Efficient Threshold Signature Scheme

Sattar J Aboud
Department of Information Technology
Iraqi Council of Representatives
Baghdad-Iraq

Mohammad AL-Fayoumi
Faculty of Computer and Information Systems,
Umm Al-Qura University
Saudi Arabia

Abstract— **In this paper, we introduce a new threshold signature RSA-typed scheme. The proposed scheme has the characteristics of un-forgeable and robustness in random oracle model. Also, signature generation and verification is entirely non-interactive. In addition, the length of the entity signature participate is restricted by a steady times of the length of the RSA signature modulus. Also, the signing process of the proposed scheme is more efficient in terms of time complexity and interaction.**

Keywords- Shamir secret sharing; threshold signature; random oracle model.

I. Introduction

Disclosure of a private key for non-cryptography purposes for example a compromise of the basic system, human mistake or insider attacks, is actually the highest threat to many cryptography schemes. The most generally suggested solution is distribution of the private key over multiple servers by secret sharing. For digital signature, the primitive we deal with in this paper is the main direction of this thought threshold signature scheme.

However, the interesting type of secret sharing scheme contains threshold scheme with a set of n participants. Their access structure contains all subgroup of t or more participants. Such schemes are called t out of n threshold schemes or just (t,n) schemes. Threshold scheme was independently presented by Shamir [1]. This scheme is relied on polynomial interpolation over a finite field. Suppose $K = GF(q)$ is a finite field with q elements. To build a (t,n) threshold scheme a dealer D selects n distinct nonzero numbers of $GF(q)$ indicated by $x_1,\ldots,x_n$, and passes x_i to P_i upon a public key channel $(i=1,\ldots,n)$. For a secret $K \in GF(q)$, D arbitrarily selects $t-1$ set $a_1,\ldots,a_{t-1}$ from $GF(q)$ and builds a polynomial $f(x) = K + \sum_{i=1}^{t-1} a_i * x^i$ .The share for participant P_i is $s_i = f(x_i)$ .The degree of $f(x)$ is at most $t-1$. It is documented that Shamir scheme is perfect. That is, when a collection of fewer that t participants work together, their original doubt about K is not reduced. Suppose that any subset of r players out of R generate a signature, but reject the generation of a valid signature when less than r players involve in the scheme. This unforgeability characteristic must keep even when certain subgroup of fewer than r players are cheated and act mutually.

For a threshold scheme to be practical if certain players are cheated, it must also be strong, meaning that cheated players must not be capable to stop honest players from creating signature. In this paper, we will consider suggested scheme which face at least one of the following difficulties:

a) *With no accurate security proof, even with a random oracle model.*

b) *Signature generation and verification is not interactive.*

c) *The length of an entity signature explodes linearly in the number of players.*

To enhance this, we will introduce a new threshold RSA-based signature scheme which faces these difficulties. We will highlight that the signature outcome is an entirely invert RSA signature, meaning that the generation and verification algorithms are the same as for common RSA signature. But, there are certain limitations on the public key which should be a prime and the modulus should be the result of two strong prime numbers. The suggested scheme is easy to calculate, and has not previously suggested. However, preceding schemes of threshold signature have that $r = w+1$. This generalization is practical in situations where the honest players is not necessity choose what they are signing, but capable to verify that a big number of them have authorized a specific signature. In specific, threshold signatures with $r = R - w$ and $w < R/3$ is used to decrease the lengths of the messages pass in coordinated network agreement scheme [1]. The use to coordinated network agreement was in fact the original purpose for this study. Almost all preceding work on threshold signatures supposes with a coordinated network, and any players in some way simultaneously agree to commence the signing scheme on a known document. Obviously, we cannot act in such a system when we desire to employ coordinated network agreement protocol.

We also highlight that the idea of a twin parameter threshold scheme gives robust security than one parameter threshold scheme; such scheme is actually more challenging to build and to discuss. The proposed idea of a twin parameter threshold scheme must not be confused with a vulnerable idea that from time to time seems in a threshold cryptosystem research [2]. For this vulnerable idea, there is a parameter $r' > w$ where the rebuilding algorithm needs r' shares, but the security is lost when only one truthful player discloses a share. In proposed idea, no security is lost unless $r - w$ truthful players disclose their shares. We work with a static cheating system; the opponent should select which players to cheat at the start of the attack. This is in line with preceding studies into threshold signatures, which also suppose static cheating. The proposed system can be verified if $r = w + 1$ in the random oracle model using the RSA signature.

II. Related Work

In 1989, Desmedt and Frankel [3] describe the difficulty with threshold signature scheme. This appear from the truth that polynomial interpolation by a coefficient ring $Z_{\theta(n)}$ such that n the RSA modulus and θ is the Euler phi. Also, Desmedt and Frankel in 1991[4] return again to the difficulty of threshold, and introduce a non-robust threshold scheme that is non-interactive but with small share length and without security discussion. Frankel and Desmedt in 1992 [5] introduce approach that providing a proof of security for a non-robust threshold scheme with small share length, but which needs coordinated interaction. Harn in 1994 [6] introduces a robust threshold scheme with small share length that also needs coordinated interaction. Gennaro et al. in 1996 [7] describe a robust threshold scheme with small share length, but again needs coordinated interaction. Actually, Gennaro et al. scheme can be examined with no reconstruction of random oracle. But this will have some practical disadvantages, demanding a particular relationship between the sender and receiver about the share of a signature. It appears that the security of these systems needs carefully examination by an acceptable approach. However, the above schemes are interactive and any threshold signature scheme relied on integer factoring seems inevitable to be interactive, because such signature schemes are randomized, and thus the signers have to create random values, which actually needs coordinated interaction.

But, in 1996 De Santis et al. [8] introduce a variant scheme that uses interaction for large share length. This scheme prevents the difficulties of polynomial interpolation over $Z_{\theta(n)}$ by working with $Z_{\theta(n)}(i)/(\theta_q(i))$, such that $\theta_q(i)$ is the q^{th} polynomial taken $\bmod \theta(n)$, and q is a prime larger than l. This is suitable, as standard secret sharing method can be directly used, but guides to a more difficult scheme that need coordinated interaction. In 1998, Rabin [9] suggests a strictly robust threshold scheme that has small share length, but need coordinated interaction. This scheme takes a diverse line of the interpolation over $Z_{\theta(n)}$ problem, avoiding it by presenting an additional layer of secret sharing and a lot more interaction. In 2006, Jun et al [10] described a non-interactive verifiable secret sharing scheme built by Shamir secret sharing scheme for secure multi-party communication scheme in distributed networks. In 2007, Li et al. [11] they introduce a secure threshold signature scheme without trusted dealer. In the meantime, the signature share generation and verification algorithms are non-interactive. In 2010 Gu, et al. [12] discuss the security of Jun et al. scheme and show that their scheme cannot withstand the misleading performance as they claimed.

$z'_A = z_A \oplus w_A \oplus w'_A$.

III. Scheme Requirments

There are three entities the player R, the dealer and an opponent. There are also a signature verification phase, a share verification phase and a share combination phase. In addition, there are two other variables, w represent number of cheated players; and r denote the number of signatures required to get a signature. The only restrictions are that $r \geq w + 1$, and $R - w \geq r$.

The opponent chooses a subset of w players to cheat. In the dealing phase, the dealer establishes a public key e and private key shares $sk_1..sk_R$, and verification keys $vk_1..vk_R$. The opponent gets the private key shares of the cheated players and the public key and verification keys. Following the dealing phase, the opponent passes signing demand to the honest players for document of his choice. Upon such a demand, a player results a signature share for the known document. The signature verification phase obtains a document, a signature and the public key, then verifies whether the signature is valid or not. The signature share verification phase obtains a document, a signature share on that document from players i, with pk, sk_x, vk_x, and verifies whether the signature share is valid or not.

IV. The Proposed Scheme

In this section, we describe the proposed scheme.

The dealer. The dealer must do the following:

1. Selects arbitrarily two primes p and q, such that $p = 2 * p' + 1, q = 2 * q' + 1$ with p', q' are also primes.
2. Finds the modulus $n = p * q$.
3. Selects the message $m = p' * q'$.
4. Selects the public key e as a prime $e > 1$.
5. The public key is (e, n).
6. Finds $d = e^{-1} \bmod m$.
7. Let $v_0 = d$.
8. Selects v_x arbitrarily from $(0, \ldots, m-1)$ for $1 \leq x \leq r - 1$.
9. The vector $v_0, \ldots, v_{r-1}$ determine the polynomial $f(i) = \sum_{x=0}^{r-1} v_x * i^x$.
10. Finds $s_x = f(x) \bmod m$ for $1 \leq x \leq R$. (1)
11. This element s_x is a secret key share of player x. This indicate by D_n the subgroup of squares in Z_n^*.
12. Selects an arbitrary $u \in D_n$.
13. Finds $u_x = u^s \in D_n$ for $1 \leq x \leq R$.
14. These statements determine the verification keys, $vk = u$ and $vk_x = u_x$.

Remarks. We will ensure that all set computations are performed in D_n, and equivalent exponent arithmetic in Z_m.

This is suitable, because $m = p^{'} * q^{'}$ has no small prime factors. Because the dealer selects $u \in D_n$ arbitrarily, suppose that u creates D_n, because this occurs with all but small probability. Since of this, the number u_x entirely find out the result of $s_x \bmod m$. For each subgroup of r points in $(0,\ldots,R)$, the result of $f(i) \bmod m$ at these points uniquely finds out the coefficients of $f(i) \bmod m$, and since the result of $f(i) \bmod m$ at every other point mod in $(0,\ldots,R)$. This follows from the information that the equivalent Vandermonde vector is invertible mod m, because its determinant is co-prime to m. From this, it ensures that for each subset of $r-1$ points in $(1,\ldots,R)$, the distributions of the result of $f(i)$ mod m at these points are standardized and equally independent. Suppose $a = R!$ for each subset s of k points in $(0,\ldots,R)$ and for each $x \in (0,\ldots,R) \setminus s$ and $y \in s$, we can describe:

$$H_{x,y}^{s} = a * \frac{\prod_{y^{'} \in s \setminus (y)^{(x-y^{'})}}}{\prod_{y^{'} \in s \setminus (y)^{(y-y^{'})}}} \qquad (2)$$

These results are resulting from the standard Lagrange interpolation equation. They are obviously integers; hence the denominator divides $y!(R-y)!$ which in divides $R!$. It is also obvious that these results are easy to calculate. From the Lagrange interpolation equation, we have:

$$a * f(x) \equiv \sum_{y \in S} H_{x,y}^{S} f(y) \bmod m \qquad (3)$$

Valid signature. We require a hash function h to elements of Z_n^{*}. If $i = h(m)$, thus the valid signature on m is $j \in Z_n^{*}$ where $j^{e} = i$. This is only a common RSA signature.

Generating signature share: In order to generate a signature share on a document m we should do the following.

1. Choose $i = h(m)$.
2. The signature share of player x is $i_x = i^{2*a*s_x}$ (4)

Correctness. The verification of correctness is just a proof of the discrete logarithm of i_x^{2} to the base $i^{'} = i^{4*a}$. (5)

However, we can simply adjust a well-known interactive scheme of Chaum and Pedersen [13]. We collapse the scheme, making it non-interactive, by employing a hash function to generate the challenge such that a random oracle model is required. We also have to handle the actuality that we are using a group D_n whose order is not known. So, this is unimportantly managed by just using adequately big integer. Suppose $L(n)$ is the bit-size of n. Assume that $h^{'}$ is the hash function, whose result is L_1 bit integer, such that L_1 is a security parameter. To build the verification of correctness player x select a random number $r \in (0,\ldots 2^{L(n)+2L_1} - 1)$, then finds:

- $u^{'} = u^{r}$
- $i^{'} = i^{'r}$
- $c = h(u, i^{'}, u_x, x_x^{2}, u^{'}, i^{'})$
- $z = s_x * c + k$

The verification of correctness is (z, c).

Correctness. one verifies that $c = h^{'}(u, i^{'}, u_x, x_x^{2}, u^{z} * u_x^{-c}, i^{'z} * x_x^{2*c})$. The cause for using i_x^{2} instead of i_x is that because i_x is assumed to be a square, this is not simply checked. This means, we are certain to be using D_n, so we want to ensure soundness.

Combining shares. Assume that we have valid shares from a group s of players, such that $s = (x_1,\ldots,x_r) \subset (1,\ldots,R)$. Assume $i = h(m)$ and suppose that $\boldsymbol{i}_{xy}^{2} = \boldsymbol{i}^{4*a_{s_{xy}}}$. Then to rearranged shares, we find $\boldsymbol{t} = \boldsymbol{i}_{x_1}^{2*H_{0,x_1}^{s}} \ldots \boldsymbol{i}_{xy}^{2*H_{0,,xy}^{s}}$ Such that H is the integers described in (2). From (3), we hold $t^{e} = i^{e^{'}}$, thus $e^{'} = 4 * a^{2}$ (6)
as $\gcd(e, e^{'}) = 1$, it is simple to find j where $j^{e} = i$, employing a standard method $j = t^{q} * i^{b}$ such that v and b are integers where $e^{'} * v + e * b = 1$; that can be got from the extended Euclidean method on $e^{'}$, and e

V. Security Discussion

Theorem 1: the proposed scheme is a secure threshold signature protocol if the common RSA signature scheme is secure. We illustrate that to simulate the opponent vision, if the opponent requests for a signature share from the honest player. Assume $x_1,\ldots,x_{r-1}$ is the set of cheated players. Consider $s_x \equiv f(x) \bmod m$ for all $1 \le x \le R$, and $d \equiv f(0) \bmod m$. To simulate the opponent vision, we just select the S_{xy} belonging to the group of cheated players randomly from the vector $(0,\ldots,\lfloor n/4 \rfloor - 1)$.

We have by now discussed that the cheated player private key shares are arbitrary numbers in the vector $(0,\ldots,m-1)$. We hold $n/4 - m = (p^{'} + q^{'})/2 + 1/4 = O(n^{1/2})$; and from this easy computation illustrates that the statistical distance between the regular distribution on $(0,\ldots,\lfloor n/4 \rfloor - 1)$ and the regular distribution on $(0,\ldots,m-1)$ is $O(n^{-1/2})$. When these S_{xy} members are selected, the values s_x for the honest players are also entirely fixed mod m, although cannot be simply calculated. Though, provided i, j and $j^e = i$, we can simply find $i_x = i^{2*a*s_x}$ for the honest player x as:

$$i_x = j^{2(H^s_{x,0} + e(H^s_{x,x_1} * s_{x_1} + \ldots + H^s_{x,x_{r-1}} * s_{x_{r-1}}))}.$$

Such that $s = (o, x_1, \ldots, x_{r-1})$, this results from (3). Employing this method, we can create the vector $u, u_1, \ldots, u_R$, and also create some share i_x of the signature, provided the common RSA signature. This case illustrates that we described the share i_x to be i^{2*a*s_x} and not i^{2*s_x}. This thought was employed by Feldman [14] in the situation of where another associated problem of provable secret sharing.

Proofs of correctness: entity can use the random oracle model for the hash value $h^'$ to obtain soundness and arithmetical zero-knowledge. This is very simple, but we drawing the information.

Now, we study soundness. We need to illustrate that the opponent cannot build, except with insignificant probability, the proof of correctness for an inaccurate share. Assume i and i_x is provided, and a valid proof of correctness (z, c). We hold $c = h^'(u, i^', u_x, i_x^2, u^', i^')$ such that:

- $i^' = i^{4*a}$
- $u^' = u^z * u_x^{-c}$
- $i^' = i^{'z} * i_x^{-2*c}$

Right away, $i^', u_x, i_x^2, u^', i^'$ are simply observed in D_n, and we are supposing that u create D_n. So we hold:

$$i^' = u^a$$
$$u_x = u^{s_x}$$
$$i_x^2 = u^B$$
$$u^' = u^j$$
$$i^' = u^g$$

For a number of integers v, B, j, g furthermore,

$$z - c * s_x \equiv j \bmod m$$
$$z * v - c * B \equiv g \bmod m$$

Multiplying the first formula by v and subtracting the second, we obtain: $c(B - s_x * v) \equiv v * j - g \bmod m$
(7)

So, the share is accurate when and only when $B \equiv s_j * v \bmod m$ (8)

When (8) fails to retain, therefore it should be unsuccessful to have $\bmod p^'$ or $\bmod q^'$, and thus (7) uniquely finds out $c \bmod$ one of these primes. Although in the random oracle model, the distribution of c is consistent and separate from the data to a hash value, and thus this still occurs with insignificant probability.

Now, we will study zero-knowledge. We can build a simulator that simulates the opponent vision without knowing the result of s_x. This observation contains the results of the random oracle at those situations where the opponent has queried the oracle, thus the simulator is in entire charge of the random oracle. When the opponent constructs a query to the random oracle, if an oracle has not been determine before at the provided point, the simulator describes it an arbitrary value, and in all cases return the result to the opponent. If an honest player is supposed to create a proof of correctness for a provided i, i_x, the simulator selects $c \in (0, \ldots, 2^{L_1} - 1)$ and $z \in (0, \ldots, 2^{L(n) + 2*L_1} - 1)$ randomly, and for provided integers i, i_x determines the number of the random oracle $(u, i^', u_x, x_x^2, u^z * u_x^{-c}, i^{'z} * i_x^{-2*c})$ to be c. With insignificant probability, the simulator has not described the random oracle at this point, and thus it is limitless to do so. The proof is (z, c). It is easy to check a distribution created by this simulator is statistically near to perfect.

From soundness, we obtain the strength of the threshold signature protocol. From zero-knowledge, we obtain the non-forgeability of the threshold signature protocol, supposing the common RSA signature scheme is secure, that is existentially non-forgeable anti-adaptive chosen message attack. Such approach is more correct in the random oracle model for h, this typed follows from the RSA-based provided random $i \in Z_n^*$, it is difficult to find j where $j^e = i$.

VI. Conclusion

In this paper, we illustrated the threshold signature scheme. We introduced a strong threshold signature scheme relied on a secret sharing scheme. The suggested signature scheme simplifies threshold RSA signature in which relied on Shamir secret sharing, and is an efficient. In addition, the method can be extended to further public key cryptography as the secret key is utilized in the exponent.

References

[1] Cachin C, Kursawe K, and Shoup V, “Random oracles in Constantinople: practical asynchronous Byzantine agreement using cryptography”, Manuscript, 2000.

[2] Micali S and Sidney R, “A simple method for generating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems”, Advances in Cryptology, Crypto'95, pages 185-196, 1995.

[3] Desmedt Y and Frankel Y, “Threshold cryptosystems”, Advances in Cryptology Crypto'89, pp, 307-315, 1989.

[4] Desmedt Y and Frankel Y, “Shared generation of authenticators and signatures”, Advances in Cryptology, Crypto'91, pp. 457-569, 1991.

[5] Frankel Y and Desmedt Y, “Parallel reliable threshold multi-signature”, Technical Report TR-92-04-02, University of Wisconsin, Milwaukee, 1992.

[6] Harn L, “Group-oriented (t; n) threshold digital signature scheme and digital multi-signature”, IEE Proceeding Computer Digital, Tech., 141(5):307-313, 1994.

[7] Gennaro R, Jarecki S, Krawczyk H, and Rabin T, “Robust threshold DSS”, “Advances in Cryptology, Eurocrypt'96, pp. 354-371, 1996.

[8] De Santis A, Desmedt Y, Frankel Y, and Yung M, “How to share a function securely”, 26th Annual ACM Symposium on Theory of Computing, pp. 522-533, 1994.

[9] Rabin T, “A simplified approach to threshold and proactive RSA”, Advances in Cryptology Crypto'98, 1998.

[10] Jun Ao and Guisheng Liao, “A Novel Non-interactive Verifiable Secret Sharing Scheme”, Chunbo Ma, Communication Technology, ICCT'06, International Conference on 27-30 November 2006, pp. 1 – 4.

[11] Jin Li, Tsz Hon Yuen and Kwangjo Kim, “Practical Threshold Signatures without Random Oracles”, Lecture Notes in Computer Science, 2007, Volume 4784, 2007, 198-207.

[12] Feng Wang, Yousheng Zhou, Yixian Yang and Yajian Zhou, “Comment on a Novel Non-interactive Verifiable Secret Sharing Scheme”, Communication Software and Networks, ICCSN'10, Second International Conference on, 26-28 Feb. 2010, pp. 157-159

[13] Chaum D and Pedersen T, “Wallet databases with observers”, Advances in Cryptology, Crypto'92, pp. 89-105, 1992.

[14] Feldman P, “A practical scheme for non-interactive verifiable secret sharing”, 28th Annual Symposium on Foundations of Computer Science, pp. 427-437, 1987.

AUTHORS PROFILE

Sattar J Aboud is a Professor and advisor for Science and Technology at Iraqi Council of Representatives. He received his education from United Kingdom. Dr. Aboud has served his profession in many universities and he awarded the Quality Assurance Certificate of Philadelphia University, Faculty of Information Technology in 2002. Also, he awarded the Medal of Iraqi Council of Representatives for his conducting the first international conference of Iraqi Experts in 2008. His research interests include the areas of both symmetric and asymmetric cryptography, area of verification and validation, performance evaluation and e-payment schemes.

Mohammad Al-Fayoumi is a Professor at Umm Al-Qura University in Saudi Arabia. He received his education from Romania. Dr. Fayoumi has served his profession in many universities. His research interests include the areas of software engineering, verification and validation, information security and simulation.