Soft Comput
DOI 10.1007/s00500-016-2177-z

METHODOLOGIES AND APPLICATION

Adaptable key-policy attribute-based encryption with time interval

Siqi Ma[1] · **Junzuo Lai**[2] · **Robert H. Deng**[1] · **Xuhua Ding**[1]

Abstract In this paper, we introduce a new cryptographic primitive: adaptable KP-ABE with time interval (KP-TIABE), which is an extension of key-policy attribute-based encryption (KP-ABE). Adaptable KP-TIABE specifies a decryption time interval for every ciphertext such that the ciphertext can only be decrypted within this time interval. To be more flexible, the decryption time interval associated with a ciphertext can be adjusted on demand by a semi-trusted server. We propose a formal model for adaptable KP-TIABE, present a concrete adaptable KP-TIABE scheme and prove its security under the security model.

Keywords Adaptable key-policy attribute-based encryption · Time specific · Adaptability

1 Introduction

To provide data security and privacy in cloud storage, a common practice is using encryption. However, how to share encrypted data in a scalable and flexible manner has been a challenging problem. Attribute-based encryption (ABE) (Goyal et al. 2006; Waters 2011; Sahai and Waters 2005), which encrypts messages with respect to attributes or access policies defined over a set of attributes, is considered as a very promising solution to the above challenge. There are two types of ABE schemes: ciphertext-policy attribute-based encryption (CP-ABE) (Waters 2011) and key-policy attribute-based encryption (KP-ABE) (Goyal et al. 2006). In CP-ABE, a user's private key is associated with a set of attributes and a ciphertext is associated with an access policy over attributes. The ciphertext can be decrypted only if the user's attributes satisfy the access policy of the ciphertext. KP-ABE is the dual of CP-ABE in which a ciphertext is associated with a set of attributes and a user's private key is associated with an access policy over attributes. The user can decrypt the ciphertext if and only if the set of attributes in the ciphertext satisfies the access policy associated with the private key.

In many information processing systems, time is a critical consideration. For example, sensitive data related to a project may only be accessible to project members while the project is active, and the data should be made inaccessible before or after the project duration. The first attempt to design time-sensitive encryption is the time-release encryption (TRE) scheme by May (1993) in which a ciphertext can only be decrypted after a specific release time. Paterson and Quaglia (2010) introduced time-specific encryption (TSE) as a generalization of TRE. The basic idea of TSE is that each user has a time instant key, and he/she can decrypt ciphertexts as long as the time specified in time instant key falls in the time intervals associated with the ciphertexts.

In this paper, we introduce a new notion of ABE, called *Adaptable key-policy based encryption with time interval* (KP-TIABE), which simultaneously achieves properties of attribute-based and time-specific encryptions in an efficient manner. Adaptable KP-TIABE novelly combines KP-ABE (Goyal et al. 2006), adaptable CP-ABE (Lai et al. 2014) and TSE (Paterson and Quaglia 2010). In adaptable KP-TIABE, a ciphertext is not only associated with a set of descriptive attributes, but also a decryption time interval. A user has a private key associated with an access policy over attributes as in the standard KP-ABE, as well as time instant key as in

Communicated by V. Loia.

✉ Siqi Ma
siqi.ma.2013@phdissmu.edu.sg

[1] Singapore Management University, Singapore, Singapore

[2] Jinan University, Guangzhou, China

Published online: 16 June 2016

TSE. The user is enable to decrypt the ciphertext only if the set of attributes in the ciphertext satisfies the access policy and the time instant specified in the time instant key falls in the decryption time interval of the ciphertext. In adaptable KP-TIABE, a user receives a private key associated with an access policy from a *Key Generation Center*. A semi-trusted *Time Server* broadcasts a global system parameter and a time instant key (TIK) at each time interval to all users. To make the decryption time interval adjustable, another semi-trusted party, called *Adaptation Server*, is introduced in adaptable KP-TIABE. The adaptation server is able to convert a ciphertext under a certain decryption time interval into another ciphertext of the same plaintext under a different decryption time interval but without learning anything about the plaintext. We present a formal model for adaptable KP-TIABE, provide a concrete construction and prove its security under the security model.

1.1 Application of adaptable KP-TIABE

Below we present some examples of applications that are suitable for our algorithm. Cloud computing is a powerful platform for data sharing, and our scheme could be used to ensure the confidentiality of the outsourced data in cloud storage.

Cloud data with time constraints Cloud computing, which contains massive storage capacity, provides a convenient scenario for users to rent the cloud server and share their data. Since cloud could be used by everyone, the data owner may not want the cloud and other irrelevant people to get the data. The basic idea is that the data could be encrypted before outsourcing to ensure its confidentiality.

In practice, data accessing often obeys the fine-grained access control rules. For example, suppose that a company constitutes a confidential group for a confidential project. They need to rent a cloud server for data sharing among their internal group. Access control rules must make sure that only the researcher who belongs to this confidential group is allowed to access the data. Undoubtedly, KP-ABE is an appropriate method to achieve this type of cryptographic access control.

However, every confidential project has a deadline. After this deadline, all the related data in the cloud are not allowed to be accessed by anyone. This is not a rare phenomenon in the real world. Based on this phenomenon, defining a time interval (i.e., survival time) for the data is essential. This time interval could be the period that this project lasts. Within this period, researchers could decrypt the data with their private keys.

Adaptable KP-TIABE provides an effective solution for handling the task to restrict decryption time interval. Specifically, private key is generated by both policy server and time server, and it contains the access structure and the time point represented when user obtains the private key. While decrypting, each private key is not only associated with an access structure, which describes the specific types of ciphertext that the access structure satisfied, but also related to the time point that should correspond to the time interval.

Time constraints modification Considering the above scenario again, time interval modification is another phenomenon that may happen. For example, the project has to be finished earlier due to the funding limitation. Thus, we need to modify the decryption time interval. A straightforward method is to download the encrypted data from the cloud and decrypt it to extract the original data. Then, re-encrypt it with a new time interval and upload it again. Obviously, this is a redundant task if there are large amount of data involved.

Adaptable KP-TIABE re-encrypts data to the cloud efficiently. To maintain the data confidentiality against the cloud, data owner provides a new time interval to the time-modified server, which is given a trapdoor for modification. This re-encryption approach could also be applied on resource-constrained devices (e.g., mobile devices) that mobile devices are more popular nowadays, and it is much convenient to use our approach to operate data in cloud.

1.2 Organization

This paper is organized as follows. In Sect. 2, we provide an overview of related work. In Sect. 3, we highlight some standard notations and cryptographic definitions. In Sect. 4, we present our formal model for adaptable KP-TIABE and our concrete KP-TIABE scheme together with its security analysis. Finally, we conclude in Sect. 7.

2 Related work

Attribute-based encryption, time-specific encryption and proxy re-encryption are related to our work, which are briefly reviewed below.

2.1 Attribute-based encryption

The original concept of ABE was proposed by Sahai and Waters (2005), who presented a fuzzy identity-based encryption (IBE). Fuzzy IBE defines an identity as a set of attributes. A message is encrypted by a set of attributes ω, and a decryption key is generated by another set of attributes ω'; then a ciphertext can be decrypted if and only if $|\ \omega \cap \omega'\ | \geq d$, where d is a threshold value. Goyal et al. (2006) introduced two types of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). The difference lies in that in the former, a ciphertext is associated with a set of attributes, a decryption key is associated with an access policy (also called access structure), and decryption is successful only if

the set of attributes satisfies the access policy, while the latter is the other way around. In this paper, we focus on KP-ABE.

2.2 Time-specific encryption

The first notion of encryption scheme with time constraint was introduced by May (1993), called time-release crypto, where the goal is to encrypt a message that cannot be decrypted by anyone, not even the sender, until a predetermined release time is passed. Then, Rivest et al. (1996) proposed using time-lock puzzles to realize the notion of time-release crypto, but they pose heavy computational load on users. Blake and Chan (2004) constructed a time-release encryption scheme in which a trusted time server is completely passive—no interaction between it and the sender or receiver is needed, thus assuring the privacy of a message and the anonymity of both its sender and receiver.

Paterson and Quaglia (2010) generalized the notion of time-release crypto to time-specific encryption (TSE), which extends the time constraint from a time instant to a time interval $[t_L, t_R]$. Three types of TSE are presented in Paterson and Quaglia (2010): plain TSE, public-key TSE and identity-based TSE. The plain TSE is the basic form of TSE in which a message is encrypted by a decryption time interval and the ciphertext can only be decrypted if a user possesses a time interval key (TIK) which falls within the decryption time interval. The plain TSE is only related to the decryption time interval, instead of any specific user. In the public-key TSE, a message is encrypted by both a user's public key and a decryption time interval. Therefore, the user needs to decrypt the ciphertext using her corresponding private key and a time interval key which falls within the decryption time interval. The identity TSE is related to a user's identity in which a message is encrypted by a decryption time interval and the identity of the user. The user can extract the message using her private key associated with her identity and an appropriate time interval key. Note that both the public-key TSE and the identity-based TSE are one-to-one schemes; hence, they are not suitable for scalable access control of encrypted data in the cloud computing scenario. Recently, Kasamatsu et al. (2012) combined TSE with forward-secure encryption based on hierarchical IBE (Boneh et al. 2005) which decreases the size of both ciphertexts and public parameters.

2.3 Re-encryption

Proxy re-encryption (PRE) was first introduced by Blaze et al. (1998) that employs a semi-trusted proxy to convert ciphertexts encrypted using one key into ciphertexts encrypted using another key while without learning anything about the underlying plaintexts. However, the PRE in Blaze et al. (1998) is based on the symmetric proxy function. Later, Jakobsson (1999) proposed a more practical and efficient asymmetric PRE.

To further strengthen PRE, Weng et al. (2009) proposed the notion of conditional proxy re-encryption (CPRE) that defines a condition for a user's public key and certain properties for a re-encryption key. A ciphertext can be converted only if the properties satisfy the condition of the public key. Yet, this scheme is not secure enough since conditions are represented by keywords. Recently, Lai et al. (2014) introduced the notion of adaptable CP-ABE. The key idea of adaptable CP-ABE is the introduction of a new constraint called trapdoor. Using the trapdoor, a semi-trusted server converts a ciphertext with one access policy to another ciphertext with another access policy while without learning the underlying plaintext message.

The notion of KP-TIABE combines the key features of KP-ABE, TSE and adaptable CP-ABE, as will be described in detail in the rest of the paper.

2.4 Application of cryptographic technique

Cryptographic techniques are rapidly used in our daily life. They are applied to protect our communication, privacy and some important data, etc. Identity-based encryption (Mora Afonso and Carballero-Gil 2014) is used to protect users' communication data when they are using mobile phone to send e-mail or make payment. Moreover, a toolbox (Muñoz et al. 2013) is proposed to defend the attack on smart card. The toolbox controls digital oscilloscope which could trace the operation.

3 Preliminary

In this section, we provide the definitions of access structures, linear secret sharing schemes and bilinear groups.

3.1 Access structures

Definition 1 (*Access Structure* Beimel 1996) Let $P = \{P_1, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^P$ is monotone for $\forall B$ and C, if $B \in A$, $B \in C$, then $C \in \mathbb{A}$. An access structure(respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $P_1, \ldots, P_n$, i.e., $\mathbb{A} \subseteq 2^P \backslash \{\emptyset\}$. The sets in $\mathbb{A}$ are called authorized sets, and the sets not in $\mathbb{A}$ are called unauthorized set.

In this paper, we focus on the monotone access structure with sets of attributes, instead of parties.

3.2 Linear secret sharing schemes

We adopt the definition of linear secret sharing schemes from Beimel (1996).

Definition 2 (*Linear Secret Sharing Schemes (LSSS)*) Let $\mathbf{M}$ be a matrix with size of $\ell \times n$. A secret sharing scheme Π for an access structure $\mathbb{A}$ over a set of parties $\mathcal{P}$ is defined as a linear secret sharing scheme over $\mathbb{Z}_p$ if it satisfies the following:

1. The matrix $\mathbf{M}$ represents the share-generating matrix for Π. Let ρ be a function from $\{1, \ldots, \ell\}$ to $\mathcal{P}$, which labels each row of $\mathbf{M}$. When we consider the column vector $v = (s, r_2, \ldots, r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $r_2, \ldots, r_n \in \mathbb{Z}_P$ are chosen randomly, then $\mathbf{M}v$ is the vector of ℓ shares of the secret s according to Π. The share $\mathbf{M_i} \cdot v$ belongs to party $\rho(i)$.
2. Let Π be a LSSS for access structure $\mathbb{A}$ over a set of parties $\mathcal{P}$, which takes $S \in \mathbb{A}$ as input. Let $I = \{i \mid \rho(i) \in S\}$, where $I \subset \{1, \ldots, \ell\}$. For the existence constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$, there is $\sum_{i \in I} \omega_i \lambda_i = s$ if λ_i are valid shares of any secret s. Then we have $\sum_{i \in I} \omega_i M_i = (1, 0, \ldots, 0)$ such that M_i denotes the ith row of $\mathbb{A}$. However, no such constant ω_i exists for unauthorized sets.

Access structures could be described in monotonic boolean formulas, which can be transformed to an LSSS representation. When considering a boolean formulation as an access tree with ℓ nodes, the corresponding LSSS matrix consists of ℓ rows.

3.3 Bilinear groups

Let $\mathbb{G}, \mathbb{G}_T$ be multiplicative cyclic groups of prime order p. Then $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map such that

1. **Bilinearity**: $e(u^a, v^b) = e(u, v)^{ab}$, where $u, v \in \mathbb{G}, a, b \in \mathbb{Z}_p^*$.
2. **Non-degeneracy**:$e(u^a, v^b) \neq 1$ whenever $u, v \neq 1_{\mathbb{G}}$.
3. **Computable**: The bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be computed efficiently.

3.4 Decision bilinear Diffie–Hellman(BDH) assumption

Definition 3 (*DBDH Problem*) Let $a, b, c, z \in \mathbb{Z}_p^*$ be chosen uniformly at random. Given a bilinear group $\mathbb{G}$ of prime order p and a generator g of $\mathbb{G}_T$. The elements are defined as $g^a, g^b, g^c \in \mathbb{G}$, $e(g, g)^z \in \mathbb{G}_T$. For a fair binary coin $\beta \in 0, 1$, if $\beta = 1$, it outputs the tuple $(g, g^a, g^b, g^c, T = e(g, g)^{abc})$; otherwise, it outputs the tuple $(g, g^a, g^b, g^c, T = e(g, g)^z)$. The Decisional Bilinear Diffie–Hellman (DBDH) problem is to distinguish the value β.

The advantage of an adversary $\mathcal{A}$ to distinguish the tuple $(g, g^a, g^b, g^c, T = e(g, g)^{abc})$ from the tuple $(g, g^a, g^b, g^c, T = e(g, g)^z)$ is denoted as

$$|\mathsf{Pr}[\mathcal{A}(g, g^a, g^b, g^c, T = e(g, g)^{abc}) = 1] - \mathsf{Pr}[\mathcal{A}(g, g^a, g^b, g^c, T = e(g, g)^z) = 1]| \quad (1)$$

where the probability is over the randomly chosen generator g, the randomly chosen a, b, c, z in $\mathbb{Z}_p$ and the random bits consumed by $\mathcal{A}$.

Definition 4 (*DBDH assumption*) The DBDH assumption holds in $\mathbb{G}$ if no polynomial-time algorithm has a non-negligible advantage in solving the DBDH problem.

4 Adaptable key-policy attribute-based encryption with time interval

In this section, we first present the formal definition of adaptable KP-ABE with time interval (KP-TIABE) and its formal security model based on those of KP-ABE (Goyal et al. 2006) and TSE (Paterson and Quaglia 2010). We then give a concrete construction of adaptable KP-TIABE.

A standard KP-ABE scheme defines four algorithms, Setup, KeyGen, Encrypt and Decrypt. Adaptable KP-TIABE consists of three servers: a fully trusted policy server generates private keys for users, a semi-trusted time server generates time instant keys, and another semi-trusted adaptation server modifies existing ciphertexts such that they are associated with new time intervals while without learning anything about the underlying plaintexts. Hence, in addition to the four algorithms in the standard KP-ABE, adaptable KP-TIABE includes several additional algorithms: Time.Setup and Token run by the time server, and Adapt.Setup and PolicyAdp run by the adaptation server.

Formally, an adaptable KP-TIABE consists of the following algorithms:

($Global - Setup(\lambda)$) takes a security parameter λ as input. It outputs a system public parameters PP.

Setup(PP, U) takes the system public parameters PP and a small universe of attributes U as inputs. It outputs an attribute public parameter MPK and an attribute master secret key MSK. This algorithm is run by the policy server.

Time.Setup(PP, T) takes as inputs the system's public parameters PP and the number of time periods T supported by the system. It outputs a time public parameter and a time master secret key, which are related to time, represented by TS-MPK and TS-MSK, respectively. This algorithm is run by the time server, which is a semi-trusted proxy.

Adapt.Setup(PP, T) takes as inputs the system's public parameters PP and the number of time periods T supported by the system. It outputs an adaptable public parameter Adp-MPK and an adaptable master secret key

Adp-MSK. This algorithm is run by the adaptation server, which is a semi-trusted proxy.

KeyGen($\mathbb{A}$, MPK, MSK) takes as inputs an access structure $\mathbb{A}$, the attribute master secret key MSK and the attribute public parameter MPK. It outputs a private key ATR-SK related to the access structure.

Token(t, TS-MPK, TS-MSK) takes as inputs a time point t, the time public parameters TS-MPK, the time master secret key TS-MSK. It outputs a time instant key TS-SK.

Encrypt (M, S, $[t_L, t_R]$, MPK, TS-MPK, Adp-MPK) takes a message M, a set of attributes S, a time interval $[t_L, t_R]$ where $t_L \leq t_R$, the attribute public parameters MPK, the time public parameters TS-MPK and the adaptable public parameters Adp-MPK as inputs. It outputs a ciphertext CT.

PolicyAdp (Adp-MSK, CT, $[t'_L, t'_R]$) takes as inputs the adaptable master secret key Adp-MSK, a ciphertext CT under a time interval $[t_L, t_R]$, and a new time interval $[t'_L, t'_R]$, where $t'_L \leq t'_R$. It outputs a new ciphertext CT' under the new time interval $[t'_L, t'_R]$.

Decrypt(CT, ATR-SK, TS-SK) takes as inputs the ciphertext CT which is encrypted under a set of attributes S, the private key ATR-SK with access control structure $\mathbb{A}$ and time instant key TS-SK. If the set of attributes S that are used to encrypt the ciphertext satisfy the access structure $\mathbb{A}$ in the private key ATR-SK, and time point specified in the time instant key TS-SK falls in the decryption time interval, $[t_L, t_R]$ (i.e., the time point t satisfies the time constraint $t_L \leq t \leq t_R$), then the algorithm will decrypt the ciphertext and return a message M; otherwise, it outputs $\perp$.

For the correctness of decryption, we require that, for all PP $\leftarrow$ $(Global - Setup(\lambda))$, (MPK, MSK) $\leftarrow$ Setup (PP, U), (TS-MPK, TS-MSK) $\leftarrow$ Time.Setup (PP, T), (Adp-MPK, Adp-MSK) $\leftarrow$ Adapt.Setup(PP, T), ATR-SK $\leftarrow$ KeyGen($\mathbb{A}$, MPK, MSK), TS-SK $\leftarrow$ Token (t, TS-MPK, TS-MSK), CT $\leftarrow$ Encrypt(M, S, $[t_L, t_R]$, MPK, TS-MPK, Adp-MPK), CT' $\leftarrow$ PolicyAdp (Adp-MSK, CT, $[t'_L, t'_R]$), the following conditions hold:

1. If the requirements shown as follows are satisfied, then $M \leftarrow$ Decrypt(CT, ATR-SK, TS-SK):
   [Attribute Constraint.] The set S of attributes satisfies the access structure $\mathbb{A}$.
   [Time Interval Constraint.] The time point t satisfies $t_L \leq t \leq t_R$.
2. The distribution of CT' and Encrypt(M, S, $[t'_L, t'_R]$, MPK, TS-MPK, Adp-MPK) are identical.

5 Security model for adaptable KP-TIABE

We consider three types of adversaries in adaptable KP-TIABE. Type 1 adversaries, who are allowed to query for any private keys related to the access structures that cannot be used to decrypt the challenge ciphertext, model adversaries in the standard KP-ABE; Type 2 adversaries are allowed to query for the time instant keys and can obtain the time instant key for any time point t that cannot be used to decrypt the challenge ciphertext. Type 3 adversaries, who are equipped with a transformation trapdoor, model security against an eavesdropping proxy. We assume that the proxy in adaptable KP-TIABE is semi-trusted. That is, the proxy does not collude with any user. Thus, Type 3 adversaries are not allowed to query for any private keys.

We now give the security model against Type 1 adversaries for adaptable KP-TIABE, described as a security game between a challenger and a Type 1 adversary. The game proceeds as follows:

Setup The challenger runs Setup, Time.Setup and Adapt.Setup separately to obtain the attribute public parameter MPK, the time public parameter TS-MPK, the adaptable public parameter Adp-MPK and an attribute master secret key MSK, a time master key TS-MSK, an adaptable master key Adp-MSK. It gives (MPK, TS-MPK, Adp-MPK, TS-MSK, Adp-MSK) to the adversary and keeps MSK to itself.

Query Phase 1 The adversary can adaptively query to a private key extraction oracle to get the private keys corresponding to access structures $\mathbb{A}_1, \ldots, \mathbb{A}_q$. Challenger will respond with ATR-SK$_{\mathbb{A}_i}$ $\leftarrow$ KeyGen($\mathbb{A}_i$, MPK, MSK).

Challenge The adversary passes two messages M_0, M_1, a time interval $t_L, t_R \subseteq T$ and a set of attributes S with the restriction that S cannot satisfy any of the queried access structures in Query Phase 1. The challenger computes CT = Encrypt(M_β, S, $[t_L, t_R]$, MPK, TS-MPK, Adp-MPK), where $\beta \in \{0, 1\}$ is chosen randomly. CT is passed to the adversary.

Query Phase 2 The adversary continues to make private key extraction queries with the same restriction as in the Challenge phase.

Guess The adversary outputs its guess β' for β.
The advantage of the Type 1 adversary in this game is defined as $|\Pr[\beta = \beta'] - \frac{1}{2}|$, where the probability is taken over the random bits used by the challenger and the Type 1 adversary.

Definition 5 An adaptable KP-TIABE scheme is secure against Type 1 adversaries if all PPT adversaries have at most a negligible advantage in the above game.

We say that an adaptable KP-TIABE scheme is *selectively* secure against Type 1 adversaries if we add an **Init** stage before **Setup** where the adversary commits to the challenge set of attributes S.

The security model against Type 2 adversaries for adaptable KP-TIABE, which describes a security game between a challenger and a Type 2 adversary, proceeds as follows:

Setup The challenger runs Setup, Time.Setup and Adapt.Setup separately to obtain the attribute public parameter MPK, the time public parameter TS-MPK, the adaptable public parameter Adp-MPK and an attribute master secret keys MSK, a time master key TS-MSK, an adaptable master key Adp-MSK. It gives (MPK, MSK, TS-MPK, Adp-MPK) to the adversary and keeps (TS-MSK, Adp-MSK) to itself.

Query phase 1 The adversary adaptively queries the challenger for time instant key corresponding to a time t_k. In response, the challenger runs $\mathsf{TS\text{-}SK}_{t_k} \leftarrow \mathsf{Token}(t_k, \mathsf{TS\text{-}MSK})$. Then, it gives the private key $\mathsf{TS\text{-}SK}_{t_k}$ to the adversary.

Challenge The adversary submits two (equal-length) messages m_0, m_1, a set of attributes S and a time interval $[t_L, t_R]$, subject to the restriction that none of the queried time instants fall within $[t_L, t_R]$. The challenger selects a random bit $\beta \in \{0, 1\}$, sets $CT = \mathsf{Encrypt}(m_\beta, S, [t_L, t_R], \mathsf{MPK}, \mathsf{TS\text{-}MPK}, \mathsf{Adp\text{-}MPK})$ and sends CT to the adversary as the challenge ciphertext.

Query phase 2 The adversary continues to adaptively query the challenger for time instant keys corresponding to certain time instants with the restriction that none of these instants fall within $[t_L, t_R]$.

Guess The adversary outputs its guess $\beta' \in \{0, 1\}$ for β. Adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$, where the probability is taken over the random bits used by the challenger and the Type 2 adversary.

Definition 6 An adaptable KP-TIABE scheme is secure against Type 2 adversaries if all PPT adversaries have at most a negligible advantage in the above game.

The security model against Type 3 adversaries for adaptable KP-TIABE is described as a security game between a challenger and a Type 3 adversary. The game proceeds as follows:

Setup The challenger runs Setup to generate a public parameter/master secret key pair (MPK, MSK) firstly and runs Time-Setup, Adapt-Setup to generate (TS-MPK,TS-MSK) and (Adp-MPK, Adp-MSK), respectively. Then, it sends (MPK, TS-MPK, TS-MSK,Adp-MPK, Adp-MSK) to the adversary and keeps MSK to itself.

Challenge The adversary submits two (equal-length) messages m_0, m_1, a set of attributes S and a time interval $[t_L, t_R]$. The challenger selects a random bit $\beta \in \{0, 1\}$, sets $CT = \mathsf{Encrypt}(m_\beta, S, [t_L, t_R], \mathsf{MPK}, \mathsf{TS\text{-}MPK}, \mathsf{Adp\text{-}MPK})$ and sends CT to the adversary as the challenge ciphertext.

Guess The adversary outputs its guess $\beta' \in \{0, 1\}$ for β. The advantage of the Type 3 adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$ where the probability is taken over the random bits used by the challenger and the Type 3 adversary.

Definition 7 An adaptable KP-TIABE scheme is secure against Type 3 adversaries if all PPT adversaries have at most a negligible advantage in the above game.

6 Construction of an adaptable KP-TIABE scheme

Based on the KP-ABE scheme (Goyal et al. 2006), the TSE scheme (Kasamatsu et al. 2012) and the adaptable CP-ABE scheme (Lai et al. 2014), we propose our concrete construction of adaptable KP-TIABE scheme. Moreover, we provide the efficiency analysis of our algorithm by comparing it with the others.

6.1 Construction of adaptable KP-TIABE

This scheme is only selectively secure against Type 1 adversaries. The size of public parameters is linear in the number of attributes in the universe. However, our adaptable KP-TIABE can be extended to support a large universe of attributes and achieve full security against Type 1 adversaries.

Concretely, the proposed adaptable KP-TIABE scheme is described as follows:

$(Global - Setup(\lambda))$ Given a security parameter λ as input. Let $\mathbb{G}$ be a bilinear group of prime order p, and let g be a generator of $\mathbb{G}$. The system public parameters (i.e., a bilinear group) are $\mathsf{PP} = (p, \mathbb{G}, \mathbb{G}_T, e, g)$.

$\mathsf{Setup}(\mathsf{PP}, U)$ Given the system's public parameters PP and a small universe of attributes $U = \{1, 2, \ldots, |U|\}$, this algorithm first chooses $h_i \in \mathbb{G}$ uniformly at random for each attribute $i \in U$. Then, it chooses a $\alpha \in \mathbb{Z}_p$. The published attribute public parameters MPK are

$$\mathsf{MPK} = (e(g, g)^\alpha, h_1, \ldots, h_{|U|}).$$

The attribute master secret key is $\mathsf{MSK} = \alpha$.

TS-Setup(PP, T) Given the system's public parameters PP and the number of time periods T, this algorithm chooses $a, b \in \mathbb{Z}_p$ and the time public parameters are published as

$$\mathsf{TS\text{-}MPK} = e(g, g)^{ab}.$$

The time server's secret key is $\mathsf{TS\text{-}MSK} = g^{ab}$. The system supports time space $[0, T-1]$.

Adapt-Setup(PP, T) Given the system's public parameters PP and the number of time periods T, this algorithm proceeds as follows. For each time point i, it chooses $\gamma_i \in \mathbb{Z}_p$ uniformly at random and sets $I_i = g^{\gamma_i}$. It then chooses $\gamma_{2,F}, \gamma_{2,B} \in \mathbb{Z}_p$ uniformly at random and sets $g_{2,F} = g^{\gamma_{2,F}}, g_{2,B} = g^{\gamma_{2,B}}$. The adaptable public parameters are published as

$$\mathsf{Adp\text{-}MPK} = (I_0, \ldots, I_T, g_{2,F}, g_{2,B}).$$

The server's master secret key is $\mathsf{Adp\text{-}MSK} = (\gamma_0, \ldots, \gamma_T, \gamma_{2,F}, \gamma_{2,B})$.

KeyGen($\mathbb{A}$, MPK, MSK) The key generation algorithm takes as inputs the attribute public parameter MPK, the attribute master secret key MSK and an LSSS access structure $\mathbb{A} = (\mathbf{A}, \rho)$, where $\mathbf{A}$ is an $\ell \times n$ matrix and ρ is a map from each row A_i of $\mathbf{A}$ to an attribute $\rho(i)$. The algorithm first chooses a random vector $\mathbf{v} \in \mathbb{Z}_p^n$ such that $\mathbf{1} \cdot \mathbf{v} = \alpha$, where $\mathbf{1}$ denotes the vector with the first entry equal to 1 and the rest equal to 0. Then, for each row A_i of $\mathbf{A}$, it chooses $r_i \in \mathbb{Z}_p$ uniformly at random. The private key related to access structure $\mathsf{ATR\text{-}SK} = (\mathbb{A} = (\mathbf{A}, \rho),\ K_i^1, K_i^2)$ is computed as

$$K_i^1 = g^{A_i \cdot \mathbf{v}} h_{\rho(i)}^{-r_i},\ K_i^2 = g^{r_i}\ \forall i \in \{1, 2, \ldots, \ell\}.$$

Token(t, TS-MPK, TS-MSK) The algorithm for time instant key generation takes as inputs the time point t, the time public parameters TS-MPK and the time master secret key TS-MSK. It uniformly chooses random values $\xi, r \in \mathbb{Z}_p$. The time instant key $\mathsf{TS\text{-}SK} = (sk_{t+1,F}, sk_{T-t,B}, t)$ is computed as

$$sk_{t+1,F} = \left(g^{ab+\xi} \cdot \left(I_0^{2T+1} \cdot \prod_{k=1}^{t+1} I_k^k \cdot g_{2,F} \right)^r, g^r, I_{t+2}^r, \ldots, I_T^r \right),$$

$$sk_{T-t,B} = \left(g^{-\xi} \cdot \left(I_0^{2T+1} \cdot \prod_{k=1}^{T-t} I_k^{T+k} \cdot g_{2,B} \right)^r \times g^r, I_{T-t+1}^r, \ldots, I_T^r \right).$$

Encrypt $(M, S, [t_L, t_R], \mathsf{MPK}, \mathsf{TS\text{-}MPK}, \mathsf{Adp\text{-}MPK})$ To encrypt a message $M \in \mathbb{G}_T$ under a set of attributes S and time interval $[t_L, t_R]$, separate the message into two parts, $M = M_0 \cdot M_1$. One part of the message, M_0, is encrypted under a set of attributes S, and another part of the message, M_1, is encrypted under the time interval $[t_L, t_R]$. In addition, it chooses random value $s, \sigma \in \mathbb{Z}_p$ and publishes the ciphertext as $CT = (S, C_0, C_0', C_i, C_1, C_2, C_3, C_4, C_5)$, where:

$$\begin{aligned}
C_0 &= M_0 \cdot e(g, g)^{\alpha s},\\
C_0' &= g^s, \{C_i = h_i^s\}_{i \in S},\\
C_1 &= M_1 \cdot e(g, g)^{ab\sigma},\\
C_2 &= g^\sigma,\\
C_3 &= (I_0^{2T+1} \cdot \prod_{k=1}^{t_R+1} I_k^k \cdot g_{2,F})^\sigma,\\
C_4 &= (I_0^{2T+1} \cdot \prod_{k=1}^{T-t_L} I_k^{T+k} \cdot g_{2,B})^\sigma,\\
C_5 &= [t_L, t_R].
\end{aligned}$$

PolicyAdp(Adp-MSK, CT, $[t_L', t_R']$) The time modification algorithm takes as inputs Adp-MSK, a ciphertext $CT = (S, C_1, C_2, C_3, C_4, C_5, C_6, C_i)$ and a new time interval $[t_L', t_R']$. With the help of $\mathsf{Adp\text{-}MSK} = (\gamma_0, \ldots, \gamma_T, \gamma_{2,F}, \gamma_{2,B})$, this algorithm modifies the ciphertext CT in to a new ciphertext CT' under the time interval $[t_L', t_R']$ without changing the underlying message of CT. Let $CT = (S, C_0, C_0', C_i, C_1, C_2, C_3, C_4, C_5)$, where:

$$\begin{aligned}
C_0 &= M_0 \cdot e(g, g)^{\alpha s},\\
C_0' &= g^s, \{C_i = h_i^s\}_{i \in S};\\
C_1 &= M_1 \cdot e(g, g)^{ab\sigma},\\
C_2 &= g^\sigma\\
C_3 &= \left(I_0^{2T+1} \cdot \prod_{k=1}^{t_R+1} I_k^k \cdot g_{2,F} \right)^\sigma,\\
C_4 &= \left(I_0^{2T+1} \cdot \prod_{k=1}^{T-t_L} I_k^{T+k} \cdot g_{2,B} \right)^\sigma,\\
C_5 &= [t_L, t_R].
\end{aligned}$$

This algorithm chooses $\tilde{s}, \tilde{\sigma} \in \mathbb{Z}_p$ uniformly at random. Let $s' = s + \tilde{s}$ and $\sigma' = \sigma + \tilde{\sigma}$. Using $C_2 = g^{\sigma}$ and $\mathsf{Adp\text{-}MSK} = (\gamma_0, \ldots, \gamma_T, \gamma_{2,F}, \gamma_{2,B})$, it first computes $\bar{C}_3 = (I_0^{2T+1} \cdot \prod_{k=1}^{t'_R+1} I_k^k \cdot g_{2,F})^{\sigma}$ and $\bar{C}_4 = (I_0^{2T+1} \cdot \prod_{k=1}^{T-t'_L} I_k^{T+k} \cdot g_{2,B})^{\sigma}$. Then, the new ciphertext $CT = (S, C'_0, C''_0, C'_i, C'_1, C'_2, C'_3, C'_4, C'_5)$ is computed as

$$
\begin{aligned}
C'_0 &= C_0 \cdot e(g,g)^{\alpha\tilde{s}} = M \cdot e(g,g)^{\alpha s'},\\
C''_0 &= C'_0 \cdot g^{\tilde{s}} = g^{s'}, \{C'_i = C_i \cdot h_i^{\tilde{s}} = h_i^{s'}\}_{i\in S},\\
C'_1 &= C_1 \cdot \cdot e(g,g)^{ab\tilde{\sigma}} = M_1 \cdot e(g,g)^{ab\sigma'},\\
C'_2 &= C_2 \cdot g^{\tilde{\sigma}} = g^{\sigma'},\\
C'_3 &= \bar{C}_3 \cdot \left(I_0^{2T+1} \cdot \prod_{k=1}^{t'_R+1} I_k^k \cdot g_{2,F}\right)^{\tilde{\sigma}}\\
&= \left(I_0^{2T+1} \cdot \prod_{k=1}^{t'_R+1} I_k^k \cdot g_{2,F}\right)^{\sigma'},\\
C'_4 &= \bar{C}_4 \cdot \left(I_0^{2T+1} \cdot \prod_{k=1}^{T-t'_L} I_k^{T+k} \cdot g_{2,B}\right)^{\tilde{\sigma}}\\
&= \left(I_0^{2T+1} \cdot \prod_{k=1}^{T-t'_L} I_k^{T+k} \cdot g_{2,B}\right)^{\sigma'},\\
C'_5 &= [t'_L, t'_R].
\end{aligned}
$$

Obviously, the distribution of CT' is the same as that of the ciphertext generated by $\mathsf{Encrypt}(M \in \mathbb{G}_T, S, T' = [t'_L, t'_R], \mathsf{MPK}, \mathsf{TS\text{-}MPK}, \mathsf{Adp\text{-}MPK})$.

$\mathsf{Decrypt}(CT, \mathsf{ATR\text{-}SK}, \mathsf{TS\text{-}SK})$ The decryption algorithm takes as inputs $\mathsf{ATR\text{-}SK}$, $\mathsf{TS\text{-}SK}$ and a ciphertext CT.

The decryption procedure consists of two parts: attribute constraint part and time constraint part.

Attribute constraint It uses the private key $\mathsf{ATR\text{-}SK} = (\mathbb{A} = (\mathbf{A}, \rho), K_i^1, K_i^2)$ for an access structure $\mathbb{A} = (\mathbf{A}, \rho)$ to recover the first part of the message, M_0, which could be successfully decrypted only if the access structure $\mathbb{A}$ is satisfied by the set of attributes S; otherwise, it outputs $\perp$. Assume that the set of attributes S satisfies the access structure $\mathbb{A}$ and we define $I \subset \{1, 2, \ldots, \ell\}$ as $I = \{i : \rho_i \in S\}$. Then, the attribute constraint part of decryption computes constant $\omega_i \in \mathbb{Z}_p$ such that $\sum_{i\in I} \omega_i A_i = \{1, 0, \ldots, 0\}$, and

$$
d_{ATR} = \frac{C_0}{\prod_{i\in I}(e(C'_0, K_i^1) \cdot e(C_{\rho(i)}, K_i^2))^{\omega_i}} = M_0
$$

Time constraint This part of decryption requires the time instant key $\mathsf{TS\text{-}SK} = (sk_{t+1,F}, sk_{T-t,B}, t)$. For each time instant key, there is a specified time point t that the key was published. As the message M_1 is encrypted by a time interval $C_5 = [t_L, t_R]$, it could be decrypted successfully only if the specified time point t falls in the time interval C_5. Then we conclude that if $t \notin C_5$, it returns $\perp$. Assuming that time point $t \in C_5$, the time point t needs to be extended to the time interval $C_5 = [t_L, t_R]$. We then have

$$
\begin{aligned}
sk_{t+1,F} &= \left(g^{ab+\xi} \cdot \left(I_0^{2T+1} \cdot \prod_{k=1}^{t_R+1} I_k^{T+k} \cdot g_{2,F}\right)^r, g^r, I_{t_R+2}^r, \right.\\
&\qquad \left. \ldots, I_T^r\right)\\
&= \left(D_1, D_2, b_{T-t_L+1}, \ldots, b_T\right),\\
sk_{T-t.B} &= \left(g^{-\xi} \cdot \left(I_0^{2T+1} \cdot \prod_{k=1}^{T-t_L} I_k^{T+k} \cdot g_{2,B}\right)^r, g^r, I_{T-t_L+1}^r, \right.\\
&\qquad \left. \ldots, I_T^r\right)\\
&= (R_1, R_2, b_{T-t_L+1}, \ldots, b_T).
\end{aligned}
$$

The time constraint part of decryption computes:

$$
d_{TS} = \frac{C_1 \cdot e(C_3, D_2) \cdot e(R_2, C_4)}{e(C_2, D_1) \cdot e(R_1 \cdot C_2)} = M_1
$$

The final message M can be obtained from $d_{ART} \cdot d_{TS} = M_0 \cdot M_1$.

Obviously, the above scheme satisfies the correctness of adaptable KP-TIABE. Next, we state the security theorems of the scheme.

Theorem 1 *If the KP-ABE scheme proposed in Goyal et al. (2006) is selectively secure, then our proposed adaptable KP-TIABE scheme is selectively secure against Type 1 adversaries.*

Proof Since Type 1 adversaries in the adaptable KP-TIABE scheme model adversaries in a standard KP-ABE scheme, and the KP-ABE scheme proposed in Goyal et al. (2006) is selectively secure, then our proposed adaptable KP-TIABE scheme is also selectively secure against Type 1 adversaries.

Theorem 2 *If the ID-TSE scheme proposed in Kasamatsu et al. (2012) is selectively secure, then our proposed adaptable KP-TIABE scheme is selectively secure against Type 2 adversaries.*

Proof Since Type 2 adversaries in an adaptable KP-TIABE scheme model adversaries in the ID-TSE scheme, and the ID-TSE scheme proposed in Kasamatsu et al. (2012) is selectively secure, then our proposed adaptable KP-TIABE scheme is also selectively secure against Type 2 adversaries.

Table 1 Efficiency summary of ABE schemes

Scheme	Out. CT size	Out. dec ops	Full CT size	Full dec ops
GPSW (Goyal et al. 2006)	$(1+l)\|\mathbb{G}\|$	$\leq (1+l)P + 2lE_{\mathbb{G}}$	$\|\mathbb{G}_T\| + (1+l)\|\mathbb{G}\|$	$E_{\mathbb{G}_T}$
LDGW (Lai et al. 2013)	$(3+4l)\|\mathbb{G}\|$	$\leq (4+2l)P + (2+4l)E_{\mathbb{G}}$	$2\|\mathbb{G}_T\| + \|\mathbb{G}\|$	$2E_{\mathbb{G}} + 2E_{\mathbb{G}_T}$
KP-TIABE	$(1+2l)\|\mathbb{G}\|$	$\leq (1+l)P + lE_{\mathbb{G}}$	$2\|\mathbb{G}_T\| + \|\mathbb{G}\|$	$E_{\mathbb{G}_T}$

Theorem 3 *If the DBDH assumption holds, then our proposed adaptable KP-TIABE is secure against Type 3 adversaries.*

Proof Suppose there exists a Type 3 adversary $\mathcal{A}$ against our proposed adaptable KP-TIABE scheme with non-negligible advantage. We are going to construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the DBDH problem with non-negligible probability.

$\mathcal{B}$ is given as input a random 5-tuple (g, g^x, g^y, g^z, T) that is either sampled from $\mathcal{P}_{BDH}$ (where $T = e(g,g)^{xyz}$) or from $\mathcal{R}_{BDH}$ (where T is uniform and independent in $\mathbb{G}_T$). Algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g,g)^{xyz}$ and 0 otherwise. Algorithm $\mathcal{B}$, playing the role of challenger, runs $\mathcal{A}$ executing the following steps.

Setup $\mathcal{B}$ chooses random elements $h_1, \ldots, h_{|U|} \in \mathbb{G}$. The adaptable public parameters are

$$\mathsf{MPK} = (e(g^x, g^y), h_1, \ldots, h_{|U|}).$$

It sets $\alpha = xy$ implicitly, which is unknown to $\mathcal{B}$. Then, $\mathcal{B}$ runs Time-Setup, Adapt-Setup to generate (TS-MPK,TS-MSK) and (Adp-MPK, Adp-MSK), respectively. Finally, $\mathcal{B}$ sends (MPK, TS-MPK, TS-MSK,Adp-MPK, Adp-MSK) to adversary $\mathcal{A}$.

Challenge The adversary $\mathcal{A}$ outputs two equal-length messages (M_0, M_1), a set S of attributes and a time interval $[t_L, t_R]$. $\mathcal{B}$ flips a fair coin $\beta \in \{0,1\}$ firstly. Then, $\mathcal{B}$ chooses a random $\tilde{M} \in \mathbb{G}_T$ and $\sigma \in \mathbb{Z}_p$ and computes

$$C_0 = M_\beta / \tilde{M} \cdot T,$$
$$C_0' = g^z, \{C_i = h_i^z\}_{i \in S},$$
$$C_1 = \tilde{M} \cdot e(g,g)^{ab\sigma},$$
$$C_2 = g^\sigma$$
$$C_3 = \left(I_0^{2T+1} \cdot \prod_{k=1}^{t_R+1} I_k^k \cdot g_{2,F} \right)^\sigma,$$
$$C_4 = \left(I_0^{2T+1} \cdot \prod_{k=1}^{T-t_L} I_k^{T+k} \cdot g_{2,B} \right)^\sigma,$$
$$C_5 = [t_L, t_R].$$

Finally, $\mathcal{B}$ sets $CT = (S, C_0, C_0', C_i, C_1, C_2, C_3, C_4, C_5)$ as the challenge ciphertext and sends it to $\mathcal{A}$. Obviously, the challenge ciphertext is a valid encryption of M_β with the correct distribution whenever $T = e(g,g)^{xyz} = e(g^x, g^y)^z = e(g,g)^{\alpha z}$ (as is the case when the input 5-tuple is sampled from $\mathcal{P}_{BDH}$). On the other hand, when T is uniform and independent in $\mathbb{G}_T$ (which occurs when the input 5-tuple is sampled from $\mathcal{R}_{BDH}$), the challenge ciphertext CT is independent of β in the adversary's view.

Guess The adversary $\mathcal{A}$ outputs a bit β'. If $\beta' = \beta$, then $\mathcal{B}$ outputs 1 meaning $T = e(g,g)^{xyz}$. Otherwise, it outputs 0 meaning $T \neq e(g,g)^{xyz}$.

Observe that when the input 5-tuple is sampled from $\mathcal{P}_{BDH}$ (where $T = e(g,g)^{xyz}$), then $\mathcal{A}$'s view is identical to its view in a real attack game. On the other hand, when the input 5-tuple is sampled from $\mathcal{R}_{BDH}$ (where T is uniform in $\mathbb{G}_T$), then the value of β is information-theoretically hidden from the adversary $\mathcal{A}$. Thus, if $\mathcal{A}$ breaks our proposed adaptable KP-TIABE scheme with non-negligible advantage, then $\mathcal{B}$ will solve the DBDH problem with non-negligible probability.

6.2 Performance comparison

We compare the performance of our scheme with the other ABE schemes (Goyal et al. 2006; Lai et al. 2013). They have already been used to encrypt users' private data with a higher encryption performance. In Table 1, l refers as an LSSS access structure of $l \times n$ matrix. We use P, $E_{\mathbb{G}}$, $E_{\mathbb{G}_T}$ to represent the maximum time to compute a pairing, an exponentiation in $\mathbb{G}$ and an exponentiation in $\mathbb{G}_T$. The "Out. CT size" and "Full CT size" represent the ciphertext that is referred as the input of PolicyAdp and Decrypt, respectively.

7 Conclusion

In this paper, we introduced an extension of KP-ABE, called adaptable key-policy attribute-based encryption with time interval (KP-TIABE), by novelly combining the standard key-policy attribute-based encryption (KP-ABE), adaptable ciphertext-policy attribute-based encryption (CP-ABE) and time-specific encryption (TSE). We formalized the notion of KP-TIABE and presented an concrete scheme based on an algebraic combination of the KP-ABE scheme in Goyal et al. (2006), the adaptable CP-ABE scheme in Lai et al. (2014) and the TSE scheme in Paterson and Quaglia (2010).

We believe that adaptable KP-TIABE finds many practical applications since it not only deals with access control of encrypted data based on the relationship between attributes and access policies, but also puts constraint on the time of decryption. Moreover, KP-TIABE is able to adjust decryption time intervals associated with ciphertexts according to users' requirements, which makes it especially attractive in dynamic system settings.

Compliance with ethical standards

Conflict of interest The authors declare that there is no conflict of interest.

References

Beimel A (1996) Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel

Blake IF, Chan ACF (2004) Scalable, server-passive, user-anonymous timed release public key encryption from bilinear pairing. In: IACR cryptology ePrint archive, 2004, p 211

Blaze M, Bleumer G, Strauss M (1998) Divertible protocols and atomic proxy cryptography. In: Advances in cryptology—EUROCRYPT'98. Springer, pp 127–144

Boneh D, Boyen X, Goh E-J (2005) Hierarchical identity based encryption with constant size ciphertext. In: Advances in cryptology—EUROCRYPT 2005. Springer, pp 440–456

Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security. ACM, pp 89–98

Jakobsson M (1999) On quorum controlled asymmetric proxy re-encryption. In: Public key cryptography, vol 1560. Springer, pp 112–121

Kasamatsu K, Matsuda T, Emura K, Attrapadung N, Hanaoka G, Imai H (2012) Time-specific encryption from forward-secure encryption. In: Security and cryptography for networks, vol 7485. Springer, Heidelberg, pp 184–204

Lai J, Deng RH, Guan C, Weng J (2013) Attribute-based encryption with verifiable outsourced decryption. IEEE Trans Inf Forensics Secur 8(8):1343–1354

Lai J, Deng RH, Yang Y, Weng J (2014) Adaptable ciphertext-policy attribute-based encryption. In: Pairing-based cryptography—pairing 2013. Springer, pp 199–214

May T (1993) Time-release crypto, Manuscript. http://www.cyphernet.org/cyphernomicon/chapter14/14.5.html

Mora Afonso V, Carballero-Gil P (2014) Using identity-based cryptography in mobile applications. In: International joint conference SOCO'13-CISIS'13-ICEUTE'13, 239. Springer, pp 527–536

Muñoz AM, Rodríguez AF, Encinas LH, Alcázar BA (2013) A toolbox for dpa attacks to smart cards. In: International joint conference SOCO. Springer, pp 399–408

Paterson KG, Quaglia EA (2010) Time-specific encryption. In: Garay JA, De Prisco R (eds) Security and cryptography for networks. Springer, Berlin, pp 1–16

Rivest RL, Shamir A, Wagner DA (1996) Time-lock puzzles and timed-release crypto. Technical report, MIT, MA

Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Advances in cryptology—EUROCRYPT 2005. Springer, pp 457–473

Waters B (2011) Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Public key cryptography—international conference on practice and theory of public-key cryptography 2011. Springer, pp 53–70

Weng J, Deng RH, Ding X, Chu CK, Lai J (2009) Conditional proxy re-encryption secure against chosen-ciphertext attack. In: Proceedings of the 4th international symposium on information, computer, and communications security. ACM, pp 322–332