Public Key Timed-Release Attribute-Based Encryption

Ke Yuan[1], Nan Shen[2], Yonghang Yan[1(✉)], Zheli Liu[2], and Chufu Jia[2]

[1] School of Computer and Information Engineering,
Henan University, Kaifeng 475004, China
yanyonghang@henu.edu.cn
[2] College of Computer and Control Engineering,
Nankai University, Tianjin 300071, China

Abstract. This paper introduces and explores a new concept of public key timed-release attribute-based encryption (PKTRABE) which can be used to solve the time-dependent ABE problem. In our PKTRABE model, the sender encrypts a message so that only the intended receivers who own some specified attributes can decrypt it after a specified time in the future. We begin by explaining what is PKTRABE. Then, we formalize the notion of basic PKTRABE and its security game model. Finally, we give two concrete schemes which are secure under the BDH and DBDH assumption in the random oracle model. Conclusions and future work are also summarized.

Keywords: Timed-release · Attribute-based encryption · Time trapdoor · Bilinear map

1 Introduction

Attribute-based encryption (ABE) is a new type of identity-based encryption (IBE) where identity is viewed as a set of descriptive attributes. In ABE, a user's public key and ciphertexts are labeled with sets of descriptive attributes and a particular private key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the target user's public key. Further more, the target receiving entity of ABE cryptosystem is a user group whose each member's exact identity needn't to be known by the sender, rather than a single user. Along with the development of research, the ABE scheme can provide more and more powerful methods to achieve both multi-receiver data security and fine-grained access control. Time has always played an important role in time-sensitive practical applications, but the research work of time-relevant ABE has not been carried out so far. The property of time here means to encrypt a message such that the receiver cannot decrypt the ciphertext until a specific time in the future. This is called timed-release encryption (TRE). For solving the problem of time-relevant ABE, we propose a new concept of public key timed-release attribute-based encryption which is abbreviated as PKTRABE. PKTRABE is

W. Niu et al. (Eds.): ATIS 2015, CCIS 557, pp. 65–73, 2015.
DOI: 10.1007/978-3-662-48683-2_7

a combination of TRE and ABE. In our PKTRABE cryptosystem, the sender uses a user group's attributes set to encrypt a message with a release time so that only the intended member can decrypt the target ciphertext after a pre-set release time in the future.

1.1 Our Contributions

The contribution of this paper is to solve the time-dependent ABE problem by combining the existing cryptographic mechanism TRE and basic ABE. Firstly, we formalizes the notion of PKTRABE and its security game model. Secondly, we proposes two provably secure constructions of PKTRABE which are secure under the BDH and DBDH assumption in the random oracle model. The former focuses on the single time server scenarios while the latter pays attention to the multiple time servers scenarios.

1.2 Related Work

We give a brief overview of the TRE and the ABE as follows:

TRE allows a sender to encrypt a message so that only the intended receiver can decrypt it only after a pre-set time. The problem of TRE was first advocated by May [11] in 1993 and demonstrated in detail by Rivest et al. [12] in 1996. And since then, extraordinary progress has been made in its theory and practice. In theoretical aspect, some new concepts of TRE was proposed in succession. The first attempt at scalable, server-passive, user-anonymous TRE was due to Chan and Blake [4] and the first try at TRE with pre-open capability was due to Hwang et al. [8] in 2005. Afterwards, Cheon et al. [6] formalize the concept of a secure public key TRE in 2008. More recently, Unruh [14] proposed revocable quantum TRE in 2014. In practical aspect, TRE has been utilized in oblivious transfer [10] and searchable encryption [15].

ABE allows users to encrypt and decrypt messages based on user attributes. The cryptology mechanism of ABE was first proposed by Sahai and Waters [13] in 2005. This original ABE is less efficient and cannot provide fine-grained access control. To solve these problems, many revisions and extensions have been given. Baek et al. [1] gives two more efficient ABE schemes in 2007. Goyal et al. [7] proposed key-policy ABE in 2006. Bethencourt et al. [2] proposed ciphertext-policy ABE and Chase [5] proposed multi-authority ABE in 2007. More recently, Li et al. [9] introduced secure outsourcing techniques into ABE in 2013.

1.3 Organization

We begin by explaining what is PKTRABE. In Sect. 2 we review our security assumptions. In Sect. 3 We formalize the notion of PKTRABE and its security game model. In Sects. 4 and 5 we provide two concrete construction schemes for PKTRABE respectively. Finally, we conclude in Sect. 6.

2 Preliminaries

Below, we briefly review the definitions of bilinear map and discuss the complexity assumption on which the security of our schemes are based.

2.1 Bilinear Maps

Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two multiplicative cyclic groups of order p for some large prime p. A bilinear map is a map $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ satisfies the following properties:

- Computable: There is an efficient algorithm to compute $e(g, h) \in \mathcal{G}_2$ for any $g, h \in \mathcal{G}_1$.
- Bilinear: For any integers $a, b \in \mathbb{Z}_p^*$ we have $e(g^a, h^b) = e(g, h)^{ab}$.
- Non-degenerate: If g is a generator of $\mathcal{G}_1$ then $e(g, g)$ is a generator of $\mathcal{G}_2$.

2.2 Complexity Assumptions

The BDH problem [3] in $\mathcal{G}_1$ is as follows: given a tuple $g, g^a, g^b, g^c \in \mathcal{G}_1$ as input, output $e(g, g)^{abc} \in \mathcal{G}_2$. An attacker $\mathcal{A}$ has advantage ϵ in solving BDH in $\mathcal{G}_1$ if

$$\Pr[\mathcal{A}(g, g^a, g^b, g^c) = e(g, g)^{abc}] \geq \epsilon$$

where the probability is over the random choice of generator $g \in \mathcal{G}_1^*$, the random choice of $a, b, c \in \mathbb{Z}_p^*$, and the random bits used by $\mathcal{A}$.

Similarly, we say that an challenger $\mathcal{B}$ that has advantage ϵ in solving the Decisional BDH (DBDH) problem in $\mathcal{G}_1$ if

$$\begin{aligned} &|\Pr[\mathcal{B}(g, g^a, g^b, g^{c,e}(g, g)^{abc}) = 0] \\ &-\Pr[\mathcal{B}(g, g^a, g^b, g^c, \mathcal{T}) = 0]| \geq \epsilon \end{aligned}$$

where the probability is over the random choice of generator $g \in \mathcal{G}_1^*$, the random choice of $a, b, c \in \mathbb{Z}_p^*$, the random choice of $\mathcal{T} \in \mathcal{G}_1$, and the random bits consumed by $\mathcal{B}$.

Definition 1. *We say that (Decisional) (t, ϵ)-BDH assumption holds in $\mathcal{G}_1$ if no t-time algorithm has advantage at least ϵ in solving the (Decisional) BDH problem in $\mathcal{G}_1$.*

Occasionally we drop the t and ϵ and refer to the BDH and DBDH assumptions in $\mathcal{G}_1$.

3 PKTRABE: Definitions

Suppose Bob as a professor needs to arrangement an online exam in next Monday for all students of the Computer Science Department of Computer College of Henan University, but unfortunately, he has to go to an important meeting

from next Monday to next Wednesday. In such case, Bob can adopt PKTRABE mechanism to solve his problem. Bob sends the following message in advance:

$$[Enc(ID', ts_{pub}, r, M, T), T)$$

where $ID' = (\text{“}Computer\ Science\ Department\text{”}, \text{“}Computer\ College\text{”}, \text{“}Henan\ University\text{”})$ is the target user group's common identity attributes set, ts_{pub} is the public key of the time server, r is a random fresh factor, M is the test questions, T is the release time. All the intended students can get the ciphertext in advance and decrypt it after the pre-set release time in the future. We call such a system non-interactive PKTRABE.

Definition 2. *A non-interactive basic PKTRABE scheme with single time server consists of the following polynomial time randomized algorithms:*

Setup. Takes a security parameter, and generates master key mk and public parameters $params$ which contains an error tolerance parameter d.

TRSetup. Generates public/private key (ts_{pub}, ts_{priv}) of the time server.

KeyGen. Given the master key mk and an identity ID as input, generates a private key associated with ID, denoted by D_{ID}.

Enc. For public key ID', ts_{pub}, a release time T and a plaintext M, produces a ciphertext (C, T).

RtTrd. Given the time server's private key ts_{priv} and a release time T, produces a time trapdoor S_T.

Dec. Given the private key D_{ID}, the time trapdoors S_T and the ciphertext (C, T) encrypted with an identity ID' such that $ID \bigcap ID' \geq d$, generates the plaintext M or a “Reject” message.

Formally, we define security against an active attacker using the simulation game between a challenger $\mathcal{B}$ and the attacker $\mathcal{A}$ as follows:

Initialization. The adversary $\mathcal{A}$ outputs an identity ID^* and a release time T^* where it wishes to be challenged.

Setup. The challenger $\mathcal{B}$ generates the public parameters $params$ and ts_{pub}, sends them to $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ issues queries $q_1, q_2, \ldots, q_m$ where query q_i is one of:

1. Private key query (ID_i) where $ID_i \bigcap ID^* < d$. $\mathcal{B}$ responds by running algorithm $KeyGen$ to generate the private key D_{ID_i} corresponding to the identity ID_i. $\mathcal{B}$ sends D_{ID_i} to $\mathcal{A}$.
2. Time trapdoor query (T_i) where $T_i \neq T^*$. $\mathcal{B}$ responds by running algorithm $RtTrd$ to generate the time trapdoor S_{T_i} corresponding to the release time T_i. $\mathcal{B}$ sends S_{T_i} to $\mathcal{A}$.

3. Decryption query (C_i, T_i) for identity ID^* and release time T^*. $\mathcal{B}$ runs algorithm *Dec* to decrypt the ciphertext (C_i, T_i) using the private key D_{ID_i} and time trapdoor S_{T_i}. $\mathcal{B}$ sends the plaintext M to $\mathcal{A}$.

These queries may be asked adaptively; that is, each query q_i may depend on the replies to $q_1, q_2, \ldots, q_{i-1}$.

Challenge: $\mathcal{A}$ outputs two equal length plaintexts $M_0, M_1 \in \mathcal{G}_2$ on which it wishes to be challenged. $\mathcal{B}$ picks a random bit $b \in \{0,1\}$ and sets the challenge ciphertext to $(C^*, T^*) = Enc(ID^*, ts_{pub}, r, M, T^*)$. $\mathcal{B}$ sends (C^*, T^*) as the challenge to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ issues additional queries $q_{m+1}, \ldots, q_{num}$ and $\mathcal{B}$ responds as in Phase 1.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$. $\mathcal{A}$ wins if $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-sID-T-CCA adversary. We define the advantage of the adversary $\mathcal{A}$ in attacking the scheme $\mathcal{E}$ as

$$Adv_{\mathcal{E},\mathcal{A}}^{CCA} = |P_r[b = b'] - \frac{1}{2}|$$

The probability is over the random bits used by the challenger $\mathcal{B}$ and the adversary $\mathcal{A}$.

Definition 3. *We say that a PKTRABE scheme $\mathcal{E}$ is $(t, q_{ID}, q_T, q_C, \epsilon)$-selective identity and release time, adaptive chosen ciphertext secure if for any t-time IND-sID-T-CCA adversary $\mathcal{A}$ that makes at most q_{ID} chosen private key queries, q_T chosen release time queries and q_C chosen decryption queries we have that $Adv_{\mathcal{E},\mathcal{A}}^{CCA} < \epsilon$. As shorthand, we say that $\mathcal{E}$ is $(t, q_{ID}, q_T, q_C, \epsilon)$ IND-sID-T-CCA secure.*

Semantic Security. As usual, we define selective identity and release time, chosen plaintext security for a PKTRABE system as in the preceding game, except that the adversary is not allowed to issue any decryption queries.

Definition 4. *We say that a PKTRABE scheme $\mathcal{E}$ is $(t, q_{ID}, q_T, \epsilon)$-selective identity and release time, adaptive chosen plaintext secure if $\mathcal{E}$ is $(t, q_{ID}, q_T, 0, \epsilon)$-selective identity and release time, chosen ciphertext secure. As shorthand, we say that $\mathcal{E}$ is $(t, q_{ID}, q_T, \epsilon)$ IND-sID-T-CPA secure.*

Similarly, we can formolize the notion of PKTRABE with multiple time servers and its security model.

4 Construction 1: Single Time Server

In this subsection, we propose our concrete single time server PKTRABE scheme and give the security assertion of our scheme.

4.1 Description of the Scheme

We build a non-interactive PKTRABE scheme from such a bilinear map defined above. The construction is based on [1]. Our PKTRABE scheme with random oracle works as follows:

Setup. Given security parameter $k \in \mathbb{Z}^+$, the following steps are taken.

1. Take k and generate a prime p. Let $(\mathcal{G}_1, \mathcal{G}_2)$ be a multiplicative group with prime order p, $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ be an admissible bilinear map and $g \in \mathcal{G}_1$ be a arbitrary generator.
2. Choose $g_1 \in_R \mathcal{G}_1$. Pick $y \in_R \mathbb{Z}_p^*$ and compute $g_2 = g^y$.
3. The following cryptographic hash function is chosen: $H : \{0,1\}^* \rightarrow \mathcal{G}_1$.
4. Select a tolerance parameter d.
5. Define the Lagrange coefficient $\triangle_{a,S(x)}$ for $a \in \mathbb{Z}_p^*$ and a set S of elements in $\mathbb{Z}_p^*$:

$$\triangle_{a,S(x)} = \prod_{a \in S, a \neq b} \frac{x-b}{a-b}$$

6. Output a public parameter $params = (p, \mathcal{G}_1, \mathcal{G}_2, g, g_1, g_2, e, d, H)$ and a private master key $mk = y$.

TRSetup. Choose $s \in_R \mathbb{Z}_p^*$ as the private key ts_{priv} and set g^s as the public key ts_{pub} of the time server.

KeyGen. To generate a private key for identity $ID = (\mu_1, \mu_2, \ldots, \mu_n)$ where $\mu_i \in \mathbb{Z}_p^*$ the following steps are taken.

1. Pick a random lagrange interpolation polynomial $f(\cdot)$ of degree $d-1$ over $\mathbb{Z}_p$ such that $f(0) = y$.
2. Compute $D_{\mu_i} = (\gamma_{\mu_i}, \delta_{\mu_i}) = ((H(\mu_i)^{f(\mu_i)}, g^{f(\mu_i)})$ for $i = 1, 2, \ldots, n$.
3. Output a private key $D_{ID} = (D_{\mu_1}, D_{\mu_2}, \ldots, D_{\mu_n})$.

Enc. To encrypt a message $M \in \mathcal{G}_2$ under identity $ID' = (\mu_1', \mu_2', \ldots, \mu_n')$, pick $r \in_R \mathbb{Z}_p^*$ and output the ciphertext $(C, T) = (c_1, c_2, c_{31}, c_{32}, \ldots, c_{3n}, c_4, T)$ where $c_1 = ID'$, $c_2 = g^r$, $c_{3i} = (g_1 H(\mu_i'))^r (i = 1, 2, \ldots, n)$, $c_4 = e(g_1, g_2)^r C_T$ and $C_T = e(ts_{pub}, H(T)^r)M$.

RtTrd. Output the time trapdoor $S_T = H(T)^s \in \mathcal{G}_1$.

Dec. To decrypt a ciphertext (C, T) using an arbitrary $S \subseteq ID \bigcap ID'$ such that $\mid S \mid = d$ and compute

$$C_T = \frac{e(\prod_{\mu_i \in S} \gamma_{\mu_i}^{\triangle_{\mu_i,S(0)}}, c_2)}{\prod_{\mu_i \in S} e(c_{3i}, \delta_{\mu_i}^{\triangle_{\mu_i,S(0)}})} \cdot c_4$$

$$M = \frac{C_T}{e(c_2, S_T)}$$

4.2 Security of the Scheme

The single time server scheme above is a non-interactive PKTRABE scheme semantically secure against a chosen plaintext attack in the random oracle model.

Theorem 1. *If an adversary $\mathcal{A}$ has advantage ϵ in breaking the PKTRABE scheme above, then an challenger $\mathcal{B}$ can be constructed to solve the BDH problem with probability at least $\epsilon' = \epsilon^2/e$ where e is the base of the natural logarithm.*

We will give the rigorous proof in the full version of this paper.

5 Construction 2: Multiple Time Servers

In this subsection, we propose our concrete multiple time servers PKTRABE scheme and give the security assertion of our scheme.

5.1 Description of the Scheme

We build a non-interactive PKTRABE scheme from such a bilinear map defined above. The construction is based on [1]. Our PKTRABE scheme with random oracle works as follows:

Setup. Given security parameter $k \in \mathbb{Z}^+$, the following steps are taken.

1. Take k and generate a prime p. Let $(\mathcal{G}_1, \mathcal{G}_2)$ be a multiplicative group with prime order p, $e : \mathcal{G}_1 \times \mathcal{G}_1 \to \mathcal{G}_2$ be an admissible bilinear map and $g \in \mathcal{G}_1$ be a arbitrary generator.
2. Choose $g_1 \in_R \mathcal{G}_1$. Pick $y \in_R \mathbb{Z}_p^*$ and compute $g_2 = g^y$.
3. The following cryptographic hash function is chosen: $H : \{0,1\}^* \to \mathcal{G}_1$.
4. Select a tolerance parameter d.
5. Define the Lagrange coefficient $\triangle_{a,S(x)}$ for $a \in \mathbb{Z}_p^*$ and a set S of elements in $\mathbb{Z}_p^*$:

$$\triangle_{a,S(x)} = \prod_{a \in S, a \neq b} \frac{x-b}{a-b}$$

6. Output a public parameter $params = (p, \mathcal{G}_1, \mathcal{G}_2, g, g_1, g_2, e, d, H)$ and a private master key $mk = y$.

TRSetup. Choose $s_i \in_R \mathbb{Z}_p^*$ as the private key ts_{priv}^i and set g^{s_i} as the public key ts_{pub}^i of the ith time server where $i = 1, 2, \ldots, n$.

KeyGen. To generate a private key for identity $ID = (\mu_1, \mu_2, \ldots, \mu_n)$ where $\mu_i \in \mathbb{Z}_p^*$ the following steps are taken.

1. Pick a random lagrange interpolation polynomial $f(\cdot)$ of degree $d-1$ over $\mathbb{Z}_p$ such that $f(0) = y$.

2. Compute $D_{\mu_i} = (\gamma_{\mu_i}, \delta_{\mu_i}) = ((H(\mu_i)^{f(\mu_i)}, g^{f(\mu_i)})$ for $i = 1, 2, \ldots, n$.

3. Output a private key $D_{ID} = (D_{\mu_1}, D_{\mu_2}, \ldots, D_{\mu_n})$.

Enc. To encrypt a message $M \in \mathcal{G}_2$ under identity $ID' = (\mu'_1, \mu'_2, \ldots, \mu'_n)$, pick $r \in_R \mathbb{Z}_p^*$ and output the ciphertext $(C, T) = (c_1, c_2, c_{31}, c_{32}, \ldots, c_{3n}, c_4, T)$ where $c_1 = ID'$, $c_2 = g^r$, $c_{3i} = e(ts^i_{pub}, H(T)^r) \cdot c'_{3i} (i = 1, 2, \ldots, n)$, $c_4 = e(g_1, g_2)^r M$ and $c'_{3i} = (g_1 H(\mu'_i))^r$.

RtTrd. Output the time trapdoor $S^i_T = H(T)^{s_i} \in \mathcal{G}_1$ where $i = 1, 2, \ldots, n$.

Dec. To decrypt a ciphertext (C, T) using an arbitrary $S \subseteq ID \bigcap ID'$ such that $| S | = d$ and compute

$$c'_{3i} = \frac{c_{3i}}{e(c_2, S^i_T)}$$

$$M = \frac{e(\prod_{\mu_i \in S} \gamma_{\mu_i}^{\Delta_{\mu_i, S(0)}}, c_2)}{\prod_{\mu_i \in S} e(c'_{3i}, \delta_{\mu_i}^{\Delta_{\mu_i, S(0)}})} \cdot c_4$$

5.2 Security of the Scheme

The multiple time servers scheme above is a non-interactive PKTRABE scheme semantically secure against a chosen plaintext attack in the random oracle model.

Theorem 2. *If an adversary $\mathcal{A}$ has advantage ϵ in breaking the PKTRABE scheme above, then an challenger $\mathcal{B}$ can be constructed to solve the BDH problem with probability at least $\epsilon' = \epsilon^{d+1}/e^d$ where e is the base of the natural logarithm.*

We will give the rigorous proof in the full version of this paper.

6 Conclusions and Future Work

We propose a new concept of PKTRABE which can be used to solve the time-dependent ABE problem. In our PKTRABE model, the sender encrypt a message so that it cannot be decrypted by anyone, including the designated receivers who have some attributes specified by the sender, until a future release time chosen by the sender. We formalize the notion of PKTRABE and its security model and propose two construction schemes of PKTRABE with single time server and multiple time servers respectively.

PKTRABE would have many practical applications. In this paper, we only research the basic PKTRABE. We will study such PKTRABE that can provide fine-grained access policy in our future work.

References

1. Baek, J., Susilo, W., Zhou, J.: New constructions of fuzzy identity-based encryption. In: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, pp. 368–370. ACM (2007)

2. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy. SP 2007, pp. 321–334. IEEE (2007)
3. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
4. Chan, A.F., Blake, I.F.: Scalable, server-passive, user-anonymous timed release cryptography. In: Proceedings. 25th IEEE International Conference on Distributed Computing Systems. ICDCS 2005, pp. 504–513. IEEE (2005)
5. Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007)
6. Cheon, J.H., Hopper, N., Kim, Y., Osipkov, I.: Provably secure timed-release public key encryption. ACM Trans. Inf. Syst. Secur. **11**(2), 1–44 (2008)
7. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98. ACM (2006)
8. Hwang, Y.-H., Yum, D.H., Lee, P.J.: Timed-release encryption with pre-open capability and its application to certified e-mail system. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 344–358. Springer, Heidelberg (2005)
9. Li, J., Chen, X., Li, J., Jia, C., Ma, J., Lou, W.: Fine-grained access control system based on outsourced attribute-based encryption. In: Crampton, J., Jajodia, S., Mayes, K. (eds.) ESORICS 2013. LNCS, vol. 8134, pp. 592–609. Springer, Heidelberg (2013)
10. Ma, X., Xu, L., Zhang, F.: Oblivious transfer with timed-release receivers privacy. J. Syst. Softw. **84**(3), 460–464 (2011)
11. May, T.: Timed-release crypto (Unpublished manuscript) (1993)
12. Rivest, R.L., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto. Technical report MIT/LCS/TR-684, MIT LCS Tech, Cambridge, MA (1996)
13. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
14. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 129–146. Springer, Heidelberg (2014)
15. Yuan, K., Liu, Z., Jia, C., Yang, J., Lv, S.: Public key timed-release searchable encryption in one-to-many scenarios. Acta Electronica Sinica **43**(4), 760–768 (2015)