Towards Time-Bound Hierarchical Key Assignment for Secure Data Access Control

Tsu-Yang Wu[1,2], Chengxiang Zhou[1], Chien-Ming Chen[1,2], Eric Ke Wang[1,2], and Jeng-Shyang Pan[1,2]

[1] Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, 518055, China
[2] Shenzhen Key Laboratory of Internet Information Collaboration, Shenzhen, 518055, China
{wutsuyang,hitcms2009,chienming.taiwan,jengshyangpan}@gmail.com, 962982698@qq.com

Abstract. Time-bound hierarchical key assignment (TBHKA) scheme is a cryptographic method to assign encryption keys to a set of security classes in a partially ordered hierarchy. Only the authorized subscriber who holds the corresponding key can access the encrypted resources. In 2005, Yeh proposed a RSA-based TBHKA scheme which is suitable for discrete time period. However, it had been proved insecure against colluding attacks. Up to now, no such TBHKA schemes were proposed. In this paper, we fuse pairing-based cryptography and RSA key construction to propose a secure TBHKA scheme. In particular, our scheme is suitable for discrete time period. The security analysis is demonstrated that our scheme is secure against outsider and insider attacks (including colluding attacks). Finally, the performance analysis and comparisons are given to demonstrate our advantage.

Keywords: Access control, key assignment, bilinear pairings, Cryptography.

1 Introduction

The access control (AC) problem is to deal with users who can access some sensitive resources in a system. According to users' priority, users are organized in a hierarchy formed by several disjoint classes (called security classes). These classes have different limitations on the resources. In other words, some users own more access rights than others. In the real world, the AC problem is applied to several applications such as hospital system, computer system, etc.. For example, in computer system, administrator has the high priority to access all files (including sensitive files), but general users only access some common files. Up to now, several famous hierarchical key assignment schemes [1,3,5,6,10,11,13,14,16] had been published to solve the AC problem and address the data security.

In some situations, time-bound property may be involved in the AC problem such as Pay-TV system. In Pay-TV system, subscriber desires to subscribe

L.S.-L. Wang et al. (Eds.): MISNC 2014, CCIS 473, pp. 437–444, 2014.

some channels for some certain time periods such as one week, one month, or one year. Hence, subscribers should be assigned different keys for each time period. If the time period expires, the subscriber should not derive any keys to access subscribed channels. Time-bound hierarchical key assignment scheme is a cryptographic method to assign encryption keys to a set of security classes in a partially ordered hierarchy, where the keys are dependent on the time. Note that if two classes form a relation, the subscriber who is in the higher class can access the resources in the lower class, however not vice versa.

In 2002, Tzeng [20] proposed the first time-bound hierarchical key assignment scheme by using Lucas function. However, Yi and Ye [27] pointed that his scheme suffered from a colluding attack in 2003. In 2004, Chien [9] proposed an efficient time-bound hierarchical key assignment scheme by using two hash values. Unfortunately, his scheme was also suffered from a colluding attack mentioned by Yi [26]. In 2005, Yeh [25] proposed an RSA-based hierarchical key assignment scheme. However, Ateniese et al. [2] pointed that Yeh's scheme [25] is insecure against colluding attack in 2006. Meanwhile, they proposed the unconditionally secure and computationally secure setting for a time-bound hierarchical key assignment scheme with a tamper-resistant device. In the same year, Wang and Laih [21] proposed a time-bound hierarchical scheme by using merging. In 2009, Sui et al. [18] proposed the first time-bound access control scheme for support dynamic access hierarchy. In 2012, Chen et al. [7] proposed a time-bound hierarchical key management scheme without tamper-resistant device. In the same year, Tseng et al. [19] proposed two pairing-based time-bound key management schemes without hierarchy. In their two schemes, one scheme combines Lucas function and is suitable for continuous time period. Another scheme fuses the RSA construction and is suitable for discrete time period. In 2013, Chen et al. [8] proposed the first hierarchical access control scheme in cloud computing. However, their scheme did not consider the time-bound property. Recently, Wu et al. [24] extended Chen et al.'s scheme [7] to propose the first time-bound hierarchical key management scheme in cloud computing.

Up to now, no secure time-bound hierarchical key assignment (TBHKA) scheme which is suitable for discrete time period is proposed. In this paper, we fuse pairing-based cryptography and RSA key construction to propose a secure TBHKA scheme. In particular, our scheme is suitable for discrete time period. The security analysis is demonstrated that our scheme is secure against outsider and insider attacks (including colluding attacks). Finally, the performance analysis and comparisons are given to demonstrate our advantage.

The rest of this paper is organize as follows: In Section 2, we introduce the concept of partially ordered hierarchy, bilinear pairings, and RSA cryptosystem. Our concrete scheme is proposed in Section 3. In Section 4, we demonstrate the security analysis of our scheme. The performance analysis is given in Section 5 and the conclusions are draw in Section 6.

2 Preliminaries

In this section, we brief review the concept of partially ordered hierarchy, bilinear pairings, and the RSA cryptosystem.

2.1 Partially Ordered Hierarchy

Consider a set of resources organized into a number of disjoint classes. A binary relation $\preceq$ partially orders the set of classes $\mathfrak{C}$. The pair $(\mathfrak{C}, \preceq)$ is called a partially ordered hierarchy. For any two classes C_i and C_j in $\mathfrak{C}$, the notation $C_j \preceq C_i$ means that the user in C_i can access the resource in C_j and the opposite is forbidden. It is easy to see that $C_i \preceq C_i$ for any $C_i \in \mathfrak{C}$. The partially ordered hierarchy $(\mathfrak{C}, \preceq)$ can be represented by a directional graph, where each class corresponds to a vertex in the graph and there exists an edge form class C_j to C_i if and only if $C_j \preceq C_i$. For the detailed descriptions about partially ordered hierarchy, readers can refer to [2,17].

2.2 Bilinear Pairings and Its Security Assumptions

Let G_1 and G_2 be two groups with a same large prime order q, where G_1 is an additive cyclic group and G_2 is a multiplicative cyclic group. A bilinear pairing e is a map defined by $e : G_1 \times G_1 \rightarrow G_2$ which satisfies the following three properties:

1. Bilinear: For all P, $Q \in G_1$, a, $b \in \mathbb{Z}_q^*$, we have $e(aP, bQ) = e(P, Q)^{ab}$.
2. Non-degenerate: For all $P \in G_1$, there exists $Q \in G_1$ such that $e(P, Q) = 1_{G_2}$.
3. Computable: For all $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

The detailed descriptions for bilinear pairings can be referred to [4,22,23].

2.3 Integer Factorization Problem and RSA Cryptosystem

As we all known, given two large prime number p and q to compute $n = p \times q$ is easy. However, given a value n to find p and q is intractable. It is well-known the integer factorization problem.

The security of RSA cryptosystem is based on the difficulty of integer factorization problem. In this cryptosystem, the two large primes p and q are selected firstly and then the two values $n = p \times q$ and $\phi(n) = (p - 1) \cdot (q - 1)$ can be computed. Then, a public value e is selected which satisfies $\gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$. According to e, a secret value d can be chosen which satisfies $e \cdot d \equiv 1 \bmod \phi(n)$. Note that given two values n and e, an adversary without p and q is unable to compute the secret value d. The detailed descriptions for the integer factorization problem and the RSA Cryptosystem can be referred to [12,15].

3 A Concrete Scheme

In this section, we propose a concrete time-bound hierarchical key assignment scheme for secure data access control. The proposed scheme combines the pairing-based public key system with the RSA cryptographic method and is suitable for subscribers in discrete time intervals. In our scheme, we assume that each user can access some resources in some discrete time interval T_i such as one weak, one month, etc.. These resources are stored in a set of classes $\mathfrak{C}$. Without loss of generality, the maximal system life time is defined as $T = \{1, 2, \ldots, z\}$, ie. $T_i \subset T$ and there are n classes, $\mathfrak{C} = \{C_1, C_2, \ldots, C_n\}$. Note that the n classes form a directional graph with the relation $\preceq$ mentioned in Subsection 2.1. The proposed scheme consists of following four phases: *System setup*, *User subscribing*, *Encryption key generation*, and *Decryption key derivation* phases.

System setup phase: Firstly, the system vender (SV) constructs a set of classes $\mathfrak{C}$ and deploys the resources into n classes. In other words, a directional graph $(\mathfrak{C}, \preceq)$ is produced. Then, the SV generates the needed keys and parameters as follows. The SV selects a bilinear pairing $e : G_1 \times G_1 \to G_2$ mentioned in Subsection 2.2. A generator $P \in G_1$ is generated and then a public value $P_{pub} = s \cdot P$ is computed, where $s \in \mathbb{Z}_q^*$ is a secret value kept by the SV. Meanwhile, the system vender selects two prime numbers p_1, q_1 and computes $n = p_1 \times q_1$ and $\phi(n) = (p_1 - 1) \cdot (q_1 - 1)$. Then, the SV determines two RSA key pairs (e_i, d_i) and (g_t, h_t) such that $e_i \cdot d_i \equiv 1 \bmod \phi(n)$ and $g_t \cdot h_t \equiv 1 \bmod \phi(n)$ for $i = 1, 2, \ldots, n$ and $t = 1, 2, \ldots, z$, where d_i and h_t are kept secret. Finally, the SV defines a cryptographic hash function $H : \{0, 1\}^* \to \mathbb{Z}_q^*$ and publishes the public parameters $\{e, G_1, G_2, q, P, P_{pub}, n, e_1, \ldots, e_n, g_1, \ldots, g_s, H\}$.

User subscribing phase: When a user subscribes class C_i to access some resource in some time period $T_i \subset T = \{1, 2, \ldots, z\}$, the system vender computes a key pair $(\alpha = a \prod_{C_k \preceq C_i} d_k P, \beta = e(P, P)^{\prod_{y \in T_i} h_y})$, where $a \in \mathbb{Z}_q^*$ is a secret value kept by the SV. Finally, (α, β) is sent to user via a secure channel.

Encryption key generation phase: For each time $t \in T = \{1, 2, \ldots, z\}$, the system vender computes a encryption key $K_{i,t} = H(k_i || k_t)$ to protect the resource in class C_i, where

$$k_i = e(\prod_{C_k \preceq C_i} d_k P, P_{pub})^a = e(P, P)^{\prod_{C_k \preceq C_i} s a d_k} \text{ and } k_t = e(P, P)^{h_t}.$$

Note that we can use the symmetric encryption algorithm such as AES with the key $K_{i,t}$ to encrypt the resource in class C_i for time period t.

Decryption key derivation phase: For any user who is in class C_i with her/his subscribing time period T_i, she/he can compute the decryption key $K_{j,t} = H(k_j || k_t)$ of class C_j if and only if $C_j \preceq C_i$ and $t \in T_i$. The key derivation is shown as follows:

$$k_j = e(\alpha, P_{pub})^{\prod_{C_k \preceq C_i, C_k \not\preceq C_j} e_k} = e(a \prod_{C_k \preceq C_i} d_k P, s \cdot P)^{\prod_{C_k \preceq C_i, C_k \not\preceq C_j} e_k}$$
$$= e(P, P)^{\prod_{C_k \preceq C_j} s a d_k}$$

and

$$k_t = (\beta)^{\prod_{y \in T_i, y \neq t} g_y} = e(P, P)^{h_t}.$$

4 Security Analysis

In this section, we demonstrate the security of our proposed scheme. It is easy to see that the security of our scheme is based on the computation of both k_i and k_t because the encryption key $K_{i,t} = H(k_i || k_t)$. In the following Lemmas 1 and 2, we will demonstrate the security of k_i and k_t, respectively.

Lemma 1. *Under the security of the RSA cryptosystem, the value k_i for $i \in \{1, 2, \ldots, n\}$ of the proposed scheme is secure against outside and inside attacks.*

Proof. Here, the security proof of Lemma 1 is divided into following three parts.

Part 1. *Any outside attacker cannot compute the value k_i.* An outside attacker only knows the public values $e_1, e_2, \ldots, e_n$, and P_{pub}. Since the value $k_i = e(\prod_{C_k \preceq C_i} d_k P, P_{pub})^a$ is generated by the secret values $d_1, d_2, \ldots, d_n$, and a, she/he has no way to know them. In other aspect, the security of d_k relies on the security of the RSA cryptosystem. The pair (e_i, d_i) is a pubic/private key pair and nobody can derive d_i from e_i.

Part 2. *Any legal user with the value k_j still cannot derive the value k_i for the two cases: (1) $C_j \preceq C_i$ and (2) $C_j \not\preceq C_i$.* For the case 1, the key point is how to find d_i such that $k_i = (k_j)^{d_i}$. However, it is impossible by the same reason mentioned in Part 1. Similarly, to find d_i such that $k_i = (k_j)^{e_j \cdot d_i}$ is also impossible for the case 2.

Part 3. *The value k_i is secure against colluding attacks.* Without loss of generality, assume that two legal users with the two values k_j and k_l and they want to derive the value k_i for the two cases: (1) $C_l \preceq C_j \preceq C_i$ and (2) $C_l \preceq C_i$ and $C_j \preceq C_i$. For the case 1, to compute k_i they must find d_i or d_j such that $k_i = (k_j)^{d_i} = (k_l)^{d_i \cdot d_j}$. However, it is impossible by the same reason mentioned in Part 1. Similarly, it is also impossible for the case 2.

Lemma 2. *Under the security of the RSA cryptosystem, the value k_t for $i \in \{1, 2, \ldots, s\}$ of the proposed scheme is secure against outside and inside attacks.*

Proof. By the similar approach in Lemma 1, we can prove (a) *any outside attacker cannot compute the value k_t*, (b) *any legal user with the value k_{t_1} still cannot derive the value k_{t_2} for $t_1 \neq t_2$*, and (c) *the value k_t is secure against colluding attacks.*

Based on the above two lemmas, the following theorem demonstrate the proposed scheme is a secure time-bound hierarchical key assignment scheme.

Theorem 1. *Under the security of the RSA cryptosystem and the security of hash function, any outside and inside attackers cannot compute the encryption key* $K_{i,t} = H(k_i||k_t)$.

Proof. By Lemmas 1 and 2, we have proven that k_i and k_t are secure against outside and inside attacks. If the outside and inside attackers can obtain a value $v = k_i||k_t$ such that $K_{i,t} = H(v)$, it is a contradiction for the security property "collusion resistance" of the hash function H.

5 Performance Analysis and Comparisons

For convenience to evaluate the performance of our scheme, we define the following notations:

- TG_e: The time of executing a bilinear pairing operation, $e : G_1 \times G_1 \to G_2$.
- TG_{mul}: The time of executing a scalar multiplication operation of point in G_1.
- T_{exp}: The time of executing a modular exponentiation operation.
- T_{mul}: The time of executing a modular multiplication operation.
- T_H: The time of executing a one-way hash function H.
- T_{syme}: The time of executing a symmetric encryption algorithm.
- d: The path length between the subscribing class and its lower level classes.
- l: The number of subscribing time interval.

In the user subscribing phase, $TG_e + TG_{mul} + T_{exp} + (d+1)T_{mul}$ is required to compute (α, β). In the encryption key generation phase, it requires $TG_e + TG_{mul} + 2T_{exp} + dT_{mul} + T_H$ to compute $K_{i,t} = H(k_i||k_t)$. In the decryption key derivative phase, $TG_e + 2T_{exp} + (d + l - 2)T_{mul}$ is required to derive $K_{i,t} = H(k_i||k_t)$.

Table 1. Comparisons between our scheme and the recent proposed time-bound hierarchical key assignment schemes

	Chen et al.'s scheme [7]	Yeh's scheme [25]	Our scheme
Key construction	Pairing-based	RSA	Pairing-based + RSA
Type of time interval	Continuous	Discrete	Discrete
User subscribing	TG_{mul} $+2T_{exp} + 2T_{mul}$	$2T_{exp}$ $+(d+l-1)T_{mul}$	$TG_e + TG_{mul}$ $+T_{exp} + (d+1)T_{mul}$
Encryption key generation	$TG_e + 3T_{exp}$ $+2T_{mul} + T_{syme}$	$2T_{exp} + dT_{mul}$	$TG_e + TG_{mul}$ $+2T_{exp} + dT_{mul} + T_H$
Decryption key derivative	$TG_e + T_{syme}$	$2T_{exp}$ $+(d+l-2)T_{mul}$	$TG_e + 2T_{exp}$ $+(d+l-2)T_{mul}$
Security	Provably secure	Existing attack [2]	Provably secure

Then, we compare the recent presented time-bound hierarchical key assignment schemes [7,25] in terms of key construction, performance, and security properties. The results are summarized in Table 1. We can see that Yeh's scheme [25] is based on the RSA key construction, Chen et al.'s scheme [7] is based on the pairing-based key construction, and our scheme fuses the pairing-based and the RSA key constructions. In other aspect, Chen et al.'s scheme focuses on continuous time interval. Our scheme and Yeh's scheme are suitable for discrete time interval. Though Yeh's scheme is efficient, it suffered from colluding attack mentioned in [2]. Our scheme and Chen et al.'s scheme are provably secure.

6 Conclusions

In this paper, we have proposed a time-bound hierarchical key assignment scheme. Our scheme fuse pairing-based cryptography and RSA key construction and is suitable for discrete time interval. The security analysis is demonstrated that our scheme is secure against and outsider and insider attacks (including colluding attacks). In the future, we will extend our scheme to the cloud environments.

Acknowledgments. This work is supported by Shenzhen Peacock Project of China (No. KQC201109020055A), Shenzhen Strategic Emerging Industries Program of China (No. ZDSY20120613125016389 and No. JCYJ20120613151032592), and National Natural Science Foundation of China (No. 61100192).

References

1. Akl, S.G., Taylor, P.D.: Cryptographic solution to a problem of access control in a hierarchy. ACM Transactions on Computer Systems (TOCS) 1(3), 239–248 (1983)
2. Ateniese, G., De Santis, A., Ferrara, A.L., Masucci, B.: Provably-secure time-bound hierarchical key assignment schemes. Journal of Cryptology 25(2), 243–270 (2012)
3. Blanton, M., Fazio, N., Frikken, K.B.: Dynamic and efficient key management for access hierarchies. In: Proceedings of the ACM Conference on Computer and Communications Security (2005)
4. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. SIAM Journal on Computing 32(3), 586–615 (2003)
5. Chen, C.M., Lin, Y.H., Lin, Y.C., Sun, H.M.: Rcda: recoverable concealed data aggregation for data integrity in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems 23(4), 727–734 (2012)
6. Chen, C.M., Wang, K.H., Wu, T.Y., Pan, J.S., Sun, H.M.: A scalable transitive human-verifiable authentication protocol for mobile devices. IEEE Transactions on Information Forensics and Security 8(8), 1318–1330 (2013)
7. Chen, C.M., Wu, T.Y., He, B.Z., Sun, H.M.: An efficient time-bound hierarchical key management scheme without tamper-resistant devices. In: 2012 International Conference on Computing, Measurement, Control and Sensor Network (CMCSN). pp. 285–288. IEEE (2012)
8. Chen, Y.-R., Chu, C.-K., Tzeng, W.-G., Zhou, J.: CloudHKA: A cryptographic approach for hierarchical access control in cloud computing. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 37–52. Springer, Heidelberg (2013)

9. Chien, H.Y.: Efficient time-bound hierarchical key assignment scheme. IEEE Transactions on Knowledge and Data Engineering 16(10), 1301–1304 (2004)
10. Jiang, T., Zheng, S., Liu, B.: Key distribution based on hierarchical access control for conditional access system in dtv broadcast. IEEE Transactions on Consumer Electronics 50(1), 225–230 (2004)
11. Kayem, A.V., Martin, P., Akl, S.G.: Heuristics for improving cryptographic key assignment in a hierarchy. In: 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW 2007, vol. 1, pp. 531–536. IEEE (2007)
12. Lenstra, A.K.: Integer factoring. Designs, Codes and Cryptography 19, 101–128 (2000)
13. Lin, C.W., Hong, T.P., Chang, C.C., Wang, S.L.: A greedy-based approach for hiding sensitive itemsets by transaction insertion. Journal of Information Hiding and Multimedia Signal Processing 4(4), 201–227 (2013)
14. Lin, C.W., Hong, T.P., Hsu, H.C.: Reducing side effects of hiding sensitive itemsets in privacy preserving data mining. The Scientific World Journal 2014, Article ID 235837, 12 pages (2014)
15. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. CRC Press (2010)
16. Naor, D., Naor, M., Lotspiech, J.: Revocation and tracing schemes for stateless receivers. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 41–62. Springer, Heidelberg (2001)
17. Sandhu, R.S., Samarati, P.: Access control: principle and practice. IEEE Communications Magazine 32(9), 40–48 (1994)
18. Sui, Y., Maino, F., Guo, Y., Wang, K., Zou, X.: An efficient time-bound access control scheme for dynamic access hierarchy. In: 5th International Conference on Mobile Ad-hoc and Sensor Networks, MSN 2009, pp. 279–286. IEEE (2009)
19. Tseng, Y.M., Yu, C.H., Wu, T.Y.: Towards scalable key management for secure multicast communication. Information Technology and Control 41(2), 173–182 (2012)
20. Tzeng, W.G.: A time-bound cryptographic key assignment scheme for access control in a hierarchy. IEEE Transactions on Knowledge and Data Engineering 14(1), 182–188 (2002)
21. Wang, S.Y., Laih, C.S.: Merging: an efficient solution for a time-bound hierarchical key assignment scheme. IEEE Transactions on Dependable and Secure Computing 3(1), 91–100 (2006)
22. Wu, T.Y., Tsai, T.T., Tseng, Y.M.: A revocable id-based signcryption scheme. Journal of Information Hiding and Multimedia Signal Processing 3(3), 240–251 (2012)
23. Wu, T.Y., Tseng, Y.M.: An id-based mutual authentication and key exchange protocol for low-power mobile devices. The Computer Journal 53(7), 1062–1070 (2010)
24. Wu, T.-Y., Zhou, C., Wang, E.K., Pan, J.-S., Chen, C.-M.: Towards time-bound hierarchical key management in cloud computing. In: Pan, J.-S., Snasel, V., Corchado, E.S., Abraham, A., Wang, S.-L. (eds.) Intelligent Data Analysis and Its Applications, Volume I. AISC, vol. 297, pp. 31–38. Springer, Heidelberg (2014)
25. Yeh, J.H.: A secure time-bound hierarchical key assignment scheme based on rsa public key cryptosystem. Information Processing Letters 105(4), 117–120 (2008)
26. Yi, X.: Security of chien's efficient time-bound hierarchical key assignment scheme. IEEE Transactions on Knowledge and Data Engineering 17(9), 1298–1299 (2005)
27. Yi, X., Ye, Y.: Security of tzeng's time-bound key assignment scheme for access control in a hierarchy. IEEE Transactions on Knowledge and Data Engineering 15(4), 1054–1055 (2003)