Signatures. *Proceedings of Advances in Cryptology EUROCRYPT* 2000. Berlin: Springer-Verlag, 2000. 207-220.

[4] Gennaro R, Jarecki S, Krawczyk H, *et al*. Robust threshold DSS signatures. *Proceedings of Advances in Cryptology - EUROCRYPT'96*. Berlin: Springer-Verlag, 1996. 354-371.

[5] Abdalla M, Miner S, Namprempre C. Forward Security in Threshold Signature Schemes. *Proceedings of Topics in Cryptology CT-RSA* 2001. Berlin: Springer-Verlag, 2001. 143-158.

[6] Liu L S, Chu C K, Tzeng W G. A Threshold GQ Signature Scheme. *Proceedings of Applied Cryptography and Network Security Conference ACNS* 2003. Berlin: Springer-Verlag, 2003. 137-150.

[7] Wang H, Feng D G. Robust Threshold FFS Signature Scheme. *Proceedings of the 8th Joint International Computer Conference*, JICC 2002. Hangzhou: Zhejiang University Press, 2002. 382-384.

[8] Frankel Y, MacKenzie P D, Yung M. Robust Efficient Distributed RSA-Key Generation. *Proceedings of the 30th ACM Symposium on the Theory of Computation - STOC'98*. New York: ACM Press, 1998. 663-672.

[9] Guillou L C, Quisquater J. A Paradoxical Indentity-Based Signature Scheme Resulting from Zero-Knowledge. *Proceedings of Advances in Cryptology - CRYPTO '88*. Berlin: Springer-Verlag, 1988. 216-231.

[10] Abe M. Robust Distributed Multiplication without Interaction. *Proceedings of Advances in Cryptology - CRYPTO'99*. Berlin: Springer-Verlag, 1999. 130-147.

□