A New Signcryption Scheme and its Threshold Protocol

Yiliang Han Guangming Wu Xiaoyuan Yang

Key Laboratory on Network and Information Security of Armed Police Force, Xi'an, 710086*, P. R.China*

E-mail:yilianghan@hotmail.com

Abstract

Signcrytion scheme firstly presented by Yuliang Zheng uses hash function and symmetrical cipher to encrypt message. The first protocol for threshold generation of Zheng's signcryption couldn't support multi public verifiers. In this paper, we proposed a new signcryption scheme based on EC-ELGamal type encryption. Message to be signed and encrypt was embedded in Elliptic Curve as a point ***P***(***m***) *and encrypted by point addition which is efficient and has the same security level as exiting schemes at least. By using verifiable secret sharing and secure multi-party computation we propose a protocol for threshold generation of the signcryption. Because point addition couldn't map coordinate addition directly, we introduce a linear sum of coordinates to reconstruct the private coordinate. The protocol supports* ***k*** *out of* ***n*** *senders and the public verifier. The specific receiver can verify the validity of the signcryption before decrypting the cipher. Because the protocol is a perfect threshold scheme, it can defend the attack launched by* ***k***-1 *players. Complexity of them is less than the same schemes based on DLP.*

Keywords: *signcryption Threshold signcryption Secure multiparty computation*

1. Introduction

Secret sharing used broadly in information security systems is a valid way to protect private key. Since Shamir and Blakley presented the scheme independently in 1979[1]. Plenty of schemes are designed in the past twenty years. A secret sharing scheme consists of secret splitting stage and secret reconstructing stage. In a (***k***, ***n***) threshold scheme, a secret will be divided into ***n*** shares and each of share is held by a player. Only a qualified subset of ***k-1*** players can reconstruct the secret. In a VSS (verifiable secret sharing) scheme, players can verify whether the secret shares are correct without recovering the whole secret in splitting stage [2]. So the secret and secret pieces can be used repeatedly. VSS is a useful tool in secure multi-party computation research.

In some cases, we often complete the signature followed by encryption when a message must be private and integrated at the same time. Signcryption is a new cryptographic primitive which simultaneously fulfills both the functions of signature and encryption in a logically single step. The first signcrytion scheme was presented by Yuliang Zheng in 1997 which uses hash function and symmetrical cipher to encrypt message [4]. Zhang F., Ji D. and Wang Y. proposed the first protocol for threshold generation of Yuliang Zheng's signcryption scheme in 2002[5]. In the scheme, only specific receiver can verify the signature. Zhi Gan, Xin Li, Kefei Chen proposed a publicly verifiable threshold signcryption scheme based on DLP[6]. There are few signcryption scheme based on ECDLP.

In this paper, an implementation of Pedersen'VSS on elliptic curve was described in section 2, a

new signcryption scheme based on ECC was proposed in section 3 and its threshold protocol was proposed in section 4. Because of the peculiarity of elliptic curve, point addition couldn't map the coordinate addition, which means the sum of coordinates is not equivalent to the coordinate of the point's sum. We introduce a linear sum of coordinates to reconstruct the private coordinate.

2. Verifiable Secret Sharing Scheme for Elliptic Curve

Verifiable Secret Sharing proposed by Chor B., Goldwasser S., Micali S. and Awerbuch B. in 1985 is a useful tool to resolve Multi-party computation problems. Feldman proposed the first non-interactive VSS in 1987[3]. An implementation of Feldman'VSS on elliptic curve was described [8]. Pedersen proposed a non-interactive and information-theoretic secure verifiable secret sharing scheme in 1991[7]. Pedersen'VSS based on Shamir's scheme is a (k, n) threshold. A trusted dealer is required to charge the whole process. In this section, the scheme will be described in an elliptic curve point group. We call it EC-Pedersen Scheme in the following section.

Throughout this paper, we use capital letters to denote points on an elliptic curve and participants, lower-case letters to denote number in a finite field. Choosing an elliptic curve $E(Fq)$ in a finite field Fq (q>max (n, d), is a prime number), G is a base point, ord(G)=l. The secret to be shared is a private key $d \in Zq$, public key is $Q=dG$. A point H on $E(Fq)$ is generated by G.

Secret Splitting

Step 1: **Dealer** chooses $t \in \{1,\ldots,l-1\}$at random, computes a commitment to s: $E_0= E(s,t) =sG+tH$ and open it.

Step 2: **Dealer** chooses a secret polynomial $f(x) = (\sum_{i=0}^{k-1} f_i x^i) \bmod l$, computes $s_i=f(i)$ (i=1,2,..., n).

Set $f_0=d$, it is the secret to be shared.

Dealer chooses $g_1,\ldots,g_{k-1} \in \{1,\ldots,l-1\}$, computes a commitment $E_i =E(f_i, g_i) = f_iG+ g_i H$ (i=0,1,..., k-1).

Step 3: Let $g(x) = (\sum_{i=0}^{k-1} g_i x^i) \bmod l$, and let $t_i=g(i)$ (i=1,2,..., n).

Dealer computes a secret share (s_i, t_i)(i=1,2,..., n) and send the share to player P_i through a perfect private channel.

Dealer computes commitments $E_j =f_jG$ (j=0,1,..., k-1) which will be broadcasted to the whole group and be used to verify the shares later.

Sharers verify

When a player receives (s_i, t_i), he checks if $E(s_i, t_i) = \sum_{j=0}^{k-1} i^j E_j$.

If the test fails, t_i will be rejected because it is an illegal data.

Secrets reconstruct

Only k players out of group can reconstruct the secret polynomial by Lagrange Polynomial Interpolation as following

$$f(x)=\sum_{j=1}^{k} s_j \prod_{\substack{h=1 \\ h\neq j}}^{k} \frac{x-h}{j-h} \bmod l .$$

Let x=0, with the formula $d=\sum_{j=1}^{k} s_j \prod_{\substack{h=1 \\ h\neq j}}^{k} \frac{h}{h-j} \bmod l$, the secret d can be recovered.

The scheme can defend the attack launched by (n -1)/3 players.

3. A New Signcryption scheme based on ECC

Yuliang Zheng presented the conception of signcryption in 1997 [4]. His scheme used hash function and symmetrical cipher to encrypt message. We propose a new signcryption scheme based on Elliptic Curve Cryptosystem in this section. It is a directed scheme which does not require interactive identification. All of users knowing the public key of User A can verify the signature, while only the specific receiver can decrypt.

In the scheme, a message m which is embedded to Elliptic Curve and then become a point $P(m)$ is denoted the message which will be signed and encrypted simultaneously. User A is a signer. User B is a specific receiver.

Key generation: A random number $s_A \in \{1,\ldots,l\text{-}1\}$ is the private key of User A. His public key is a point $P_A = s_A G$. User B's private key is a random number $s_B \in \{1,\ldots,l\text{-}1\}$. His public key is a point $P_B = s_B G$.

Signcryption generation: User A will complete the following operations to sign and encrypt the message.

Step 1: Chooses $r \in \{1,\ldots,l\text{-}1\}$ at random, and computes $R=rG$;

Step 2: Computes $C= P(m)+ (s_A+r)P_B=(x_C, y_C)$;

Step 3: Computes $y=r + x_C s_A$;

(C, R, y) is the signature and will be sent to User B.

Verification: User B verifies the equation $yG=R+x_C P_A$. If the check fails the signature will be rejected.

Decryption: By the formula $P(m)=C - s_B P_A - s_B R$, the point $P(m)$ will be decrypted. Message m will be recovered easily.

In the scheme, we do not encrypt the signature, but anyone could not know the message until he know the secret key s_B. If an attacker want to forge a signature, he must compute (R, C, y). Computing y and x_C is ECDLP. If he chooses y and C first, then confirms R, not knowing k will make y to be wrong. So he will not be verified successfully. The scheme uses EC-ELGamal cryptosystem to encrypt the message, which is secure and concise.

When constructing the threshold protocol based the above scheme, we must compete the multiply of the secret data x_C and s_A. Though we can use multi–party computation to implement it, its complexity makes it not suitable for usual computation environment. Keeping the same security level and complexity degree, using addition operation to replace the multiply operation can make it easy to generate the threshold protocol. We revise the signcryption generation and verification as following:

Signcryption generation:

Step 1: Chooses $r \in \{1,\ldots,l\text{-}1\}$ at random, and computes $R=rG$;

Step 2: Computes $C= P(m)+ (s_A+r)P_B=(x_C, y_C)$;

Step 3: Computes $y=r + x_R s_A + x_C$;

(C, R, y) is the signature and will be sent to User B.

Verification: User ***B*** verify the equation $yG=R+x_RP_A+x_CG$. If the check fails the signature will be rejected.

4. A Verifiable Threshold Signcryption Protocol Based on Elliptic Curve

In this section, we will construct a threshold protocol about the above scheme, which is a multi-party secure computation problem. In case of multi-receiver, after reconstructing the collective secret key of the group, we can decrypt the cipher just as original scheme. In case of multi-sender, trusted dealer must combine all of the signcryption pieces, which is difficult, after each sender completes his operation. We will complete the latter case.

4.1 Secret Split

We use EC-Pederson scheme to split and verify the shares. In the protocol, ***Group***=$\{p_1', p_2', \ldots, p_n'\}$ is a group including n players to share the secret d (a private key of ***Group***). ***QGroup***=$\{p_1, p_2, \ldots, p_k\}$ is a qualified subset of ***Group*** including k out of n players. ***D*** is a trusted dealer. We assume all the parties are honestly following the protocol. At the end of the protocol no threshold of parties has enough information to recover the secret. Details are in section 2.

4.2 Verifiable (k, n) thresholds Signcryption

In this stage, ***Group*** will sign and encrypt a message for User ***B***. User ***B*** verifies whether the signature is correct, then decrypt the cipher.

Threshold Signcryption generation

No subset of k-1 players of ***Group*** can generate a signature.

Step 1: There are k members from ***Group*** to construct a subset ***QGroup*** that will sign the message.

Step 2: A player $p_i \in QGroup$ products a private key piece $d_i = s_i \prod_{\substack{h,i=1 \\ h\neq i}}^{k} \frac{h}{h-i}$ with s_i received in Secret Split stage. Public key piece is $Q_i=d_iG$, which will be sent to ***D***.

Step 3: The player p_i selects a number $r_i \in \{1,2,\ldots, l\text{-}1\}$ at randomly, and computes a point on elliptic curve $R_i=r_iG$, broadcasts it to ***QGroup***.

Step 4: The player p_i computes $R=\sum_{j=1}^{k} R_j = (x_R, y_R)$.

Step 5 The player p_i computes $C_i = P(m) + (d_i+r_i)P_U = (x_C, y_C)$; $y_i=r_i + x_Rd_i + x_{Ci} \bmod l$, and sends (C_i, y_i) to ***D***.

Step 6: ***D*** verifies the formula $y_iG=R+x_RQ_i+x_{Ci}G$. If the test succeeds, go to step 7, otherwise he reject the player p_i and declare him as a fake.

Step 7: ***D*** computes $x=\sum_{i=1}^{k} x_{Ci}$, $C=\sum_{i=1}^{k} C_i$, $R=\sum_{i=1}^{k} R_i$, $y=\sum_{i=1}^{k} y_i$.

In this stage, the signature is(x, C, R, y). The number x is a linear sum of coordinates.

Verify operation

User ***U*** computes the collective public key ***Q*** of ***QGroup*** and verifies whether $yG=R+x_RQ+xG$ is

correct. If the test fails, he will reject the signature and declare the signature is illegal or the group is a fake.

Decrypt operation

User U decrypt the message by the formula $P(m)=k^{-1}(C - s_B Q - s_B R)$.

4.3 Validity, security and efficiency

4.3.1 The scheme is a typical verifiable threshold system.

The scheme use Pederson'VSS scheme which is an information-theoretic secure verifiable secret sharing scheme. In secret splitting stage, players can verify whether the secret pieces are correct without recovering the secret. In signcryption generation stage, dealer can verify each signcryption pieces produced by players without recovering the secret.

At the end of the signcryption operation, each of players produces a piece of signcryption share (C_i, y_i) which matches the formula $y_i G=R+x_R Q_i+x_{Ci} G$. The collective signcryption is (x, C, R, y).

$$yG = \sum_{i=1}^{k} y_i G = \sum_{i=1}^{k} (r_i + x_R s_i \prod_{\substack{h,i=1 \\ k\neq i}}^{k} \frac{h}{h-i} + x_{Ci})G = (r + x_R d + x)G = R + x_R Q + xG .$$

User U must compute the collective public key of ***QGroup***. Player p_i computes $d_i = s_i \prod_{\substack{h,i=1 \\ h\neq i}}^{k} \frac{h}{h-i}$, $Q_i=d_i G$. Q_i is public. Thus the collective public key can be computed by the formula

$$\sum_{i=1}^{k} d_i G = \sum_{i=1}^{k} (s_i \prod_{\substack{h,i=1 \\ h\neq i}}^{k} \frac{h}{h-i})G = dG = Q .$$

So the signature is correct and easy to verify. The whole process can be done without recovering the secret.

In Decrypt operation:

$\sum_{i=1}^{k} (d_i + r_i)P_U = \sum_{i=1}^{k} (d_i + r_i)s_B G = s_B \sum_{i=1}^{k} (d_i G + r_i G) = s_B Q + s_B R$. So decryption is correct and secret information can be reconstructed without being recovered.

4.3.2 The scheme is secure.

4.3.2.1Attackers imitates legal players.

Only must attackers obtain the secret piece s_i or private piece d_i they can succeed.

In secret splitting stage, secret pieces are transmitted through a perfect private channel that can protect s_i. In all of published data, Q_i and $d_i P$ include knowledge of d_i in signcrypt operation. So attackers only can analyze Q_i ,y_i and C_i to obtain d_i. Computing d_i through Q_i and C_i are ECDLP. There is no valid way to compute d_i through y_i too.

So, we can see that attackers have no way to obtain the correct secret pieces and have no chance to finish fake operation correspondingly.

4.3.2.2 Legal signers forge illegal signature pieces to spoil the whole group's signature.

If a legal signer want to forge a signature piece, he must forge a fake (C_i, y_i) which fit for the formula $y_iG=R+x_RQ_i+x_{Ci}G$. Since R and x_R are public, computing a pair of (C_i, y_i) by $y_iG=R+x_RQ_i+x_{Ci}G$ is an ECDLP.

If a legal signer wants to forge a fake signature, he must finish it together with other players. Because the scheme is a (k,n) threshold system, so he must persuade at least of k-1 members, which means that he could accomplish the fake operation if constructing a qualified subset. Because Pedersen'VSS don't allow the shareholders talk with each other or the dealer when verifying a share, dishonest players have no chance to collaborate with each other.

4.3.3 Efficiency and complexity.

Complexity of the scheme lies in secret splitting and reconstructs operation, which is $\mathbf{O}(k^3)$, just as others based on Shamir's scheme.

The communication complexity of the scheme is far belowwer than other systems based on DLP[5][6]. In secret split stage, D broadcasts the verify data E_j, that is k points on elliptic curve and data amount is $2t\log q$ bit. D sends a $2\log l$ bit data (s_i, t_i) to each player. In signcryption operation, each player send $2\log q+\log l$ bits data to D and broadcast $2\log q$ bits data. If q is a 160 bit data, which is safe currently, the total communicate data of the scheme are no more than 1/6 of other systems'.

Conclusion

A pure elliptic curve signcryption scheme and its threshold generation protocol are firstly proposed in this paper. Just as other schemes, the multiply operation of two secret shares is complex to implement. So we revise the original scheme in the condition of keeping the same security degree. The threshold cryptosystem based on ECC is different to systems based on DLP just because of the peculiarity of ECC. Designing special mathematical frame fit for ECC is a hard work in the area. The access structure on ECC is the next research topic.

References

[1] A. Shamir, "How to Share a Secret", *Communications of the ACM*, 1979, 22(11), pp.612-613

[2] Chor B.,Goldwasser S. Micali S. Awerbuch B. "Verifiable secret sharing and achieving simultaneity in the presence of faults.", *Proceedings of 26th IEEE symposium on foundations of computer science*, 1985, pp.151-160

[3] Feldman P. "A Practical Scheme for Mon-Interactive Verifiable Secret Sharing", *Proceedings of 28th IEEE symposium on Foundations of Computer Science*, 1987:427-437

[4] Yuliang Zheng, "signcryption and its application in efficient public key solutions." *Proceedings of Information Security Workshop*, Spring-Verlag, 1997, pp.201-208

[5] Zhang Futai, Ji Dongyao, Wang Yumin, "A Protocol for Threshold Generation of Signcryption", *Proc of Chinacrypt'2002*, Beijing: Publishing House of Electronics Industry, 2002, pp.193-202

[6] Zhi Gan, Xin Li, Kefei Chen, "A Publicly Verifiable Threshold Signcryption Scheme", *Proc of Chinacrypt'2004*, Beijing: ,Science Publish House, 2004, pp.105-109

[7]T.P.Pedersen, "Distributed Provers with Applications to Undeniable Signatures", *Proc of Eurocrypt'91*, *Lecture Notes in Computer Science*, *LNCS 547*, Berlin: Spring-Verlag, 1991, pp. 221-238

[8]Han Yiliang, Yang Xiaoyuan, Sun Jun, Li Delong, "Verifiable Threshold Cryptosystems Based on Elliptic Curve", *Proc of ICCNMC'2003*, IEEE Computer Society, 2003, pp.334-337