Exclusion-Intersection Encryption

Sherman S.M. Chow[1]* and Siu-Ming Yiu[2]

[1] Department of Combinatorics and Optimization
University of Waterloo
Ontario, Canada N2L3G1
smchow@math.uwaterloo.ca

[2] Department of Computer Science
University of Hong Kong
Pokfulam, Hong Kong
smyiu@cs.hku.hk

Abstract. Identity-based encryption (IBE) has shown to be a useful cryptographic scheme enabling secure yet flexible role-based access control. We propose a new variant of IBE named as *exclusion-intersection encryption*: during encryption, the sender can specify the targeted groups that are legitimate and interested in reading the documents; there exists a trusted key generation centre generating the *intersection* private decryption keys on request. This special private key can only be used to decrypt the ciphertext which is of all the specified groups' interests, its holders are *excluded* from decrypting when the documents are not targeted to all these groups (e.g., the ciphertext of only a single group's interest). While recent advances in cryptographic techniques (e.g., attribute-based encryption or wicked IBE) can support a more general access control policy, the private key size may be as long as the number of attributes or identifiers that can be specified in a ciphertext, which is undesirable, especially when each user may receive a number of such keys for different decryption power. One of the applications of our notion is to support an ad-hoc joint project of two or more groups which needs extra helpers that are not from any particular group. We also present an online/offline variant such that encryption can be computed quickly after offline precomputation.

Key words: access control, compact private key, data confidentiality, exclusion-intersection encryption, identity-based encryption, online/offline

1 Introduction

Controlling the access of data via complex policies is always a challenging issue, especially for dynamic organizations where people assume different roles in different (possibly ad-hoc) projects and people's roles may change over time. Identity-based encryption (IBE) [BF03] (and the references in [Cho09]) has shown to be a

* Corresponding author. Part of the work described here is done while visiting Department of Computer Science, The University of Hong Kong.

useful cryptographic scheme enabling secure yet flexible role-based access control [CHSS02, MB03, MBD03, Sma03, ARMLS06, CRR08, CY08] (in particular, the access of the plaintext encrypted in a ciphertext). One of the reasons is that the access control policy can be expressed using an identity string as a basic unit, for example, we may specify a time in the string to realize a time-specific access control policy (e.g., [CRR08, CY08] and the references within). This identity-based encryption technique has also been leveraged to devise attribute-based encryption (e.g., [GPSW06, BSW07, CC09]) which provide a cryptographic access control solution with a more fine-grained access policy. On the other hand, many identity-based (ID-based) schemes have been adopted to solve a particular set of problems more efficiently, e.g., for speeding up the signing algorithm we have ID-based signature scheme which allows multiple keys per user [LP07]; for speeding up the encryption algorithm we have IBE for multiple recipients [BSNS05]; and we have IBE schemes for other design goals such as having a "powerful" identity-based private key where wildcards can be specified as part of the identity-strings (without giving an exponential number of private keys) in wicked IBE [AKN08], etc.

In this paper, we propose a special kind of IBE named as *exclusion-intersection encryption*: during encryption, the sender can specify the target groups (say A, B, and C) that are legitimate and interested to read the documents. There exists a trusted key generation centre (KGC) generating *intersection* private decryption keys (e.g., $A \cap B \cap C$, $B \cap C$ or just A) on request. We use the "$\cap$" notation from the key's decryption power perspective: the key for $A \cap B$ is a less powerful key than the key for A, analogous to the fact that $A \cap B$ is a subset of A. This private key can be used to decrypt the ciphertext which is of all the groups' interests as specified by the *key* (e.g., the decryption key of $A \cap B \cap C$ can decrypt the ciphertext which is of all of A and B and C's interests). Decryption is also possible when the group-identifiers specified in the ciphertext *contains* the identifiers specified in the key (e.g., the decryption key of A can decrypt the ciphertext designated to only A, or both A and B, or all of A, B and C). But its holders are *excluded* from decrypting when the documents are not targeted to all these groups (e.g., the decryption key of $A \cap B \cap C$ can *neither* decrypt the ciphertext targeted to $A \cap B$, *nor* the ciphertext targeted to C). In other words, decryption is not possible since the group-identifiers specified in the ciphertext does not *contain* all the identifiers specified in the key (e.g., C is missing from the description $A \cap B$, so the decryption key of $A \cap B \cap C$ *cannot* decrypt the ciphertext targeted to $A \cap B$).

Obviously, we do not want the ciphertext size to be in the order of the size of the power set, i.e., $O(2^\ell)$ for ℓ possible groups. On the other hand, constant size private keys are desirable. Otherwise, this can be trivially done by a traditional IBE when users get the private keys corresponding to all possible "extension" of identifiers (e.g., $\{A, A \cap B, A \cap C, \cdots, A \cap B \cap C, \cdots\}$). In this paper, we propose a scheme which achieves linear-size ciphertexts and constant-size private key. Our proposed scheme uses an identity-based key structure modified from Sakai-Kasahara IBE [SK03] and uses REACT transformation [OP01] to achieve chosen-ciphertext security, and hence our security analysis is given in the random oracle model.

1.1 Applications

Ad-Hoc Collaborative Group Work. This class of encryption scheme finds natural application in supporting ad-hoc joint projects of two or more groups which needs extra helpers that are not from any particular group. The KGC only needs to generate the intersection private key to these extra helpers, then all parties concerned (both the original groups and those new helpers) can decrypt the documents for this joint project, but these new helpers cannot decrypt the documents which are confidential to any proper subset of groups. The key distribution is minimal as only these new helpers (instead of all related people of the project) need to get a new key. In particular, the people who already got the decryption right do not require to get another key, and hence the trouble of managing many keys such as deciding which key to use in which situation can be avoided. Besides, our proposed scheme supports constant private key size[3] which is especially helpful when people may have multiple duties and get a number of keys corresponding to different decryption power.

Our scheme supports cryptographic workflow [ARMLS06, BF06] in the sense that sender can create the encrypted documents even if the decryption key are yet to be generated by KGC and obtained by the related parties. Our scheme is useful when the sender does not have the knowledge of the access-control policy nor the hierarchy of the groups in an organization. Consider an applicant for PhD programme who just got a few more papers accepted for publication and wants to submit a more updated version of his curriculum vitae (CV) to a certain university so as to increase his chance of being admitted. The application committee usually consists of the staff members from both the graduate school ("Grad. Sch."), the admission office ("Admission"), and the department of interest, say Department of Computer Science ("CS"). By using our proposed exclusion-intersection encryption, he can encrypt his CV to *"Grad. Sch."*, *"Admission"*, *"CS"*. As a result, the staff members at graduate school, admission office, and CS department or a special group of people (hereinafter referred as *"Helpers"*) only handling graduate admission of CS (if such a group exists) can decrypt and read his CV, irrespective of the private key issuing policy of the university. On the other hand, if there are other emails directed at Graduate School and CS Department which are not related to admission, say the annual review of CS graduate students, this group of admission helpers cannot decrypt.

Privacy-Respecting Supervision. We can also use this scheme in another way round. In hierarchical IBE [GS02] (and the references in [Cho09]), the one

[3] As a consequence, there should be many different attribute sets that result in the same key. The structure of the key should ensure that if an adversary can find such two attribute sets, it results in some non-trivial relation between a set of collision-resistant hash functions.

at a higher level of hierarchy (say the manager) has a higher decryption power (i.e., can decrypt the ciphertext designated to the users at a lower level of hierarchy, usually his group of sub-ordinates). Now we consider the scenario that the privacy of sub-ordinates is of importance, such that their manager cannot read their private message unless the message is of whole group's interests. Suppose there is a group of students $\{\mathsf{id}_i | i \in [1, t]\}$ with a supervisor. One can assign the key $\mathsf{id}_1 \cap \mathsf{id}_2 \cdots \cap \mathsf{id}_t$ to the supervisor. In doing so, the supervisor cannot read a private message directed to only one or a subgroup of students, but he can decrypt the encrypted messages when all students in his group are appointed as receivers. Unfortunately, in contrast to the previous application, re-keying (to the manager) is required if some new members join the group. We also remark that there is a variant of hierarchical IBE which is called structural IBE [AY07], in which a user can decrypt ciphertext for all his/her ancestors (but not descendants) in the hierarchy, in contrast with a normal hierarchical IBE.

1.2 Online/Offline Encryption

[GMC08] first studied the notion of identity-based online/offline encryption. The main idea is that, encryption can be done in a very efficient manner when offline pre-computation is allowed. During the offline phase, part of the encryption process can be started, without knowing the message to be encrypted nor the identity of the recipient. Efficient online encryption can be done when the message and the identity are available. [CLZ11] proposed an identity-based online/offline encryption scheme which is more efficient than those by [GMC08] by relying on the random oracle model. They also put forth the notion of identity-based online/offline key-encapsulation mechanism and presented a generic transformation to get security against chosen-ciphertext attack.

1.3 Organizations

The rest of the paper is organized as follows. Related work on access control from elliptic curve pairings and various different variants of identity-based encryption are discussed in next section. Section 3 contains the framework and the security notions for exclusion-intersection encryption. Our proposed construction will be presented in Section 4, which includes a description of the building blocks being used in our proposed scheme, and the number-theoretical assumptions related to the security of our scheme. Efficiency and security analysis will also be given. We conclude the paper in Section 6.

2 Related Work

2.1 Conjunction and Disjunction Policy by IBE Techniques

Notions similar to our concept of exclusion-intersection encryption can be found in [CHSS02] and [Sma03], which considered the "conjunction" and "disjunction" of private keys associated with multiple identities. By conjunction, any entity who has all the private keys involved with an encrypted message can do the decryption; while disjunction means any one who has at least one of the private keys involved with an encrypted message can get the plaintext. In [BSNS05, BF05, CS06, PKL08], efficient multi-receiver identity-based encryption (i.e., encryption in "disjunction" model) were proposed together with formal models and security proofs. In [Del07], identity-based *broadcast* (multi-receiver) encryption with constant size ciphertexts and private keys are proposed. However, there is no work addressing *exactly* the access control policy we considered. We acknowledge that schemes supporting even more general access control policy exist, but we will see shortly afterward that the generalities come with higher computational costs or secure storage requirements. In particular, our scheme supports constant size private key and requires only a constant number of pairing operations in decryption.

2.2 Hierarchical IBE and Wicked IBE

It may seem possible to achieve the same functionalities with hierarchical IBE, but we argue that it is not always the case. Back to our example on CS graduate school application, the applicant may not know the hierarchy of the groups in that university (for examples, whether the graduate school is at a level higher than the CS department or if there is a group of people handling graduate admissions under the CS department), or simply there is no such hierarchy. One of the possible solution is that both of the graduate school and the CS department generate the "descendants private key" for CS department and graduate school respectively, i.e., the helpers will get both the private key corresponding to *"Grad. Sch."* → *"CS"* and *"CS"* → *Grad. "Sch"* (where $A \rightarrow B$ denotes A is at a level higher than B). It seems that the same result can be achieved as (1) the sender does not need to know the hierarchy (i.e., he can use either *"Grad. Sch."* → *"CS"* or *"CS"* → *"Grad. Sch."* as the identifier), (2) the helpers cannot read the existing encrypted document for *"Grad. Sch."* and *"CS"* (as being at the lower level of the hierarchy), (3) the KGC only needs to generate private key for the helpers. However, this way is not scalable if the number of different groups involved increases.

While one can solve the above problem by restricting the level where an identity can appear (in other words, the identifiers space are partitioned) [CS06, PKL08], e.g., for a 2-level IBE, *"CS Department"* is restricted to appear only at the second level. This does not make the problem trivial since the KGC is now required to generate a private key for the second level directly which "skips" the first level. This leads to the notion of identity-based encryption with wild-card key derivation (or wicked IBE) [AKN08], such that a private key for a vector of identity strings can have entries which are left blank using a wildcard. However, both constructions in [AKN08] have decryption key sizes grow linearly with the number of wildcards, i.e., the more powerful the key, the larger it is. One may view our proposal as a wicked IBE without further key derivation, which is the price we pay for a constant size private key.

2.3 Attribute-Based Encryption and Hidden-Vector Encryption

The access control policy considers in this paper is actually covered by key-policy attribute-based encryption (KP-ABE) [GPSW06]. For a ciphertext marked with attributes A, B and C, all the keys in the powerset of $\{A, B, C\}$, e.g., $A \cap B \cap C$ or $B \cap C$, can be generated by the KGC and can be used for decryption of such a ciphertext. However, the size of the key in KP-ABE usually grows linearly with the number of attributes it encompasses. Besides, for these schemes the number of pairing operations required in decryption also grows linearly with the number of attributes embedded in the decryption key.

On the other hand, it is unclear how to use ciphertext-policy ABE [BSW07] to achieve our purpose efficiently. The private key size usually grows linearly with the number of attributes. We may also need to specify the ciphertext under a policy like "A OR B OR C OR $(A \cap B) \cdots$ OR $(A \cap B \cap C)$.

One may also realize the same functionality as our scheme by using hidden-vector encryption (HVE) [BW07], which provides conjunctive queries over multi-valued attributes. HVE associates a ciphertext with a vector $x = (x_1, \cdots, x_\ell)$ and each key K with a vector $y = (y_1, \cdots, y_\ell)$. Each element of a vector can be chosen from a predefined range. Key K can decrypt ciphertext C if and only if $x = y$ for all i where $y_i \neq *$ ($*$ is a wildcard symbol). Using our previous example, we may identify A with x_1, B with x_2 and C with x_3. A ciphertext for B and C is encrypted under vector $x = (0, 1, 1)$. The decryption key of B is identified with vector $(*, 1, *)$, for C it will be identified with vector $(*, *, 1)$, $B \cap C$ uses $(*, 1, 1)$, and finally the decryption key of $A \cap B \cap C$ is identified with vector $(1, 1, 1)$. However, existing schemes [BW07, IP08] have $O(\ell)$-size keys and use $O(\ell)$ pairings per decryption where ℓ is the number of the fields; but HVE supports more expressive queries and these two schemes can be proven secure in the standard model.

3 Exclusion-Intersection Encryption

From now on, we will use the generic term "identity" throughout our discussion to replace the notion of "group" we used in the introduction in Section 1. To bridge the gap, one may simply think of the groups involved in our motivating scenario are now all identified by different strings. In other words, the identity in the scheme will be the group identifier.

3.1 Framework

- $\mathtt{Setup}(1^k, \ell)$: On an unary string input 1^k and a positive integer ℓ where k is a security parameter and ℓ denotes the maximum number of identity that can be associated to a user trapdoor, it produces the master secret key msk and the public parameters param, which include a description of a finite plaintext space and a description of a finite ciphertext space. We omitted the inclusion of the public parameters as part of the input in the descriptions of the remaining algorithms.

- $\texttt{Trapdoor}(\mathsf{msk}, \{Q_i\})$: Taking a single identity or a list of identities $\{Q_i\}$ as the input, where the size of $\{Q_i\}$ cannot be larger than ℓ, it uses the master secret key msk to produce a trapdoor $T_{\{Q_i\}}$, which is the private key for a single identity or an "intersection private key"' for the identities string, depending on the size of $\{Q_i\}$).
- $\texttt{Encrypt}(m, \{W_i\})$: For a plaintext message m together with a single identity or a list of targeted identities $\{W_i\}$, it produces an exclusion-intersection encryption $S_{\{W_i\}}$ of m.
- $\texttt{Decrypt}(S, T_{\{Q_i\}})$: Given a ciphertext $S_{\{W_i\}}$ encrypting m, if the identities associated with the trapdoor $T_{\{Q_i\}}$ is a subset of the targeted identities associated with $S_{\{W_i\}}$, i.e., $\{Q_i\} \subseteq \{W_i\}$, outputs m; '$\perp$' otherwise.

3.2 Security

We consider the de-facto standard of a secure identity-based encryption scheme, which is indistinguishability against adaptive chosen-ciphertext attacks. For our exclusion-intersection encryption, security is defined by the sID-IND-EIE-CCA2 game below played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup: The challenger $\mathcal{C}$ takes a security parameter k and the parameter ℓ which governs the maximum number of identities that can be associated to a user trapdoor as input, runs $\texttt{Setup}(1^{\mathsf{k}}, \ell)$ to generate common public parameters param and the master secret key msk. $\mathcal{C}$ sends param to $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can perform a polynomially (in k) bounded number of queries in an adaptive manner (that is, each query may depend on the responses to the previous queries). The types of queries allowed are described below.

- $\texttt{Trapdoor}$: $\mathcal{A}$ chooses a list of identities $\{Q_i\}$, $\mathcal{C}$ computes $\texttt{Trapdoor}(\mathsf{msk}, \{Q_i\})$ and sends the result to $\mathcal{A}$.
- $\texttt{Decrypt}$: $\mathcal{A}$ chooses a ciphertext S, $\mathcal{C}$ computes a trapdoor that can decrypt S according to the identities specified by the adversary, decrypts the ciphertext S and sends the resulting plaintext m or the symbol $\perp$ to $\mathcal{A}$.

Challenge: The adversary $\mathcal{A}$ decides when Phase 1 ends. Then, it outputs two equal length plaintexts, m_0 and m_1, and a set of identities $\{\mathsf{id}_i\}_{i\in[1,t],t\leq\ell}$ on which it wishes to be challenged. The set $\{\mathsf{id}_i\}_{i\in[1,t],t\leq\ell}$ *or a subset of it* should not appear in any $\texttt{Trapdoor}$ queries in Phase 1. The challenger $\mathcal{C}$ picks a random bit b from $\{0, 1\}$, computes $S = \texttt{Encrypt}\ (m_b, \{\mathsf{id}_i\}_{i\in[1,t],t\leq\ell})$ and returns S to $\mathcal{A}$.

Phase 2: The adversary $\mathcal{A}$ can ask a polynomially bounded number of queries adaptively again as in Phase 1 with the similar restriction on $\texttt{Trapdoor}$ query and the restriction that a $\texttt{Decrypt}$ query to obtain the plaintext for S cannot be made.

Guess: The adversary $\mathcal{A}$ has to output a guess b'. It wins the game if $b' = b$. The *advantage* of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = |2\Pr[b' = b] - 1|$ (where $\Pr[b' = b]$ denotes the probability that $b' = b$).

For our scheme, we consider a "selective-ID" (sID) variant, such that the adversary's choice of all identifiers for the challenge ciphertext must be in given before the setup of the public system parameter.

Definition 1. *An exclusion-intersection encryption scheme is said to have the indistinguishability against adaptive chosen-ciphertext attacks property if no adversary has a non-negligible advantage in the sID-IND-EIE-CCA2 game.*

4 Proposed Construction

4.1 Building Blocks

Pairings and Related Number-Theoretic Problems. Pairing is an useful number-theoretic primitive for cryptographic uses. In particular, many cryptographic access control schemes, and identity-/attribute-based encryption schemes are based on elliptic-curve pairings. Some examples include [BF03, Cho09, CHSS02, MB03, MBD03, Sma03, ARMLS06, CRR08, CY08, BSNS05, AKN08, SK03, BF06, GS02, AY07, BF05, CS06, PKL08, Del07, GPSW06, BSW07, BW07]. We describe some of the key properties of these bilinear groups and the pairing function.

Let $(\mathbb{G}_0, +)$ and $(\mathbb{G}_T, \cdot)$ be two cyclic groups of prime order p. Pairing is given as $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_T$, which satisfies the following properties:

1. *Bilinearity*: $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$ $\forall P, Q, R \in \mathbb{G}_0$.
2. *Non-degeneracy*: There exists $P, Q \in \mathbb{G}_0$ such that $\hat{e}(P, Q) \neq 1$.
3. *Computability*: It is efficient to compute $\hat{e}(P, Q)$ $\forall P, Q \in \mathbb{G}_0$.

Definition 2. *Given two groups $\mathbb{G}_0$ and $\mathbb{G}_T$ of the same prime order p, and a generator P of $\mathbb{G}_0$, the Computational/Decisional q-Bilinear Diffie-Hellman Inversion (q-BDHI) problem in $(\mathbb{G}_0, \mathbb{G}_T)$ is, given $(P, xP, x^2P, \cdots, x^qP)$ to compute $\hat{e}(P, P)^{1/x}$, or to decide if $\hat{t} = \hat{e}(P, P)^{1/x}$ when additionally given $\hat{t}$, respectively.*

We relate the decisional 1-BDHI problem and the DBDH problem defined below.

Definition 3. *Given two groups $\mathbb{G}_0$ and $\mathbb{G}_T$ of the same prime order p, a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_T$ and a generator P of $\mathbb{G}_0$, the Decisional Bilinear Diffie-Hellman (DBDH) problem in $(\mathbb{G}_0, \mathbb{G}_T)$ is to decide whether $h = \hat{e}(P, P)^{abc}$ given (P, aP, bP, cP) and an element $h \in \mathbb{G}_T$.*

Lemma 1. *DBDH problem is easy implies decisional* 1*-BDHI problem is easy.*

Proof. Proof Given $(P, xP, \hat{t}) \in \mathbb{G}_0^2 \times \mathbb{G}_T$, feed $(xP, P, P, P, \hat{t})$ into a DBDH oracle, let $R = xP$, i.e., $P = \frac{1}{x}R$, $\hat{t} = \hat{e}(P, P)^{1/x}$ if and only if $\hat{t} = \hat{e}(R, R)^{\frac{1}{x}\frac{1}{x}\frac{1}{x}}$. To see, $\hat{e}(\frac{1}{x}R, \frac{1}{x}R)^{\frac{1}{x}} = \hat{e}(P, P)^{\frac{1}{x}}$.

REACT CCA Transformation. There exists transform techniques such as [FO99] which can convert a "weakly-secure" (security against a weaker form of attack which is called chosen-plaintext attack (CPA), in which the adversary does not have access of any decryption oracle), e.g., OW-CPA or IND-CPA encryption scheme, into one that is indistinguishable against adaptive chosen-ciphertext attack (CCA). REACT [OP01] is the one we chose in our proposed construction. It is quite efficient as it just adds two more hashings to the underlying encryption and the decryption algorithm, assuming the underlying scheme is one-way against plaintext checking attack (PCA). PCA means that the adversary has access to an oracle which, on input a message/ciphertext pair (m, c), tells if c encrypts m or not.

While this oracle maybe easy to simulate for plain RSA-based cryptosystem, we often need to employ some kind of gap assumption for Diffie-Hellman-based encryption scheme, i.e., a certain computational problem is intractable even if there exists an oracle which solve the decisional version of the problem. For our reduction, the simulator just requires an oracle to solve the decisional 1-BDHI problem (instead of q-BDHI problem for $q > 1$), which can be easily solved when there is a DBDP oracle as shown by Lemma 1. We call this as the *gap* q-BDHI problem.

We stress that the actual construction does not require the DBDP oracle. We chose to use the REACT transformation for simpler design of our CCA-secure scheme. A shortcoming of this is that the security proof may not be falsifiable.

Identity Partition. As discussed in the review section, another tool we need is the concept of identity partition, such that the whole identity space is partitioned into ℓ different disjoint partitions and encryption can only be done with respect to identities which do not come from the same partition. The partition is defined by a publicly computable surjective function from an identity to a number between 1 and ℓ. While it is a restriction, we note that it is not entirely impractical; for example, a ciphertext cannot be marked as both "casual" and "urgent" at the same time.

Hash Functions. Our scheme employs the following cryptographic (collision-resistant) hash functions, which are modelled by random oracles in our security analysis:

- $H_1 : \{0, 1\}^* \to \mathbb{Z}_p$,
- $H_2 : \mathbb{G}_T \to \{0, 1\}^{|M|}$ where $|M|$ denotes the length of the message,
- $H_3 : \{0, 1\}^* \to \{0, 1\}^k$, where k is the security parameter of the scheme.

4.2 Algorithms

The key generation center executes the `Setup` algorithm at the first place. After that, it also generates on demand the trapdoor $T_{\{Q_i\}}$ for a set of identities $\{Q_i\}$ using the `Trapdoor` algorithm. Anyone can use the `Encrypt` algorithm to encrypt a message m for the appointed recipients as defined by $\{W_i\}$. Finally, the one holding the trapdoor $T_{\{Q_i\}}$ can decrypt the ciphertext if $\{Q_i\} \subseteq \{W_i\}$.

The design of our scheme is largely based on one of the public-key encryption schemes supporting conjunctive field keyword proposed by Park *et al.* [PKL04]. We use the random-looking element which determining the search result in their scheme as an one-time pad for encrypting the message in our case. Nevertheless, not every such a scheme can be easily converted to an exclusion-intersection encryption scheme. In particular, if we try to use a similar kind of transformation on another scheme [PKL04], it is not clear how all possible decryption keys can lead to the same random padding. In more details, there are an exponential number (in ℓ) of possible elements from their search algorithm, which also makes the ciphertext-size to be exponential (in ℓ, the number of identities associated with a ciphertext) in our case when these elements are used as one-time pads to encrypt the message. Moreover, as a searchable encryption, their work did not consider chosen-ciphertext security. For this we applied REACT transformation [OP01] to get this higher level of security.

– $\texttt{Setup}(1^k, \ell)$: Let p be the order of the groups $\mathbb{G}_0$ and $\mathbb{G}_T$ which is determined by the security parameter k. Let $G : \mathbb{Z}_p \to \{1, \cdots, \ell\}$ be a publicly computable surjective function which defines the partition of the identities, and let $h(\cdot) = G(H_1(\cdot))$. The algorithm chooses random numbers $y_1 \cdots, y_\ell, z_1, z_2 \in \mathbb{Z}_p$ and a generator U of $\mathbb{G}_0$. It outputs the public parameters $\mathsf{param} = \langle U, Y_1 = y_1 U, \cdots, Y_\ell = y_\ell U, Z_1 = z_1 U, Z_2 = z_2 U, \hat{g} = \hat{e}(U, U)\rangle$ and the master secret key $\mathsf{msk} = \langle y_1, \cdots, y_\ell, z_1, z_2\rangle$.

– $\texttt{Trapdoor}(\mathsf{msk}, \{Q_i\}_{i\in[1,t],t\leq\ell})$: Selects a random number $u \in \mathbb{Z}_p$ and computes $T_{\{Q_i\}_{i\in[1,t],t\leq\ell}} = \langle T_1, T_2, u\rangle$ where
  - $T_1 = (\frac{1}{y_{h(Q_1)} + \cdots + y_{h(Q_t)} + H_1(Q_1) + \cdots + H_1(Q_t) + z_2 u})U$
  - $T_2 = \frac{1}{z_1} T_1$

– $\texttt{Encrypt}(m, \{W_i\}_{i\in[1,n],n\leq\ell})$:
  1. Computes a set $\mathcal{W}' = \{h(W_1), \cdots, h(W_n)\}$.
  2. For each $j \in \mathcal{W}'$, selects a random number $r_j \in \mathbb{Z}_p$.
  3. Computes a set $\mathcal{B} = \{r_j Z_1\}$.
  4. Picks $r_0 \in \mathbb{Z}_p$ and $\hat{r} \in \mathbb{G}_T$ uniformly at random.
  5. Computes $C = r_0 Z_2$.
  6. Computes $\hat{x} = \hat{g}^{r_0} \cdot \hat{r}$.
  7. Encrypts the message by $E = m \oplus H_2(\hat{r})$.
  8. Computes a set $\mathcal{A} = \{r_0(Y_j + H_1(W_j)U) + r_j U\}$.
  9. Computes $\sigma = H_3(\hat{r}||m||\mathcal{A}||\mathcal{B}||C||E||\hat{x})$, where all the group elements are interpreted as bit strings and $||$ represents the string concatenation operator.
  10. Outputs the ciphertext as $\langle\mathcal{A} = (A_1, \cdots, A_n), \mathcal{B} = (B_1, \cdots, B_n), C, E, \hat{x}, \sigma\rangle$.

– $\texttt{Decrypt}(S = \langle A_1, \cdots, A_n, B_1, \cdots, B_n, C, E, \hat{x}, \sigma\rangle,$
$T_{\{Q_i\}} = \langle T_1, T_2, u\rangle)$:
  1. Proceeds if $\{Q_i\} \subseteq \{W_i\}$, aborts otherwise.
  2. Computes a set $\mathcal{Q}' = \{h(Q_1), \cdots, h(Q_t)\}$.

3. Computes $\hat{r}' = \hat{x}/\frac{(\hat{e}(\sum_{i\in\mathcal{Q}'} A_i)+uC,T_1)}{\hat{e}(\sum_{i\in\mathcal{Q}'} B_i,T_2)}$.
4. Recovers $m' = E \oplus H_2(\hat{r}')$.
5. If $\sigma = H_3(\hat{r}||m'||A_1||\cdots||B_1||\cdots||B_n||C||E||\hat{x})$, outputs m' which is the decrypted message; otherwise, outputs $\perp$.

4.3 Correctness

For correctness, if $\{Q_i\} \subseteq \{W_i\}$, that means $\mathcal{Q}' \subseteq \mathcal{W}'$; we have

$$\begin{aligned}
\hat{r}' &= \hat{x}/\frac{(\hat{e}(\sum_{i\in\mathcal{Q}'} A_i) + uC, T_1)}{\hat{e}(\sum_{i\in\mathcal{Q}'} B_i, T_2)} \\
&= \hat{x}/\frac{(\hat{e}(\sum_{i\in\mathcal{Q}'} A_i) + uC, T_1)}{\hat{e}(\frac{1}{z_1}\sum_{i\in\mathcal{Q}'} B_i, T_1)} \\
&= \hat{x}/\frac{(\hat{e}(\sum_{i\in\mathcal{Q}'} r_0(Y_i + H_1(W_i)U) + r_iU) + uC, T_1)}{\hat{e}(\sum_{i\in\mathcal{Q}'} r_iU, T_1)} \\
&= \hat{x}/(\hat{e}(\sum_{i\in\mathcal{Q}'} r_0(Y_i + H_1(W_i)U) + uC, T_1) \\
&= \hat{x}/(\hat{e}(\sum_{i\in\mathcal{Q}'} r_0(y_i + H_1(W_i))U + ur_0z_2U, T_1) \\
&= \hat{g}^{r_0} \cdot \hat{r}/\hat{g}^{r_0} \\
&= \hat{r}
\end{aligned}$$

4.4 Efficiency

Regarding efficiency, our scheme inherits the following benefits of Sakai-Kasahara IBE [SK03]. The admissible encoding scheme hashing to $\mathbb{G}_0$ [BF03], which may be computationally expensive in some settings, is not needed. Besides, no pairing operation is needed for the generation of trapdoor and encryption, while it only takes two pairing operations for decryption.

4.5 Security

The following theorem summarizes the security of our scheme.

Theorem 1. *In the random oracle model (the hash functions are modeled as random oracles), if we have an adversary $\mathcal{A}$ that is able to win the sID-IND-EIE-CCA2 game (i.e., $\mathcal{A}$ is able to distinguish ciphertexts given by the challenger), with an advantage ϵ when running in a time t and asking at most q_H identifier hashing queries, at most q_T trapdoor generation queries, at most q_S H_2 queries, at most q_R H_3 queries, and q_D decryption queries; there exists a simulator $\mathcal{C}$ that can solve the gap (q_T+1)-BDHI problem with non-negligible probability.*

Proof. Proof On input of $(P, xP, x^2P, \cdots, x^{q_T+1}P)$, $\mathcal{C}$'s goal is to compute $\hat{R} = \hat{e}(P,P)^{1/x}$. The adversary $\mathcal{A}$ gives a list of group identifier $\{\mathsf{id}_i^* | i \in [1,t], t \leq \ell\}$. $\mathcal{C}$ then setups the system as follows.

`Setup`:

1. Chooses ζ_1, ζ_2, $\cdots$, $\zeta_{q_T} \in_R \mathbb{Z}_p^*$.
2. Expands the term in $f(z) = \prod_{j=1}^{q_T} (z + \zeta_j)$ by $f(z) = \sum_{i=0}^{q_T} c_i z^i$.
3. Computes $U = f(x)P$ by $\sum_{i=0}^{q_T} c_i x^i P$ and $V = xU$ by $\sum_{i=1}^{q_T+1} c_{i-1} x^i P$.
4. For $1 \leq i \leq q_T$, computes $\frac{1}{x+\zeta_i} U = \frac{f(x)}{x+\zeta_i} P = \sum_{j=0}^{q_T-1} d_j x^j P$, these values will be used in handling the `Trapdoor` queries.
5. Chooses $\beta_1', \cdots, \beta_\ell'$.
6. Rearrange $\{\beta_j'\}$ as $\{\beta_j\}$ in the order of $\{G(\beta_j')\}$, i.e., $\beta_{G(\beta_j')} = \beta_j'$.
7. If duplication occurs, chooses another β' until $\beta_{G(\beta')}$ is unassigned.
8. Repeats until all of $\{\beta_j\}$ are assigned.
9. Chooses $\alpha_1, \cdots, \alpha_\ell \in_R \mathbb{Z}_p^*$, computes $Y_1 = \alpha_1 V - \beta_1 U, \cdots, Y_\ell = \alpha_\ell V - \beta_\ell U$.
10. Chooses γ_1, $\gamma_2 \in_R \mathbb{Z}_p^*$, computes $Z_1 = \gamma_1 U$ and $Z_2 = \gamma_2 V$.
11. Outputs $\mathsf{param} = [U, Y_1, \cdots, Y_\ell, Z_1, Z_2, \hat{g} = \hat{e}(U,U)]$. Notice that all parts of the corresponding master secret key $\mathsf{msk} = \langle y_1 = \alpha_1 x - \beta_1, \cdots, y_\ell = \alpha_\ell x - \beta_\ell, z_1 = \gamma_1, z_2 = \gamma_2 x \rangle)$ are unknown to $\mathcal{C}$ except z_1.

(The selection of $\{\beta_j\}$ are restricted by the function $G(\cdot)$ such that $G(\beta_j) = j$, but random $\{\alpha_j\}$ makes $\{Y_j\}$ indistinguishable from the real distribution.)

H_1 queries: Roughly speaking, these answers are randomly generated, but to maintain the consistency, $\mathcal{C}$ keeps the list L_1 to store the answers used (i.e., the same answer will be returned if the query has been made before). If W_i is not in the set given by the adversary, randomly chooses $h_i \in_R \mathbb{Z}_p^*$; otherwise set $h_i = \beta_j$ where β_j has not been assigned as the output of H_1 for any previous queries. For either way, return h_i as the answer and store $\langle W_i, h_i \rangle$ in list L_1.

H_2 and H_3 queries: When $\mathcal{A}$ asks queries on these hash values, $\mathcal{C}$ checks the respective list L_2 or L_3. If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a randomly generated value will be used as an answer to $\mathcal{A}$, the query and the answer will then be stored in the list.

`Trapdoor` queries: For the j-th time, suppose $\mathcal{A}$ asks for the trapdoor corresponding to the group $\{Q_i\}_{i \in [1,t], t \leq \ell} = \{Q_1, Q_2, \cdots, Q_t\}$.

1. Gets the entries $\{\langle Q_i, h_i, c_i \rangle\}$ in L_1, if $c_i = 0\ \forall i$, aborts the simulation.
2. Computes $e_i = y_{h(Q_1)} + \cdots + y_{h(Q_t)} + h_1 + h_2 + \cdots + h_t = (\alpha_{h(Q_1)} + \cdots + \alpha_{h(Q_t)})x + (h_1 + h_2 + \cdots + h_t) - (\beta_{h(Q_1)} + \cdots + \beta_{h(Q_t)})$. For simplicity, let $\alpha^* = (\alpha_{h(Q_1)} + \cdots + \alpha_{h(Q_t)})$ and $\beta^* = (h_1 + h_2 + \cdots + h_t) - (\beta_{h(Q_1)} + \cdots + \beta_{h(Q_t)})$, so e_i can be expressed as $\alpha^* x + \beta^*$, for known α^*, β^*. Furthermore, since $\exists i$ such that $c_i = 1$, $\beta^* \neq 0$.
3. Picks j-th pair $(\zeta_j, \frac{1}{x+\zeta_j} U)$ generated at the `Setup` phase.
4. Computes $v_j = \beta^* / \zeta_j$ and $u_j = (v_j - \alpha^*)/\gamma_2$ (such that the equation $\frac{1}{v_j(x+\zeta_j)} = \frac{1}{\alpha^* x + \beta^* + \gamma_2 x u_j}$ holds).

5. Computes $F_j = \frac{1}{v_j(x+\zeta_j)}U$ ($v_j \neq 0$ since $\beta^* \neq 0$).
6. Outputs $[F_j, \frac{1}{\gamma_1}F_j, u_j]$ (which is a valid trapdoor since $\frac{1}{\alpha^* x+\beta^*+\gamma_2 x u_j} = \frac{1}{e_j+z_2 u_j}$).

`Decrypt` queries: Suppose $\mathcal{A}$ asks for the decryption of the ciphertext $S_i = \langle A_1, A_2, \cdots, A_n, B_1, B_2, \cdots, B_n, C, E, \hat{x}, \sigma\rangle$, and $I_1, I_2, \cdots, I_t$ are the positions of the groups from $\{Q_i\}$ which are also in the list $\{W_i\}$. For $i \in \{I_1, I_2, \cdots, I_t\}$ corresponding to the group $\{Q_1, Q_2, \cdots, Q_t\}$, $t \leq \ell$.

1. Gets the entries $\{\langle Q_i, h_i, c_i\rangle\}$ in L_1, if there exists i such that $c_i = 1$, generates the trapdoor using the above simulation and decrypts S_i.
2. Otherwise, $\forall i, c_i = 0$, $A_i = r_0(Y_i + h_i U) + r_i U$ is thus in the form of $r_0(\alpha_i V - h_i U + h_i U) + r_i U = r_0 \alpha_i V + r_i U$.
3. For a valid ciphertext, $B_i = r_i Z_1$ and $C = r_0 Z_2$. Since γ_1 and γ_2 in $Z_1 = \gamma_1 U$ and $Z_2 = \gamma_2 V$ are known, $\mathcal{C}$ can get $r_0 \alpha_i V = r_0 \alpha_i x U$ from $A_i - \frac{1}{\gamma_1}B_i$ and check if $\langle A_1, A_2, \cdots, A_n, B_1, B_2, \cdots, B_n, C\rangle$ is consistent. Returns $\perp$ if not.
4. Looks up in L_3 for entry which defines the relation $\sigma = H_3(\hat{r}||m'||A_1||\cdots||B_n||C||E||\hat{x})$ for some message m' such that there exists an entry $E \oplus m' = H_2(\hat{r})$ in L_2.
5. If such entry is found, feeds $(U, xU, r_0 x U, \hat{r})$ to the decisional 1-BDHI oracle (to see if $\hat{r} = \hat{e}(U,U)^{\frac{1}{x}}$) outputs m' if the oracle returns true; $\perp$ otherwise.

Challenge: Eventually adversary $\mathcal{A}$ produces a pair of message m_0, m_1 on which it wishes to be challenged. The challenge ciphertext is generated as follows.

1. Picks a random bit b.
2. Gets $\{\langle \mathsf{id}_i^*, h_i, c_i\rangle\}$ from list L_1.
3. Selects random ρ, $r_1, \cdots, r_m \in \mathbb{Z}_p$.
4. Computes $C = (\rho/x)Z_2$ (i.e., $r_0 = \rho/x$),
5. Computes $A_i = \rho\alpha_i U + r_i U$ and $B_i = r_i Z_1$ for $1 \leq i \leq t$
($\forall i$, $A_i = r_0(Y_i + h_i U) + r_i U = r_0(\alpha_i x - \beta_i + \beta_i)U + r_i U$),
6. Picks $\hat{r}, \hat{x} \in_R \mathbb{G}_T$, $m' \in \{0,1\}^{|M|}$, $\sigma \in_R \{0,1\}^k$ and computes $E = m_b \oplus m'$.
7. Outputs $\langle A_1, \cdots, A_n, B_1, \cdots, B_n, C, E, \hat{x}, \sigma\rangle$.

It is easy to see that the ciphertext is valid except the terms E and σ. Notice that $\mathcal{C}$ does not know the randomness “r_0'' associated with this ciphertext, which may make the simulation of H_2 unfaithful if the adversary asks for $H_2(\hat{e}(U,U)^{\rho/x})$ (and a similar H_3 query corresponding to the challenge ciphertext). However, since ρ is chosen at random, it is of negligible probability that $\mathcal{A}$ has made such queries before it sees the ciphertext. After the challenge ciphertext is given, if $\mathcal{A}$ made such queries, $\mathcal{C}$ can solve the underlying hard problem as shown below.

Output: Finally $\mathcal{A}$ outputs a bit b'. Since m_b is perfectly hidden, any non-negligible advantage of $\mathcal{A}$ in winning this game must come from that fact that it has queried $H_3(\hat{r}||m_b||\cdots)$. $\mathcal{C}$ thus retrieves such $\hat{r}$. Note that $\hat{e}(U,U)^{1/x} = (\hat{e}(P,P)^{1/x})^{c_0^2} \cdot \hat{e}(\sum_{i=0}^{q_T} c_i x^i P, \sum_{i=0}^{q_T-1} c_{i+1} x^i P)$, hence the answer of the q-BDHI problem is $(\hat{r}^{1/\rho}/\hat{e}(\sum_{i=0}^{q_T} c_i x^i P, \sum_{i=0}^{q_T-1} c_{i+1} x^i P)^{1/c_0^2}$.

□

5 Exclusion-Intersection Encryption with Efficient Online Encryption

The idea of splitting the encryption process into offline and online phases is the same as that employed by [GMC08] and [CLZ11]. However, instead of using n parallel invocations, we make the observation that one of the random factor can be re-used.

5.1 Algorithms

- `Setup`, `Trapdoor` remain the same.
- $\texttt{Encrypt}^{\texttt{Off}}(n)$:
  1. Randomly choose $r_1, \cdots, r_n \in \mathbb{Z}_p^n$.
  2. Computes a set $\mathcal{B} = \{r_j Z_1\}$.
  3. Picks $r_0 \in \mathbb{Z}_p$ and $\hat{r} \in \mathbb{G}_T$ uniformly at random.
  4. Computes $C = r_0 Z_2$.
  5. Computes $\hat{x} = \hat{g}^{r_0} \cdot \hat{r}$.
  6. Computes $K = H_2(\hat{r})$.
  7. Randomly choose $\pi_1, \cdots, \pi_n \in \mathbb{Z}_p^\ell$.
  8. Computes a set $\mathcal{A} = \{r_0(Y_j + \pi_j U) + r_j U\}$.
  9. Randomly choose $\phi \in \mathbb{Z}_p$.
  10. Computes $F = r_0 \phi U$.
  11. Outputs the offline ciphertext as $\langle \mathcal{A}' = (A'_1, \cdots, A'_n), \mathcal{B} = (B_1, \cdots, B_n), C, K, F, \hat{x} \rangle$.
- $\texttt{Encrypt}^{\texttt{On}}(\langle \mathcal{A}', \mathcal{B}, C, K, \hat{x} \rangle, m, \{W_i\}_{i \in [1,n], n \leq \ell})$:
  1. Computes a set $\mathcal{W}' = \{h(W_1), \cdots, h(W_n)\}$.
  2. Computes a set $\mathcal{T} = \{\phi^{-1}(h(W_j) - \pi)\}$.
  3. Computes $E = m \oplus K$.
  4. Computes $\sigma = H_3(\hat{r}||m||F||\mathcal{T}||\mathcal{A}||\mathcal{B}||C||E||\hat{x})$, where all the group elements are interpreted as bit strings and $||$ represents the string concatenation operator.
  5. Outputs the ciphertext as
     $\langle F, \mathcal{T} = (t_1, \cdots, t_n), \mathcal{A}' = (A'_1, \cdots, A'_n), \mathcal{B} = (B_1, \cdots, B_n), C, E, \hat{x}, \sigma \rangle$.
- $\texttt{Decrypt}(S = \langle F, \mathcal{T} = (t_1, \cdots, t_n), \mathcal{A}' = (A'_1, \cdots, A'_n), \mathcal{B} = (B_1, \cdots, B_n), C, E, \hat{x}, \sigma \rangle,$ $T_{\{Q_i\}} = \langle T_1, T_2, u \rangle)$:
  1. Proceeds if $\{Q_i\} \subseteq \{W_i\}$, aborts otherwise.
  2. Computes a set $\mathcal{Q}' = \{h(Q_1), \cdots, h(Q_t)\}$.
  3. Computes $\hat{r}' = \hat{x} / \frac{(\hat{e}(\sum_{i \in \mathcal{Q}'} A'_i + t_i F) + uC, T_1)}{\hat{e}(\sum_{i \in \mathcal{Q}'} B_i, T_2)}$.
  4. Recovers $m' = E \oplus H_2(\hat{r}')$.
  5. If $\sigma = H_3(\hat{r}||m'||F||\mathcal{T}||\mathcal{A}||\mathcal{B}||C||E||\hat{x})$, outputs m' which is the decrypted message; otherwise, outputs $\perp$.

5.2 Correctness

The correctness boils down to the following equations:

$$\begin{aligned}&A'_i + t_i F \\ &= r_0(Y_j + \pi_j U) + r_j U + \phi^{-1}(h(W_j) - \pi_j)(r_0 \phi U) \\ &= r_0(Y_j + \pi_j U) + r_j U + r_0(h(W_j) - \pi_j)U \\ &= r_0(Y_j + h(W_j)U) + r_j U\end{aligned}$$

5.3 Security

Security of the online/offline version can be easily established by simulating the new ciphertext structure by a standard ciphertext as follows. Firstly, the input materials of the hash function H_3 for the new ciphertext uniquely determine a standard ciphertext, and hence it does not affect the simulation in the random oracle model. Furthermore, we can pick a random group element F, many random t_j's, and define $A'_j = A_j - t_i F$. This can be simulated without any secret knowledge, such as any trapdoor or the randomness in encryption.

6 Conclusion

We introduce the notion of *Exclusion-Intersection Encryption*, with a concrete construction, which provides a flexible solution for the access control of the plaintext message encrypted in a ciphertext. We argue that exclusion-intersection encryption maybe more suitable than traditional PKI-based schemes, hierarchical identity-based encryption schemes or attribute-based encryption schemes, for scenarios where ad-hoc collaborative group work are often and compact private keys are desirable. The security of our scheme is asserted in the random oracle model, assuming the hardness of the gap q-bilinear Diffie-Hellman inversion problem. We believe that exclusion-intersection encryption will give rise to other innovative applications other than those we described. We left as open problems to construct an exclusion-intersection encryption scheme which either works without identity-partition or is secure without random oracles.

Acknowledgement

The authors would like to thank the anonymous reviewers for their useful comments. Thanks also go to Pierre K.Y. Lai for her help in the preparation of a preliminary version of this paper, and Boris W.S. Yiu for naming the proposed notion. Last but not the least, thanks to Yang Xiao for his help during the preparation of the journal version.

Bibliography

[AKN08] Michel Abdalla, Eike Kiltz, and Gregory Neven. Generalized Key Delegation for Hierarchical Identity-Based Encryption. *IET Information Security*, 2(3):67–78, 2008.

[ARMLS06] Sattam S. Al-Riyami, John Malone-Lee, and Nigel P. Smart. Escrow-free Encryption supporting Cryptographic Workflow. *Intl. J. of Information Security*, 5(4):217–229, 2006.

[AY07] Man Ho Au and Siu-Ming Yiu. Structural Identity-Based Encryption. Cryptology ePrint Archive, Report 2007/422, 2007. `http://eprint.iacr.org/`.

[BF03] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM J. Computing*, 32(3):586–615, 2003.

[BF05] Manuel Barbosa and Pooya Farshim. Efficient Identity-Based Key Encapsulation to Multiple Parties. In Nigel P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 428–441. Springer, 2005.

[BF06] Manuel Barbosa and Pooya Farshim. Secure Cryptographic Workflow in the Standard Model. In Rana Barua and Tanja Lange, editors, *INDOCRYPT*, volume 4329 of *Lecture Notes in Computer Science*, pages 379–393. Springer, 2006.

[BSNS05] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption. In Serge Vaudenay, editor, *Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 380–397. Springer, 2005.

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In *IEEE Symposium on Security and Privacy, Oakland, California, USA*, pages 321–334. IEEE Computer Society, 2007.

[BW07] Dan Boneh and Brent Waters. Conjunctive, Subset, and Range Queries on Encrypted Data. In Salil P. Vadhan, editor, *TCC*, volume 4392 of *Lecture Notes in Computer Science*, pages 535–554. Springer, 2007.

[CC09] Melissa Chase and Sherman S. M. Chow. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *ACM Conference on Computer and Communications Security, Chicago, Illinois, USA*, pages 121–130. ACM, 2009.

[Cho09] Sherman S. M. Chow. Removing Escrow from Identity-Based Encryption. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 256–276. Springer, 2009.

[CHSS02] Liqun Chen, Keith Harrison, David Soldera, and Nigel P. Smart. Applications of Multiple Trust Authorities in Pairing Based Cryptosystems. In George I. Davida, Yair Frankel, and Owen Rees, editors, *InfraSec*, volume 2437 of *Lecture Notes in Computer Science*, pages 260–275. Springer, 2002.

[CLZ11] Sherman S. M. Chow, Joseph K. Liu, and Jianying Zhou. Identity-based online/offline key encapsulation and encryption. In Ravi Sandhu and Duncan S. Wong, editors, *ASIACCS*, pages 52–60. ACM, 2011.

[CRR08] Sherman S. M. Chow, Volker Roth, and Eleanor G. Rieffel. General Certificateless Encryption and Timed-Release Encryption. In Rafail Ostrovsky, Roberto De Prisco, and Ivan Visconti, editors, *SCN*, volume 5229 of *Lecture Notes in Computer Science*, pages 126–143. Springer, 2008.

[CS06] Sanjit Chatterjee and Palash Sarkar. Multi-Receiver Identity-Based Key Encapsulation with Shortened Ciphertext. In Rana Barua and Tanja Lange, editors, *INDOCRYPT*, volume 4329 of *Lecture Notes in Computer Science*, pages 394–408. Springer, 2006.

[CY08] Sherman S. M. Chow and Siu-Ming Yiu. Timed-Release Encryption Revisited. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *ProvSec*, volume 5324 of *Lecture Notes in Computer Science*, pages 38–51. Springer, 2008.

[Del07] Cécile Delerablée. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In Kaoru Kurosawa, editor, *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 200–215. Springer, 2007.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In Michael J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554. Springer, 1999.

[GMC08] Fuchun Guo, Yi Mu, and Zhide Chen. Identity-Based Online/Offline Encryption. In Gene Tsudik, editor, *Financial Cryptography*, volume 5143 of *Lecture Notes in Computer Science*, pages 247–261. Springer, 2008.

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security*, pages 89–98. ACM, 2006.

[GS02] Craig Gentry and Alice Silverberg. Hierarchical ID-Based Cryptography. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.

[IP08] Vincenzo Iovino and Giuseppe Persiano. Hidden-Vector Encryption with Groups of Prime Order. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing*, volume 5209 of *Lecture Notes in Computer Science*, pages 75–88. Springer, 2008.

[LP07] Hoon Wei Lim and Kenneth G. Paterson. Multi-Key Hierarchical Identity-Based Signatures. In Steven D. Galbraith, editor, *IMA Int. Conf.*, volume 4887 of *Lecture Notes in Computer Science*, pages 384–402. Springer, 2007.

[MB03] Marco Casassa Mont and Pete Bramhall. IBE Applied to Privacy and Identity Management. Technical Report HPL-2003-101, HP Labs., 2003.

[MBD03] Marco Casassa Mont, Pete Bramhall, and Chris R. Dalton. A Flexible Role-Based Secure Messaging Service: Exploiting IBE Technology in a Health Care Trial. Technical Report HPL-2003-21, HP Labs, 2003.

[OP01] Tatsuaki Okamoto and David Pointcheval. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. In David Naccache, editor, *CT-RSA*, volume 2020 of *Lecture Notes in Computer Science*, pages 159–175. Springer, 2001.

[PKL04] Dong Jin Park, Kihyun Kim, and Pil Joong Lee. Public Key Encryption with Conjunctive Field Keyword Search. In Chae Hoon Lim and Moti Yung, editors, *WISA*, volume 3325 of *Lecture Notes in Computer Science*, pages 73–86. Springer, 2004.

[PKL08] Jong Hwan Park, Ki Tak Kim, and Dong Hoon Lee. Cryptanalysis and Improvement of a Multi-Receiver Identity-Based Key Encapsulation at INDOCRYPT 06. In Masayuki Abe and Virgil D. Gligor, editors, *ASIACCS*, pages 373–380. ACM, 2008.

[SK03] Ryuichi Sakai and Masao Kasahara. ID based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive, Report 2003/054, 2003.

[Sma03] Nigel P. Smart. Access Control Using Pairing Based Cryptography. In Marc Joye, editor, *CT-RSA*, volume 2612 of *Lecture Notes in Computer Science*, pages 111–121. Springer, 2003.