Construction of Dynamic Threshold Decryption Scheme from Pairing

Yu Long and Ke-Fei Chen
(Corresponding author: Yu Long)

Department of Computer Science and Engineering, Shanghai Jiao Tong University
Postbox A0403391, 800 DongChuan Road, Shanghai 200240, P. R. China (Email: longyu@sjtu.edu.cn)

(Received July 6, 2005; revised and accepted Aug. 9, 2005)

Abstract

The first dynamic threshold decryption scheme from pairing is presented. It is secure in groups equipped with a bilinear map, and caters to some important requirements in real application; including the needs to renew the master key, or to add/remove or update a decryption sever, without leaking any information on the master key and changing other decryption servers' secret keys.

Keywords: Dynamic, pairing, threshold decryption

1 Introduction

In 2001, Boneh and Franklin [1] proposed a practical identity based (ID-based) encryption scheme from the weil paring, which provides a public key encryption mechanism that a public key is an arbitrary string. Then, ID-based threshold decryption from pairing has been considered in [2, 3]. However, these schemes do not solve the problem of updating the system's master key without additional security communications between the trusted third party and every decryption server, and they are hard to be applied. The main idea underlying a threshold decryption scheme is that the ciphertext cannot be decrypted unless of decryption servers collude. In [5], a dynamic threshold scheme was proposed. It has the advantage that the shared secret can be renewed without changing the shares. However, if shareholders collude, the shared secret can be recovered by Lagrange interpolation as described in [5].

In this paper, we construct a successful dynamic threshold decryption scheme from pairing which not only keeps merits of [5], but also solves the problem of decrypting the ciphertext without betraying the master key.

2 Preliminaries

2.1 Bilinear Pairings

Let G be a cyclic additive group and G_1 be a cyclic multiplicative group of the same prime order q. Assuming that the discrete logarithm problems in both G and G_1 are hard. A bilinear pairing is a map $e : G \times G \to G_1$ which satisfies the following properties:

1) Bilinear: for any $P, Q \in G$, and $a, b \in Z_q^*$, we have $e(P^a, Q^b) = e(P, Q)^{ab}$.

2) Non-degenerate: there exists $P \in G$ and $Q \in G$ such that $e(P, Q) \neq 1$.

3) Computable: Given $P, Q \in G$, there is an efficient algorithm to compute $e(P, Q) \in G_1$.

Such a bilinear pairing may be realized using the modified Weil pairing and Tate pairing associated with supersingular elliptic curve.

2.2 Threshold Scheme

The idea of (k, n) threshold secret sharing was proposed in [4]. In a (k, n) threshold scheme, the secret is divided into n pieces, and:

1) The shared secret s is recoverable from any k pieces $(k \leq n)$.

2) Knowledge of $k-1$ or fewer pieces provides absolutely no information about s.

In conventional (k, n) threshold decryption schemes, the private key for decryption is divided into n parts. Less than k decryption servers can't reveal any information on the ciphertext, and k or more of them can decrypt the ciphertext with their secret shares. However, when the private key is renewed, n decryption servers' secret shares must be updated accordingly, by secure channels. It is time-consuming and very inconvenient.

2.3 Dynamic Threshold Decryption

One dynamic secret sharing scheme was proposed in [5], applying the idea to decryption, a dynamic (k, n) threshold decryption scheme should satisfy four properties:

1) Renewing the private key for decryption without change n decryption server's secret shares.

2) Adding a decryption server without changing other decryption servers' secret shares and with leaking no information about the private key.

3) Removing a decryption server without changing other decryption severs' secret shares and leaking no information about the decryption private key.

4) Renewing one decryption server's secret share without changing other decryption servers' secret shares and with leaking no information about the private key.

3 Dynamic Threshold Decryption Scheme from Pairing

Our scheme can be described in terms of following five phases:

1) Setup:
In our setting, there exists a trusted authority private key generator (PKG), who chooses two bilinear groups G and G_1 of the same prime order p, and g be a generator of G. Let $e : G \times G \mapsto G_i$ be a bilinear map (e.g., weil pairing). The plaintext $M \in G_1$, and the public key $ID \in Z_p^*$. ID can be an arbitrary string such as the hash value of telephone number. PKG randomly selects $x, y \in Z_p^*$ and compute $X = g^x, Y = g^y$, . The public parameters cp and the master key are given by: $cp = (g, X, Y)$, $mkey = (x, y)$. Where x is kept in secret for long term and y needs to be renewed periodically.

2) KeyGen:
Assume n decryption servers are $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$. The PKG takes the following steps to set up the relationship between y and Γ_i:

   a. Each Γ_i chooses a secret key $s_i \in Z_p^*$ and computes a public key

   b. The PKG picks randomly a polynomial of degree $k-1$ over $Z_p : f(\alpha) = y + \sum_{i=1}^{k-1} b_i \alpha^i, b_{k-1} \in Z_p^*$.

   c. The PKG computes $k_i = g^{\frac{f(i)}{(ID+x)(p_i)^y}}$, $v_i = e(g, g)^{f(i)}$ and then publishes k_i, v_i.

3) Encryption:
To encrypt a message M under public key ID, pick a random $S \in Z_p^*$ and output ciphertext: $C = (g^{S \cdot ID} \cdot X^S, e(g, Y)^S \cdot M) = (A, B)$.

4) Γ_i's Sub-decryption:
To compute a decryption share δ_i of the ciphertext $C = (A, B)$, using its private key s_i, decryption sever Γ_i calculates:

$$\begin{aligned} \delta_i &= e(A, g^{Y_i^S})^{k_i} \\ &= e(A, g)^{Y^{S_i} \cdot k_i} \\ &= e(g, g)^{S \cdot (ID+x) \cdot (p_i)^{y \cdot k_i}} \\ &= e(g, g)^{S \cdot f(i)} \end{aligned}$$

5) Decryption:
Without loss of generality, assume Γ_1, Γ_2, $\cdots$, Γ_k are k decryption servers who want to decrypt the ciphertext. A dealer (one of the servers) collects δ_1, δ_2, $\cdots$, δ_k and computes

$$\begin{aligned} \Delta &= \prod_{j=1}^{k} (\delta_j)^{\prod_{i=1, i \neq j}^{k} \frac{-i}{j-i}} \\ &= e(g, g)^{S \cdot (\sum_{j=1}^{k} f(j) \cdot \prod_{i=1, i \neq j}^{k} \frac{-i}{j-i})} \\ &= e(g, g)^{S \cdot y} \end{aligned}$$

by employing Lagrange interpolation. Therefore, M can be recovered by $\frac{B}{\Delta} = \frac{e(g,g)^{y \cdot S} \cdot M}{e(g,g)^{S \cdot y}}$. Note $g, X, Y, ID, p_i, k_i, v_i$ for $1 \leq i \leq n$ 1 are public information of our scheme. Γ_i could examine the validity of k_i by checking $e(g^{ID} \cdot X, (k_i)^{Y^{S_i}}) = v_i$.

4 Security and Dynamic

4.1 Security Discussion

For $1 \leq i \leq n$, $\Gamma_i$can obtain only public information k_i, $v_i (= e(g, g)^{f(i)})$, $Y (= g^y)$, X. However, to derive $f(i)$ or y from v_i or y, Γ_i has to cope with the difficulty of solving the discrete logarithm problem in G. Thus even k members of our dynamic (k, n) threshold decryption scheme collude, a valid single share $f(i)$ of y could not be obtained. Thus y cannot be derived.

4.2 Dynamic Analysis

1) Consider the case when y is renewed. Assume (x, y') is the new master key. The PKG picks another polynomial over $Z_p^* : f'(x) = y' + \sum_{i=1}^{k-1} b_i' \alpha^i$, and refreshes public information Y, k_i, v_i to be $Y' = g^{y'}$, $(i = 1, 2, \cdots, n)$.

2) Adding decryption sever Γ_{n+1}. Γ_{n+1} selects $s_{n+1} \in Z_p^*$ to calculate and publish $p_{n+1} = g^{s_{n+1}}$. The PKG computes $k_{n+1} = g^{\frac{f(n+1)}{(ID+x)(p_{n+1})^y}}$, $v_{n+1} = e(g, g)^{f(n+1)}$ and then publishes k_{n+1}, v_{n+1}.

3) Removing decryption sever Γ_i $(i \in \{1, 2, \cdots, n\})$. The PKG selects another polynomial $f'(\alpha)$ of degree $k-1$ in Z_p with $f'(0) = y$, and refreshes $(k_1, k_2, \cdots, k_n)$, $(v_1, v_2, \cdots, v_n)$ accordingly. Set the value of v_i and k_i to be "NULL".

4) Consider the case when Γ_i's secret key s_i is renewed. Γ_i chooses s_i' as the new secret key. Then Γ_i refreshes public information to be k_i, and the PKG refresh to be $k_i' = g^{\frac{f(i)}{(ID+x)(p_i')^y}}$ $(i = 1, 2, \cdots, n)$.

5 Conclusions

In this paper, we propose a secure dynamic (k, n) threshold decryption scheme from pairing, which allows the master key and n decryption servers' secret keys to be renewed, or to add/remove a decryption server, without secure channels between PKG and decryption servers. In addition, k of n decryption servers can decrypt the ciphertext without revealing the master key.

Acknowledgements

This work was partially supported by NSFC under the grants 60273049, 90104005 and 60303026.

References

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Crypto 2001*, LNCS 2139, pp. 213-229, 2001.

[2] Z. C. Chai, Z. F. Cao, and R. X. Lu, "ID-based threshold decryption without random oracles and its application in key escrow," in *Inforsec 2004*, ACM press, pp. 119–124, 2004.

[3] B. Libert and J. J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in *PODC 2003*, ACM press, pp. 163–171, 2003.

[4] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[5] H. M. Sun and S. P. Shieh, "Construction of dynamic threshold schemes," *Electronics Letters*, vol. 30, no. 24, pp. 2023–2025, 1994.

Yu Long received the B.S. degree in computer science and technology in South West Jiao Tong University, China, and received the M.S. degree in information security engineering department, Shanghai Jiao Tong University, China, and now she is a Doctor Candidate in the same school. Her research interests include information theory and modern cryptography.

Ke-Fei Chen received his Ph.D degree in Justus Liebig University Giessen, Germany, 1994. His main research areas are classical and modern cryptography, theory and technology of network security, etc. Since 1996, he came to Shanghai Jiao Tong University and become the Professor at the Department of Computer Science and Engineering. Up to now (1996-2005), more than 80 academic papers on cryptology and information security have been published in Journals.