A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing

Zhiguang Qin*, Hu Xiong*,†, Shikun Wu, and Jennifer Batamuliza

***Abstract*—Never before have data sharing been more convenient with the rapid development and wide adoption of cloud computing. However, how to ensure the cloud user's data security is becoming the main obstacles that hinder cloud computing from extensive adoption. Proxy re-encryption serves as a promising solution to secure the data sharing in the cloud computing. It enables a data owner to encrypt shared data in cloud under its own public key, which is further transformed by a semi-trusted cloud server into an encryption intended for the legitimate recipient for access control. This paper gives a solid and inspiring survey of proxy re-encryption from different perspectives to offer a better understanding of this primitive. In particular, we reviewed the state-of-the-art of the proxy re-encryption by investigating the design philosophy, examining the security models and comparing the efficiency and security proofs of existing schemes. Furthermore, the potential applications and extensions of proxy re-encryption have also been discussed. Finally, this paper is concluded with a summary of the possible future work.**

***Index Terms*—Proxy Re-Encryption, Data Sharing, Security, Cloud Computing.**

I. Introduction

THE rapid development and wide adoption of cloud computing have brought convenience for data storage and sharing [1]. As a representative example, a government agency enables its employees in the same group to outsource and share files in the public cloud. Fueled by the cloud computing, the employees in the same group can access the shared data uploaded by the other members of the group without huge capital investments in local storage deployment and maintenance. Furthermore, the sharing data stored in the cloud can be accessed by any member in the group at any time from any place provided this member can access the Internet. In spite of tremendous benefits, data sharing in cloud computing is depriving user's direct control over the outsourced data, which inevitably raises security concerns and challenges [2, 3]. Specifically, the outsourced data containing sensitive information should only be accessed by the authorized users. Encryption is a special kind of cryptographic technology that enforces access control over encrypted data [4]. It can protect sensitive data that is outsourced in the cloud server as long as the data has been encrypted by the data owner before uploading to the semi-trusted cloud. One promising approach to protect the security of the data stored in cloud computing is to encrypt these data with normal asymmetric encryption owning to the elimination of cumbersome key management in the symmetric encryption. To share storage with many other members in the group, the data owner needs to download and decrypt the requested data, and further re-encrypt it under the target user's public key. In this way, normal public key encryption cannot be regarded as the best candidate to achieve the goal of confidentiality since extra computation cost and communication overhead have been introduced to the data owner, which contradicts the motivation of cloud computing. Another way to think of is to allow data owners to define access policies and encrypt the sharing data with the attribute-based encryption under the access policies where only authenticated users whose attributes matching these policies can decrypt the ciphertext [5]. However, the data owner also needs to download, decrypt and re-encrypt the requested data in case data access policies change dynamically and frequently.

Proxy re-encryption (PRE), initially introduced by Blaze, Bleumer and Strauss [6], enables a semi-trusted proxy to transform a ciphertext encrypted under the public key of delegator into another ciphertext under the public key of delegatee without leaking the underlying encrypted messages or private keys of delegator/delegatee to the proxy. This special kind of public key encryption seems to be an optimal candidate to ensure the security of sharing data in cloud computing. Suppose the data owner (say, Alice) intends to share the sensitive data stored in the cloud with another granted user (say, Bob). It is desirable that the requested data can be accessed by nobody other than Bob. Inspired by the primitive of PRE, Alice can encrypt the sensitive data under her own public key before uploading the shared data to the semi-trusted cloud. After receiving the request of data sharing from Bob, Alice generates a proxy re-encryption key using her own private key and Bob's public key, and sends this proxy re-encryption key to the semi-trusted cloud server. Equipped with this proxy re-encryption key, cloud server can transform the ciphertext encrypted under the public key of Alice into an encryption under the public key of Bob. By utilizing the PRE primitive, the transformed ciphertext can only be decrypted by Bob whereas the cloud server is unable to learn the plaintext or private keys of Alice or Bob. Finally, Bob can download and decrypt the requested data with his own private key. In this way, the costly burden of secure data sharing can be offloaded to the semi-trusted cloud server with abundant resources. An example of secure data sharing based on PRE is illustrated in Fig. 1.

† Hu Xiong is the corresponding author.
* Authors equally contributed to this work.
Z. Qin, H. Xiong, S. Wu and J. Batamuliza are with the School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China, 610054.
Hu Xiong is also with State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China.
E-mail: xionghu.uestc@gmail.com
Manuscript received April 19, 2015; revised September 17, 2015.

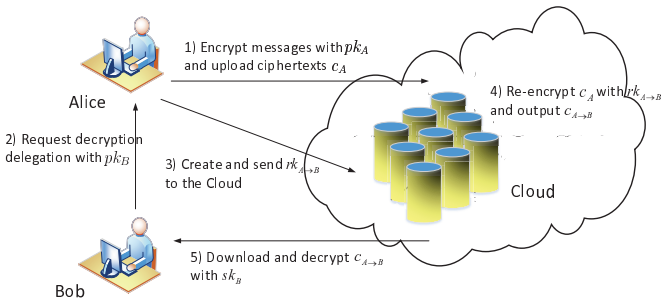

Fig. 1. Secure Data Sharing with PRE in Cloud Computing.

Featured with the specific translation property, proxy re-encryption has attracted a lot of attentions from industry and research community since its introduction in [6]. In addition to secure data sharing in the cloud computation, PRE has also found many applications ranging from digital right management (DRM) [7, 8], vehicular ad hoc networks (VANETs) [9, 10], encrypted email forwarding [6], group key management [11] to distributed system [12, 13]. Furthermore, new definitions, security models, concrete constructions and extensions of PRE have also been suggested so far. By considering the fruitful achievements in this field, it is non-trivial for the researchers to obtain a comprehensive overview of this research direction from the scattered literature. To fill this gap, a solid survey of PRE from a number of perspectives has been presented to facilitate a global view and offer researchers with a better understanding of this primitive. In particular, we first examine the existing security models for PRE in terms of the oracles available to the adversary during the security game, and survey the existing PRE schemes with respect to their security models, properties and efficiency. We also investigate the pros and cons of the available constructions of PRE in the current literature by surveying the literature over the period 1998-2015 and comprehensively reviewing the developments in this area. We then provide a description of several typical PRE schemes paired with the investigation of design philosophy behind them. We also describe the extensions of PRE along with their applications in different scenarios.

II. Definitions and Security Models for Proxy Re-Encryption

In this section we first formalize the syntax for PRE scheme, and examine the various security models proposed for PRE schemes with respect to the oracles available to the adversary. Furthermore, we survey the properties of PRE schemes to evaluate the advantages and drawbacks of existing constructions.

A. Syntax of PRE Schemes

Despite the notion of PRE has been initialized by Blaze *et al.* [6] in 1998, the formal definition and security model for the PRE scheme has been given by Ateniese and Hamburger [14] until 2005. By incorporating the definitions by Ateniese *et al.* [12, 13] and Canetti *et al.* [15], the syntax for PRE is defined as follows.

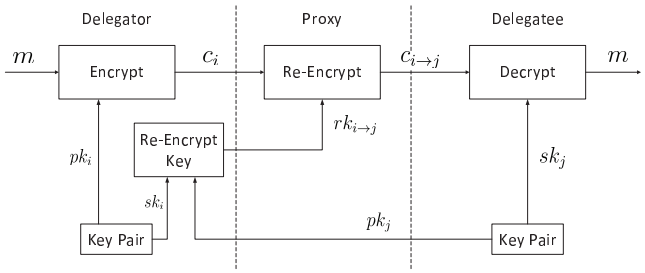

Fig. 2. The intuition of Proxy Re-Encryption Primitive.

Definition 1 (Proxy Re-Encryption): A proxy re-encryption scheme is defined by the following randomized algorithms.

- KeyGen: On input the security parameter $k \in \mathbb{K}$, the key generation algorithm KeyGen outputs a public/private key pair (pk, sk).
- ReKey: On input a key pair (pk_i, sk_i) for user i and a key pair (pk_j, sk_j) for user j (sk_j is optional), the re-encryption key generation algorithm ReKey is performed by user i to output a re-encryption key $rk_{i\to j}$. In this case, user i acts as the delegator and user j acts as the delegatee.
- Encrypt: On input a plaintext message $m \in \mathcal{M}$ and a public key pk_i for user i, the encryption algorithm Encrypt outputs an original ciphertext $c_i \in \mathcal{C}_1$.
- ReEncrypt: On input a ciphertext $c_i \in \mathcal{C}_1$ for user i and a re-encryption key $rk_{i\to j}$ for $i \to j$, the re-encryption algorithm ReEncrypt is performed by the proxy to return a transformed ciphertext $c_j \in \mathcal{C}_2$ for user j or the error symbol $\perp$ indicating c_i is invalid.
- Decrypt: On input a private key sk_i and a ciphertext $c_i \in \mathcal{C}_l (l \in \{1, 2\})$ for user i, the decryption algorithm Decrypt is performed by user i to output the corresponding plaintext message $m \in \mathcal{M}$ or a error symbol $\perp$ indicating c_i is invalid.

Correctness. Typically, the algorithms of KeyGen, Encrypt and Decrypt in PRE scheme are identical to those of normal public key encryption. For any plaintext $m \in \mathcal{M}$ and two public/private key pairs $(pk_i, sk_i), (pk_j, sk_j) \leftarrow \mathsf{KeyGen}(k)$, the correctness of a proxy re-encryption scheme requires that the following equations hold with probability one:

$$\mathsf{Decrypt}(sk_i, \mathsf{Encrypt}(pk_i, m)) = m,$$
$$\mathsf{Decrypt}(sk_j, \mathsf{ReEncrypt}(\mathsf{ReKey}(pk_i, sk_i, pk_j, sk_j), \mathsf{Encrypt}(pk_i, m))) = m.$$

As shown in Fig. 2, the aforementioned PRE enables the proxy using a re-encryption key $rk_{i\to j}$ to transform a ciphertext c_i for user i under the public key pk_i into another ciphertext c_j for user j under the public key pk_j on the same message $m \in \mathcal{M}$. Then user j is able to obtain the plaintext message *m* with his/her private key sk_j. During the execution of a secure PRE scheme, an attacker (e.g. the proxy)

cannot learn any information such as the underlying encrypted message $m \in \mathcal{M}$ or private keys (e.g. sk_i or sk_j).

B. Properties

To get a sense of the benefits and drawbacks we expect out of a PRE scheme, the most desirable properties of PRE scheme are listed as follows [12, 13].

1) Unidirectional/Bidirectional: The PRE scheme is regarded as unidirectional such that the proxy is only allowed to translate the delegator's ciphertext into the delegatee's ciphertext on the same message but not vice versa. On the contrary, a bidirectional PRE scheme enables the proxy equipped the re-encryption key to transform not only the delegator's ciphertext into the delegatee's ciphertext on the same message but also vice versa. One notable difference between the unidirectional and bidirectional PRE scheme relies on the fact that whether the delegatee's private key is involved in the re-encryption key generation algorithm ReKey or not. Specifically, the *bidirectional* PRE scheme require that both the delegator (user i) and delegatee (user j) must provide their secret keys sk_i and sk_j to generate the re-encryption key $rk_{i\rightarrow j}$, whereas only the delegator (user i)'s private key sk_i is involved to generate the transformation key in the *unidirectional* PRE scheme.

2) Multi-use/Single-use: In a multi-use PRE scheme, ciphertexts generated by either the Encrypt algorithm or ReEncrypt algorithm can be taken as input to ReEncrypt to be re-encrypted. In contrast, only the original ciphertexts generated by Encrypt can be re-encrypted by performing the ReEncrypt algorithm in the single-use PRE scheme.

3) Key-privacy: In a key-private PRE scheme, even the proxy performing the translations is unable to disclose the identities of the delegator and delegatee from transformation keys or ciphertexts. In other words, the PRE is considered to achieve ciphertext anonymity (a.k.a key privacy) if the malicious proxy and colluding users cannot identify the sender or receiver by observing sufficient re-encryption keys or ciphertexts.

4) Transparent: In a transparent PRE, neither the delegator or the delegatee is able to be aware of the existence of the proxy. More formally, it is impossible for any delegatee to distinguish an original encryption computed under his public key using the Encrypt algorithm from a re-encryption ciphertext on the same message generated by the proxy as the output of the ReEncrypt algorithm. Notably, the input and the corresponding output of the ReEncrypt algorithm in the transparent PRE scheme cannot be linked to each other.

5) Key-optimal: A user (i.e., the delegator or delegatee) is only required to protect and store a small constant number of secret data (i.e., private keys) regardless of how many decryption delegations he/she delegates or accepts. Moreover, the size and number of keys that the proxy is required to safeguard should also remain constant. The purpose of this property is to minimize the safe storage cost for each entity involved in the PRE scheme.

6) Non-interactive: If the secret key sk_j of the delegatee (user j) is not required in the re-encryption key generation algorithm ReKey, then the underlying PRE scheme is regarded to be *non-interactive*. That is to say, a re-encryption key $rk_{i\rightarrow j}$ can be generated with the delegator's private/public key pair (sk_i, pk_j) and the delegatee's public key pk_j. I.e., the private key sk_j of the delegatee (user j) is not required as the input of the algorithm ReKey.

7) Non-transitive: The PRE scheme is called to be *non-transitive* if the decryption rights cannot be redelegated by the proxy along. Formally speaking, it is infeasible for the proxy to calculate $rk_{i\rightarrow k}$ from $rk_{i\rightarrow j}$ and $rk_{j\rightarrow k}$.

8) Temporary: To deal with the case where the delegator needs to revoke the delegated decryption rights, it is desirable to equip the PRE with the temporary property such that the re-encryption right for the proxy and the decryption right for the delegatee can be deleted according to the request of delegator. It means that the delegator always has power to revoke the delegated right by updating the global parameter or issuing appropriate instructions to the proxy.

9) Collusion-resistant: In a collusion-resistant PRE scheme, even the proxy colluding with the delegatee cannot recover the delegator's private key. Otherwise, the private key of the user will be disclosed in case this user delegates its decryption rights to the malicious proxy and participants.

Indeed, there are variant definitions of syntax for PRE schemes, such as the one from Ateniese *et al.* [12] where sets of Encrypt and Decrypt algorithms instead of single Encrypt and Decrypt algorithms are defined. In this case, these algorithms are defined over different ciphertext spaces ($\mathcal{C}_1 \neq \mathcal{C}_2$) [16, 17], where the re-encryption function transforms ciphertexts from one space to another, as opposed to the case of a single ciphertext space ($\mathcal{C}_1 = \mathcal{C}_2$) [6, 15, 18], where re-encryption maintains the same space. The former syntax is usually associated with multi-use PRE schemes in spite of some recent single-use schemes are constructed based on the latter syntax [18, 19]. The latter syntax is typically associated with unidirectional PRE schemes where there may be only one direction transformations between ciphertext spaces. It is natural to observe that the syntax of PRE scheme can be adapted dynamically according to the properties featured with the PRE scheme.

C. Security Models

In normal public key encryption environment, security definitions are generally developed from the antagonistic relationship between a security goal and an adversary with a specific attack. With the indistinguishability of encryptions (IND) goal and three attacks (chosen-plaintext attack (CPA), non-adaptive chosen-ciphertext attack (CCA1) and adaptive chosen-ciphertext attack (CCA2)), three security models are usually taken into consideration: IND-CPA security, IND-CCA1 security and IND-CCA2 security [20]. Due to the fact that the PRE is one special kind of public key encryption cryptosystem, PRE schemes are also expected to offer IND-CPA security [12], IND-CCA1 security [18] and IND-CCA2 security [15]. This subsection attempts to offer definitional union for PRE by presenting a family of attack models which captures the nature of CCA-security associated with PRE schemes and avoid the security definitions that are particular for each PRE subclass.

However, the security definitions for PRE schemes inherited from normal public key encryption cause some subtle variations and restrictions due to the introduction of re-encryption capability in PRE schemes. Distinct from the security definitions for normal public key encryption scheme, an additional re-encryption oracle $\mathcal{O}_{reenc}$ can be accessed by the adversary to capture the re-encryption capability. Thus, different levels to access the decryption oracle $\mathcal{O}_{dec}$ and re-encryption oracle $\mathcal{O}_{reenc}$ result in different attack models. In this survey, we will restrict ourselves to the indistinguishability goal and further discuss different chosen-ciphertext attack models for PRE schemes on the basis of the availability of the decryption oracle $\mathcal{O}_{dec}$ and re-encryption oracle $\mathcal{O}_{reenc}$ in each phase of the security game [21].

Despite the re-encryption capabilities can be simulated by the re-encryption oracle $\mathcal{O}_{reenc}$, accessing to this oracle without any restriction is not sufficient for the adversary to obtain proper re-encryption capability. In an effort to avoid the trivial success for the adversary, the definition of the re-encryption oracle must contain some restrictions. Particularly, any ciphertext that is not derived from the challenge ciphertext can be re-encrypted by the oracle $\mathcal{O}_{reenc}$ between any pair of users, including the target user. Otherwise, the security model would be too restrictive, which results in weaker security notions [15]. Therefore, it is important that the attack models for PRE schemes are associated with a reasonable definition of the oracles available along with corresponding restrictions.

1) Oracles: As mentioned before, the security game without any restriction would enable trivial attacks from the adversary since a decryption oracle can be simulated by a re-encryption oracle. That means the challenge ciphertext c^* can be re-encrypted from the target public key pk^* to any corrupted public key pk_{cor}. To shape the restrictions, the concept of derivatives of the challenge ciphertext was presented by Canetti and Hohenberger [15] in their CCA2 security model for bidirectional and multi-use PRE scheme. Informally speaking, the derivatives of the challenge ciphertext refer to those pairs (pk, c) connected with the pair (pk^*, c^*) obtained from the queries to the re-encryption oracle $\mathcal{O}_{reenc}$ and re-encryption key generation $\mathcal{O}_{rk}$. It is obvious that the derivatives of the challenge ciphertext allow the trivial success of the adversary and thus, this notion defined in [15] is adapted here to shape the restrictions of re-encryption oracle.

Definition 2: Derivatives of the challenge ciphertext (pk^*, c^*) is defined as follows:

- The challenge ciphertext (pk^*, c^*) is a derivative of itself.
- A pair (pk_j, c_j) is a derivative of the challenge (pk^*, c^*) if (pk_j, c_j) is a derivative of (pk_i, c_i) and (pk_i, c_i) is also a derivative of (pk^*, c^*).
- If a triple (pk_i, pk_j, c_i) has been queried to a re-encryption oracle by the adversary, who in turn obtains a re-encrypted ciphertext c_j as response, then (pk_j, c_j) is a derivative of (pk_i, c_i).
- If (pk_i, pk_j) has been queried to the re-encryption key generation oracle by the adversary, and $\mathsf{Decrypt}(pk_j, c_j) \in \{m_0, m_1\}$, then (pk_j, c_j) is a derivative of all pairs (pk_i, c).

After the introduction of derivatives of the challenge ciphertext, we describe the oracles involved in the security games for PRE scheme, which can be queried by the adversary in an adaptive manner in the security game. To deal with the inherent multi-user nature of PRE scheme, additional oracles apart from decryption and re-encryption oracles should be provided. The aim of these oracles defined here is to provide the adversary of keys for multiple users. These users can be either honest or corrupt relying on whether the adversary is unaware of the corresponding private key or not. Let $\mathcal{L}_{\mathcal{H}}$ and $\mathcal{L}_{\mathcal{C}}$ be the indices lists of honest and corrupt users respectively. Furthermore, the target user is considered honest and its index $i^* \in \mathcal{L}_{\mathcal{H}}$. The public and private keys of target user are denoted as pk_{i^*} and sk_{i^*}, respectively.

- $\mathcal{O}_{honest}$: On input a new public/private key pair (pk_i, sk_i) outputted by the $\mathsf{KeyGen}(k)$ algorithm, the honest key generation oracle $\mathcal{O}_{honest}$ inserts the index i into the list $\mathcal{L}_{\mathcal{H}}$ and outputs the public key pk_i. Here, $k \in \mathbb{K}$ denotes the security parameter.
- $\mathcal{O}_{corrupt}$: On input a new public/private key pair (pk_i, sk_i) outputted by the $\mathsf{KeyGen}(k)$ algorithm, the corrupt key generation oracle $\mathcal{O}_{corrupt}$ inserts the index i into the list $\mathcal{L}_{\mathcal{C}}$ and outputs the key pair (pk_i, sk_i).
- $\mathcal{O}_{rk}$: On input two public keys pk_i and pk_j, the re-encryption key generation oracle $\mathcal{O}_{rk}$ outputs a re-encryption key $rk_{i\to j} \leftarrow \mathsf{ReKey}(pk_i, sk_i, pk_j, sk_j)$. It is noted that the adversary is only allowed to make queries in which $i \neq j$ and either $i, j \in \mathcal{L}_{\mathcal{H}}$ or $i, j \in \mathcal{L}_{\mathcal{C}}$.
- $\mathcal{O}_{reenc}$: On input (pk_i, pk_j, c) in which $i \neq j$ and $i, j \in \mathcal{L}_{\mathcal{H}} \cup \mathcal{L}_{\mathcal{C}}$, the re-encryption oracle outputs the re-encrypted ciphertext $c' \leftarrow \mathsf{ReEncrypt}(rk_{i\to j}, c)$. Note that the adversary is not allowed to make queries such that $j \in \mathcal{L}_{\mathcal{C}}$ and (pk_i, c) is a derivative of (pk^*, c^*).
- $\mathcal{O}_{dec}$: On input (pk_i, c) in which $i \in \mathcal{L}_{\mathcal{H}} \cup \mathcal{L}_{\mathcal{C}}$, the decryption oracle $\mathcal{O}_{dec}$ outputs $m \leftarrow Decrypt(sk_i, c)$. Note that the adversary is not allowed to make queries such that (pk_i, c) is a derivative of (pk^*, c^*).

With respect to the re-encryption oracle $\mathcal{O}_{reenc}$ and the decryption oracle $\mathcal{O}_{dec}$, the restrictions on the derivatives of the challenge ciphertext disallow the adversary to attack trivially. Meanwhile, these restrictions should be flexible enough to enable the adversary to issue a wide range of queries.

The key extract oracles $\mathcal{O}_{honest}$, $\mathcal{O}_{corrupt}$ and $\mathcal{O}_{rk}$ should always be accessed by the adversary through out the security game since what actually matters among the attack models for PRE schemes is the accessibility to the re-encryption and decryption oracles. Furthermore, a static corruption model is usually assumed in the security model for PRE scheme such that the adversary should decide to corrupt a user or not before querying the private key of this user [22]. Noted that the honest key generation oracle $\mathcal{O}_{honest}$ can only return the public key of the queried user whereas the corrupt key generation oracle $\mathcal{O}_{corrupt}$ can provide the public/private key pair of the queried user. A common restriction named knowledge of secret key model is also assumed in the security game. In this model, the key material of all users are generated by the challenger. Additionally, there is a stronger chosen key model where

public keys for malicious users can be adaptively chosen by the adversary [16].

As mentioned in the definition of re-encryption key generation oracle $\mathcal{O}_{rk}$, the adversary is only allowed to make queries between two public keys pk_i and pk_j such that $i \neq j$ and either $i, j \in \mathcal{L}_H$ or $i, j \in \mathcal{L}_C$. That is to say, the re-encryption key between the honest and corrupt users cannot be generated. Otherwise, the adversary can trivially win the security game in some cases. For example, in a multi-use PRE scheme, an adversary could trivially win the game by first re-encrypting the challenge ciphertext to a honest user, and then using the honest-to-corrupt transformation key to re-encrypt it to a corrupt user. In the non collusion-resistant PRE schemes, the adversary could also leverage the honest-to-corrupt transformation key and a corrupt private key to obtain the private key of the honest user. Similarly, the corrupt-to-honest transformation key should not be generated to avoid the trivially attack from the adversary. Despite the stronger notions can be defined without restrictions on this oracle, these definitions are clearly useless for the PRE schemes featured with multi-user or transitive property. For example, Libert and Vergnaud [16] defined a new notion by removing the restrictions on oracle $\mathcal{O}_{rk}$, which allow all possible re-encryption key generation queries only with the restrictions for those from the target user to a corrupt user. Obviously, this model only works when the PRE scheme is single-use, non-transitive and collusion-resistant.

2) Attack Models: Motivated by the mnemonic described in [20] for attack models CCA1 and CCA2, a pair of indices $i, j \in \{0, 1, 2\}$ are used to represent attack models for PRE. Concretely, indices i and j denote that the last adversarial stage during which the adversary has access to the decryption oracle $\mathcal{O}_{dec}$ and re-encryption oracle $\mathcal{O}_{reenc}$, respectively. Hence, $\text{CCA}_{i,j}$ represents an attack model that the adversary has access to an oracle $\mathcal{O}_{dec}$ until Phase i and an oracle $\mathcal{O}_{reenc}$ until Phase j. In particular, a pure CPA model is recognized as $\text{CCA}_{0,0}$ and a pure CCA model is considered as $\text{CCA}_{2,2}$. Then, a set of intermediate attack models for PRE between $\text{CCA}_{0,0}$ and $\text{CCA}_{2,2}$ is ranked by the last stage during which the adversary has access to the decryption oracle $\mathcal{O}_{dec}$ and the re-encryption oracle $\mathcal{O}_{reenc}$.

As mentioned above, the accessibility to the $\mathcal{O}_{dec}$ oracle and $\mathcal{O}_{reenc}$ oracle varies among the presented attack models. Instead, the adversary can always access to the oracles $\mathcal{O}_{honest}$, $\mathcal{O}_{corrupt}$ and $\mathcal{O}_{rk}$ during the whole security game. Thus, $\mathcal{O}^{kg}$ are used to represent the set that comprises the key generation oracles $\mathcal{O}_{honest}$, $\mathcal{O}_{corrupt}$ and $\mathcal{O}_{rk}$. Then, assume $\mathcal{O}_1^{cca}$ and $\mathcal{O}_2^{cca}$ respectively to be the sets of the $\mathcal{O}_{dec}$ oracle and $\mathcal{O}_{reenc}$ oracle that are available in Phase 1 and 2. Evidently, $\mathcal{O}_1^{cca}$ and $\mathcal{O}_2^{cca}$ may be one of the following values $\emptyset$, $\{\mathcal{O}_{dec}\}$, $\{\mathcal{O}_{reenc}\}$ and $\{\mathcal{O}_{dec}, \mathcal{O}_{reenc}\}$. Furthermore, let $\mathcal{O}_1 = \mathcal{O}^{kg} \cup \mathcal{O}_1^{cca}$ and $\mathcal{O}_2 = \mathcal{O}^{kg} \cup \mathcal{O}_2^{cca}$ be the sets of oracles available in Phases 1 and 2, respectively. Since $\mathcal{O}^{kg}$ is always accessible in the whole security game, the expected attack models for PRE are materialized thoroughly by sets of $\mathcal{O}_1^{cca}$ and $\mathcal{O}_2^{cca}$. We can describe the available oracles in a more formal manner as follows. Let $\text{CCA}_{i,j}$ be an attack model for PRE and $t \in \{1, 2\}$, then $\{\mathcal{O}_{dec}\} \in \mathcal{O}_t^{cca}$, for $i \geq t$, and $\{\mathcal{O}_{reenc}\} \in \mathcal{O}_t^{cca}$, for $j \geq t$.

TABLE I
DIFFERENT ATTACK MODELS FOR PRE

$\mathcal{O}_1^{cca}$	$\mathcal{O}_2^{cca}$	Attack Model
$\varnothing$	$\varnothing$	$\text{CCA}_{0,0}$ = CPA
$\{\mathcal{O}_{reenc}\}$	$\varnothing$	$\text{CCA}_{0,1}$
$\{\mathcal{O}_{reenc}\}$	$\{\mathcal{O}_{reenc}\}$	$\text{CCA}_{0,2}$
$\{\mathcal{O}_{dec}\}$	$\varnothing$	$\text{CCA}_{1,0}$
$\{\mathcal{O}_{dec}, \mathcal{O}_{reenc}\}$	$\varnothing$	$\text{CCA}_{1,1}$
$\{\mathcal{O}_{dec}, \mathcal{O}_{reenc}\}$	$\{\mathcal{O}_{reenc}\}$	$\text{CCA}_{1,2}$
$\{\mathcal{O}_{dec}\}$	$\{\mathcal{O}_{dec}\}$	$\text{CCA}_{2,0}$
$\{\mathcal{O}_{dec}, \mathcal{O}_{reenc}\}$	$\{\mathcal{O}_{dec}\}$	$\text{CCA}_{2,1}$
$\{\mathcal{O}_{dec}, \mathcal{O}_{reenc}\}$	$\{\mathcal{O}_{dec}, \mathcal{O}_{reenc}\}$	$\text{CCA}_{2,2}$

There are nine possible attack models for PRE described in Table I according to the different combinations of available oracles which are materialized by sets of $\mathcal{O}_1^{cca}$ and $\mathcal{O}_2^{cca}$. Naturally, it is not possible to have an oracle in Phase 2 but not in Phase 1 since the term used in the definition of the parametric attack models is "until Phase" for defining oracles' accessibility insted of "in Phase". Moreover, in Table I there is a particular case that when $\mathcal{O}_1^{cca} = \mathcal{O}_2^{cca} = \varnothing$, the attained model $\text{CCA}_{0,0}$ is actual CPA where $\mathcal{O}_{dec}$ and $\mathcal{O}_{reenc}$ oracles can not be accessed.

From Table I, we can find that more $\mathcal{O}_{dec}$ than $\mathcal{O}_{reenc}$ are provided in attacks models for PRE. Actually, it is easier for the adversary to access to $\mathcal{O}_{reenc}$ oracle than to $\mathcal{O}_{dec}$ oracle. Because the re-encryption capability is carried out by the semi-trusted proxy while the decryption function can only be performed by the user him/herself. In this way, the $\text{CCA}_{1,0}$ and $\text{CCA}_{2,0}$ is not appropriate for defining security in a PRE scheme.

3) Security Definitions: Similar to the normal public key encryption scheme, the security notion is defined by incorporating the indistinguishability of encryptions and the family of the above-mentioned attack models.

Definition 3: Let $\Sigma = (\mathsf{KeyGen}, \mathsf{ReKey}, \mathsf{Encrypt}, \mathsf{ReEncrypt}, \mathsf{Decrypt})$ be a proxy re-encryption scheme, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a polynomial-time adversary and $\mathcal{O}_1$ and $\mathcal{O}_2$ be the set of available oracles for $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. For $i, j \in \{0, 1, 2\}$, $b \in \{0, 1\}$ and the security parameter $k \in \mathbb{K}$, the indistinguishability game is defined by the following experiment.

$\mathbf{Exp}_{\Sigma,\mathcal{A},b}^{\text{IND-CCA}_{i,j}}(k)$:

$$
\begin{aligned}
&(pk^*, sk^*) \leftarrow \mathsf{KeyGen}(k);\\
&(m_0, m_1, s) \leftarrow \mathcal{A}_1(pk^*);\\
&c^* \leftarrow \mathsf{Encrypt}(pk^*, m_b);\\
&d \leftarrow \mathcal{A}_2(m_0, m_1, s, c^*);\\
&\text{return} \quad d.
\end{aligned}
$$

Note that when *i = 2* or *j = 2* the available oracles for $\mathcal{A}_2$ must be subjected to the derivatives of the challenge ciphertext c^*. In the security game, $\mathcal{O}_1^{cca}$ and $\mathcal{O}_2^{cca}$ are defined according to the attack model $\text{CCA}_{i,j}$, as described in Table I.

Definition 4: Let Σ be a PRE scheme and $\mathcal{A}$ be a polynomial-time adversary. For $i, j \in \{0, 1, 2\}$ and $k \in \mathbb{K}$,

the advantage of $\mathcal{A}$ to win the experiment $\mathbf{Exp}^{\text{IND-CCA}_{i,j}}_{\Sigma,\mathcal{A},b}(k)$ is given by

$$\begin{aligned}&\mathsf{Adv}^{\text{IND-CCA}_{i,j}}_{\Sigma,\mathcal{A}}(k)\\ =&|\Pr[\mathbf{Exp}^{\text{IND-CCA}_{i,j}}_{\Sigma,\mathcal{A},1}(t)=1]-\Pr[\mathbf{Exp}^{\text{IND-CCA}_{i,j}}_{\Sigma,\mathcal{A},0}(t)=1]|.\end{aligned}$$

The PRE scheme Σ is said to be $\mathsf{IND\text{-}CCA}_{i,j}$ secure if the advantage $\mathsf{Adv}^{\text{IND-CCA}_{i,j}}_{\Sigma,\mathcal{A}}$ is negligible.

To improve the clarity, the *selective model* is assumed in the security game depicted by the experiment $\mathbf{Exp}^{\text{IND-CCA}_{i,j}}_{\Sigma,\mathcal{A},b}(k)$ such that the target public key pk^* is fixed by the challenger at the beginning of the game [12, 16].

It is desirable to illustrate the defined security models with examples of representative PRE schemes and expect that most of these schemes are accompanied with these security notions. For instance, Blaze *et al.*'s [6] and Ateniese *et al.*'s [12] PRE schemes are only secure under $\mathsf{IND\text{-}CCA}_{0,0}$, which is indeed CPA security. Canetti and Hohenberger [15] proposed a scheme featured with the $\mathsf{IND\text{-}CCA}_{2,2}$ security. A PRE scheme proposed by Kirshanova [18] is claimed to achieve $\mathsf{IND\text{-}CCA}_{1,1}$ security but this scheme is indeed $\mathsf{IND\text{-}CCA}_{1,0}$ secure as shown in [21]. And as far as we know there is not a PRE scheme satisfying the $\mathsf{IND\text{-}CCA}_{1,1}$ security. The comparison of the representative PRE schemes in terms of security notions can be found in the Table IV.

III. Surveying Proxy Re-Encryption Schemes

Now we attempt to survey the existing literature and constructions for PRE schemes over the period 1998-2015 in terms of efficiency, security and properties. Also, we provide a description of several representative PRE schemes together with the investigation of design philosophy behind them.

A. State-of-the-Art of PRE

1) Basic PRE schemes: In 1998, Blaze *et al.* [6] initially introduced the notion of proxy re-encryption, which is called atomic proxy encryption in [6]. They constructed a bidirectional and multi-use PRE scheme based on the ElGamal public key encryption [23]. However, their scheme can only achieve CPA security and suffer from the collusion attack such that the proxy can reveal the delegator's private key by colluding with the delegatee. They left an interesting open problem to construct an unidirectional or a single-use PRE scheme. One year later, Jakobsson [24] devoted to present unidirectional proxy re-encryption, which was regarded as an open problem in [6]. Concretely, a unidirectional PRE scheme was constructed under quorum controlled such that the ciphertext transformation can only be performed by multiple proxies where each proxy owns a share of re-encryption key secret. In other words, if the number of honest proxies is larger than pre-defined, the private key of the delegator will not be disclosed even though the delegator is under collusion attacks.

In 2003, to realize unidirectional transformation, Ivan and Dodis [25] proposed a general construction of unidirectional single-use PRE by splitting the delegator's secret key into two parts and distribute to the proxy and delegatee separately. Despite the unidirectional transformation can be achieved, their private key sharing approach suffers from the following drawbacks. In particular, the original ciphertext under the delegator's public key can not be translated into the ciphertext intended for the delegatee purely. That is to say, the transformed ciphertext cannot be opened by the delegatee with his own private key. To perform the decryption operation over the transformed ciphertext, additional secrets from the delegator should be stored and managed by the delegatee. What make matters worse, the ciphertext under the other member's public key can also be decrypted in case the proxy and any delegatee in the system collude together. It is fair to say that the construction of unidirectional PRE scheme still remains an open problem.

In 2005, Ateniese *et al.* [12, 13] outlined the desired characteristics and formalized the definition of PRE scheme by considering that only informal notion of PRE was given by Blaze *et al.* [6]. Also, they put forward several PRE scheme featured with unidirectional property relying on bilinear pairings for the first time. Furthermore, they presented the first temporary PRE schemes such that the delegator can periodically update delegation relationships without changing his public key and the re-encryption key is only valid during a given time period. However, the re-encryption algorithm in [12, 13] is single-use where only the original ciphertext can be re-encrypted. Thus, constructing the multi-hop unidirectional PRE scheme is viewed as an open problem.

In 2007, Canetti and Hohenberger [15] formulated a meaningful security definition in the CCA sense [26] for PRE schemes whereas only the CPA security is considered in the previous works [6, 25, 12, 13]. In this security model, they presented the first CCA-secure PRE scheme featured with bidirectional and multi-use properties. Moreover, the security proof of their scheme does not rely on random oracles. Meanwhile, severl interesting open problems were left for further investigation in [15]. Independently, Green and Ateniese [27] introduced the PRE into the ID-based public key cryptosystem environment and proposed the identity-based proxy re-encryption (ID-PRE) scheme based on Boneh-Franklin's ID-based encryption scheme [28], where ciphertexts under the delegator's identity can be converted into the encryption under the delegatee's identity. Despite their scheme can achieve CCA security, the random oracles are needed in their security proof.

In 2008, Deng *et al.* [29] first proposed a pairing-free bidirectional and single-use PRE scheme in an effort to avoid the expensive bilinear pairing operations. Their scheme is provable secure against chosen-ciphertext attacks in the random oracle model by reducing its security to the Computational Diffie-Hellman (CDH) problem. Libert *et al.* [30] presented the first construction of unidirectional PRE scheme featured with the replayable chosen-ciphertext security (RCCA-security) in the non-adaptive corruption model, which partially solved one open problem left in [15].

In 2009, Shao *et al.* [31] aimed to solve one of the open problems left in [15] by constructing the first unidirectional PRE scheme simultaneously achieving CCA security and collusion-resistance. Furthermore, the bilinear pairing operation was eliminated from their construction. To achieve fine-grained access control, Liang *et al.* [32] first presented

the notion of attribute-based PRE (AB-PRE) by integrating the PRE and attribute-based encryption and gave a concrete construction. In AB-PRE, the delegator associated with some specified attributes could freely allow a proxy to re-encrypt a ciphertext with respect to a certain access policy to another encryption under a different access policy. The notion of conditional PRE (C-PRE) was first introduced by Weng *et al.* [33, 34] such that the delegator owns a fine-grained control over the delegation. Specifically, the ciphertext can only be transformed by the proxy and then decrypted by the delegatee if this ciphertext satisfies a specific condition designated by the delegator. Meanwhile, Ateniese *et al.* [22] presented the first key-private PRE such that even the proxy performing the translations cannot disclose the identities of the delegator and delegatee from transformation keys or ciphertexts.

In 2010, Weng *et al.* [35] proposed a single-use unidirectional PRE scheme achieving CCA-security instead of the weaker RCCA-security in the adaptive corruption model. In addition, the security proof of Weng *et al.*'s scheme can be given in the standard model. Chow *et al.* [36] showed that the security proof in [31] is flawed by presenting a concrete attack. After that, an improved pairing-free unidirectional PRE scheme has been proposed to achieve high efficiency and CCA security. Since all previous PRE schemes are either constructed based on the bilinear pairing in the standard model or are proven secure in the random oracle model, Matsuda *et al.* [37] constructed a bidirectional, multi-use and CCA secure PRE scheme without bilinear maps in the standard model. To solve the key escrow problem in ID-PRE without losing the advantage of the ID-based cryptogryphy, the notion of certificateless based PRE (CL-PRE) was first put forward by Sur *et al.* [38] based on the idea of certificateless-based public key encryption (CL-PKE) [39]. Inspired by public-key encryption with keyword search, Shao *et al.* [40] introduced the notion of proxy re-encryption with keyword search. A digital content sharing model for DRM [8] has been proposed based on Ateniese *et al.*'s PRE scheme [12].

In 2011, to achieve CCA security in the standard model without sacrificing collusion-resistance [41], Libert *et al.* [16] presented the first construction of CCA secure and collusion-resistant unidirectional PRE scheme in the standard model. In [42], Weng *et al.* demonstrated that the PRE scheme due to Matsuda *et al.* [37] does not achieve chosen-ciphertext security and argued that it was still an open problem to constructe a pairing-free PRE scheme featuring with CCA security in the standard model. Moreover, Shao *et al.* [43] presented the first CCA secure unidirectional and multi-use PRE scheme, which gives an answer to an open problem proposed by Canetti and Hohenberger [15]. With the aid of a RSA-based PRE scheme, Chen *et al.* [11] came up with a solution to manage group keys in a secure manner.

In 2012, Hanaoka *et al.* [44] revisited the CCA security definition for PRE and defined the strongest security notion which enables adversary to own all the possible resources other than those that allow it to attack trivially. After that, the first generic construction of CCA secure unidirectional PRE scheme along with one concrete construction was presented based on the resplittable threshold public key encryption. However, their PRE scheme cannot be regarded as the pure PRE scheme since the delegatee needs a share of delegator's secret to perform the decryption over the re-encrypted ciphertext. Thanks to the fact that none of the existing schemes can achieve CCA security and key-privacy in the standard model, Shao *et al.* [45] introduced the first such PRE scheme, which solves an open problem left by Ateniese *et al.* [22].

In 2013, Isshiki *et al.* [46] pointed out the CCA security model presented in [44] is a somewhat strengthened variant of the RCCA one and does not achieve the fully CCA security. Hence, they defined a full CCA security model which is extended from [44] and proposed a PRE scheme under the stronger security model without random oracles. To achieve more fine-grained control over the delegation, Fang *et al.* [47] formalized the definition of fuzzy conditional proxy re-encryption such that the conditions in C-PRE is represented as a set of descriptive keywords.

In 2014, Zhang *et al.* [48] showed that the scheme in [16] is proven secure in the knowledge of secret key model but not secure in the chosen key model, hence, they further presented an efficient CCA secure PRE scheme in the stronger chosen key model. To resist the quantum attack, Kirshanova *et al.* [18] presented the first lattice-based PRE scheme that achieves collusion resilience and non-interactivity. Furthermore, the security proof of their scheme is given in the selective model under the Learning With Error (LWE) assumption. Guo *et al.* [49] pointed out almost all the PRE schemes failed to capture the forgeable re-encryption attack in a sense that re-encryption keys may be forged through the collusion attack launched by the proxy and a delegatee. As a result, they first defined the notion of the unforgeability of re-encryption keys to capture the above attack. Liu *et al.* [50] constructed a mechanism to achieve fine-grained secure data sharing with scalable user revocation on encrypted message by combining the PRE primitive and attribute-based encryption.

In 2015, Tang *et al.* [51] introduced an unidirectional and multi-use PRE scheme based on multi-linear maps [52] under some strong assumptions in the setting of multi-linear groups. It answers to an interesting open problem left by Canetti and Hohenberger that how to design a PRE scheme features simultaneously unidirectional and multi-hop. Nuñez *et al*. [21] examined the existing security models for PRE schemes and proposed a new nomenclature for these models in terms of the accessibility of both the decryption and re-encryption oracles during the security game. Owning to the fact that most previous PRE schemes are constructed under the number theoretic assumption, Nuñez *et al*. [19] presented a new bidirectional and multi-use PRE schemes based on the NTRU, the well known lattice-based cryptosystem. By considering the asymmetric capacity among the mobile devices and the server, Deng *et al*. [53, 54] presented asymmetric cross-cryptosystem re-encryption by allowing an authorized proxy to convert a complicated ID-based broadcast encryption ciphertext deployed in the server into a simple ID-based encryption ciphertext affordable to mobile devices.

The progress of PRE can be mainly classified into three phases as follows.

1) 1998-2004: During this infancy stage, very little follow

up work has been done after the birth of the notion of PRE primitive in [6].

2) 2005-2013: After the desired characteristics and the security definition of PRE schemes are identified and clarified [12, 13, 15], great attention has been paid on the PRE primitive again from the academic and engineering community. There are many fruitful achievements on PRE in terms of improving the efficiency, enhancing the security and facilitating the function. For instance, many new properties, new security models and new constructions are investigated during this stage.
3) 2014-Now: New constructions based on alternative mathematical foundations other than number theoretic assumptions are investigated. Motivated by the practical needs, the translation property of PRE are borrowed to devise new primitives, which are suitable for different environments. In a nutshell, the nature of PRE are investigated and efficient and provably secure primitives featured with desired properties are expected to be proposed during this stage.

2) Identity-based PRE schemes: In view of the costly certificate management overhead in the traditional public key encryption, Green *et al.* [27] introduced the notion of identity-based proxy re-encryption (IB-PRE) scheme by incorporating the idea of PRE and ID-based encryption [28]. They gave the first concrete construction of the first ID-PRE scheme based on the bilinear pairing. Their PRE scheme is unidirectional, multi-use and non-interactive but not collusion-resistant as shown in [55]. Compared with the basic PRE schemes in the traditional public key infrastructure, ID-PRE enjoys the advantage of avoiding the tedious certificates management problem. Therefore, lots of ID-PRE schemes were put forward. To close the open problems left in [27], Chu *et al.* [41] presented a unidirectionality, non-interactivity and multi-use ID-PRE scheme secure in the standard model. Unfortunately, Shao *et al.* [56] pointed out that their scheme [41] even cannot resist chosen-plaintext attack. To mirror an organizational hierarchy, Ren *et al.* [57] constructed the first hierarchical ID-PRE scheme with CCA security in the standard model. Based on the work of Green and Ateniese [27], Emura *et al.* [58] proposed an ID-PRE scheme together with source hiding property, where no information about source identity is revealed from destination ciphertext. Zhang *et al.* [59] pointed out that an unidirectional and multi-use scheme presented by Wang *et al.* [60] easily suffers from chosen-ciphertext attack. To conceal the identity of the intended delegatee and the message content together, Shao *et al.* [61] proposed the notion of anonymous ID-PRE along with the concrete construction. Inspired by the ID-PRE [27], Shao *et al.* [62] constructed the first multi-use unidirectional ID-PRE scheme achieving CCA security and collusion-resistance. Furthermore, Matsuo [63] proposed a hybrid PRE scheme to transform a ciphertexts encrypted under a traditional public key into the ciphertexts that are encrypted by an identity.

3) Attribute-based PRE schemes: By combining the identity-based PRE [27] and the attribute-based encryption [64], Liang *et al.* [32] first proposed the concept of attribute-based PRE (AB-PRE), where the delegator associated with some specified attributes could freely allow a proxy to re-encrypt a ciphertext with respect to a certain access policy to another encryption under a different access policy. A CCA secure unidirectional and multi-use AB-PRE scheme are constructed based on the ciphertext policy ABE. Luo *et al.* [65] also proposed a ciphertext policy unidirectional and multi-use AB-PRE scheme featured with re-encryption control and extra access control in the security model defined in [32]. The works in [32] and [65] were further applied to secure the data sharing in cloud computing by Yu *et al.* [66, 67].

4) Certificateless-based PRE Schemes: Sur *et al.* [38] introduced the PRE primitive into certificateless public key encryption [39] and proposed the notion of certificateless PRE (CL-PRE) in order to enjoy the advantages of traditional public key encryption and identity based encryption without suffering from their corresponding drawbacks. Based on Libert-Quisquater's certificateless encryption [68], they constructed the first unidirectional CL-PRE scheme with CCA security in the random oracle model. Concretely, CL-PRE not only eliminates the tedious public key certificate management in basic PRE in PKI environment, but also solves the inherent key escrow problem in the ID-PRE setting. Based on the Al-Riyami-Paterson [39], Xu *et al.* [69] then presented an unidirectional and single-use CL-PRE scheme for securing cloud based data sharing. Their scheme is provable CPA security in the random oracle model. However, Guo *et al.* [70] constructed a RCCA secure CL-PRE scheme. They also pointed out that in their stronger security model Xu *et al.*'s scheme [69] are vulnerable against the Type I adversary. It should be emphasized that these CL-PRE schemes above are constructed relying on the costly bilinear pairings, Yang *et al.* [71] first constructed a CCA secure CL-PRE scheme without bilinear pairings. To relax the restriction that Type I adversary is not allowed to replace the public key of the challenge identity in [71], Qin *et al.* [72] constructed a novel CL-PRE scheme in sense that a Type I adversary is allowed to replace the public key of the challenge identity in the security proof.

B. Design Philosophy of PRE

In this subsection, we review two representative PRE schemes [6, 12]. Instead of merely showing the construction details of each scheme, we attempt to investigate the philosophy behind their design. Also, we intended to unify the notations in the descriptions of different schemes.

1) Bidirectional and Multi-use PRE: Blaze *et al.* [6] constructed the first PRE scheme based on ElGmal encryption [23], which is bidirectional and multi-use. Their scheme is depicted as follows:

- $(pk, sk) \leftarrow$ KeyGen: On input $k \in \mathbb{K}$, choose $x \in_R \mathbb{Z}_{2q}^*$, compute $g^x \mod p$, and output a public/private pair $(pk, sk) = (g^x \mod p, x)$. Here, $(p, q, g, \mathbb{Z}_p^*$ are the public parameters such that $p = 2q + 1$).
- $rk_{i \to j} \leftarrow$ ReKey: On input a private key $sk_i = x_i$ for the delegator and a private key $sk_j = x_j$ for the delegatee, the proxy computes $rk_{i \to j} = x_j / x_i \mod p$ as a re-encryption key.
- $c_i \leftarrow$ Encrypt: To encrypt a message $m \in \mathbb{Z}_p^*$ under the public key $pk_i = g^{x_i} \mod p$ for user i, selects a random

number $s \in_R \mathbb{Z}_{2q}^*$ and returns a ciphertext $c_i = (c_1, c_2)$, where $c_1 = mg^s \mod p$ and $c_2 = (g^{x_i})^s \mod p$.
- $c_{i\to j} \leftarrow$ ReEncrypt: Taking as input a re-encryption key $rk_{i\to j} = x_j/x_i \mod p$ from user i to user j and the ciphertext $c_i = (c_1, c_2)$ under user i's public key, the proxy computes $c_2' = c_2^{rk_{i\to j}}$ and returns the re-encryption ciphertext $c_{i\to j} = (c_1, c_2')$.
- $m \leftarrow$ Decrypt: On input a private key $sk_i = x_i$ and a ciphertext $c_i = (c_1, c_2)$ for user i, user i returns the plaintext $m = c_1(c_2^{(x_i^{-1})})^{-1} \mod p$ or the error symbol $\perp$ indicating c_i is invalid.

According to the ReKey algorithm, the re-encryption key can only be generated by interaction among proxy, the delegator (e.g. user i) and the delegatee (e.g. user j). Firstly, the proxy randomly chooses a blind factor $r \in \mathbb{Z}_{2q}^*$ and sends r to the delegator. After that, user i computes r/x_i using her private key and sends the computation result to user j. Then, user j computes $x_j(r/x_i)$ using his private key and returns the computation result to the proxy. Finally, the proxy computes the re-encryption key $rk_{i\to j} = [x_j(r/x_i)]/r = x_j/x_i$ with the blind factor r. Hence, the re-encryption key is actually generated by the proxy rather than the delegator in this scheme.

In this PRE scheme, the value c_1 in the ciphertext $c_i = (c_1, c_2)$ generated by Encrypt dose not depend on the delegator's public key $pk_i = g^{x_i}$, which is embedded only in c_2. In ReEncrypt, with a re-encryption key $rk_{i\to j} = x_j/x_i$, the proxy removes x_i by raising c_2 to x_i^{-1} and further contributes an element of x_j to the exponent in c_2. That is, the special construction of $rk_{i\to j}$ enables the proxy successful to transform a ciphertext under pk_i into another ciphertext under pk_j.

It is easy to observe that this scheme cannot provide collusion-resistance. Concretely, the proxy may collude with the delegatee to recover the delegator's private key by calculating $x_i = (rk_{i\to j}/x_j)^{-1}$. In addition, given $rk_{i\to j}$ and $rk_{j\to k}$, the proxy can easily obtain $rk_{i\to k} = rk_{i\to j} \cdot rk_{j\to k} = (x_j/x_i) \cdot (x_k/x_j) = x_k/x_i$ illegally, even if user i does not expect to delegate her decryption power to the user k. That is to say, this scheme cannot offer non-transitivity.

Assume that user j is the delegator and user i is the delegatee, then the output of ReKey is $rk_{j\to i} = x_i/x_j$, which is the reverse of $rk_{i\to j}$. Once getting $rk_{i\to j}$ for $i \to j$, the proxy is easy to acquire $rk_{j\to i}$ by using the extended Euclidean algorithm. Then even though the delegatee does not delegate $rk_{j\to i}$ to the proxy, the proxy still enables to not only transform the the delegator's ciphertext into the delegatee's ciphertext on the same message but also vice versa. Interestingly, ciphertext $c_i = (c_1, c_2) = (mg^s, (g^{x_i})^s)$ and re-encrypted ciphertext $c_{i\to j} = (c_1, c_2') = (mg^s, (g^{x_j})^s)$ have the same ciphertext space and $c_{i\to j}$ is indeed re-encrypted. That indicates the re-encryption key in this scheme is bidirectional and multi-use.

2) Unidirectional and Single-use PRE: In [12], Ateniese *et al.* [12] proposed an unidirectional and single-use PRE scheme (Ateniese [12]-2) based on the bilinear pairings: The global parameters are $(p, g, e, \mathbb{G}_1, \mathbb{G}_2, Z)$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are groups of the prime order *p*, *g* is a random generator of $\mathbb{G}_1$, $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and $Z = e(g, g) \in \mathbb{G}_2$.

- $(pk, sk) \leftarrow$ KeyGen: On input a security parameter $k \in \mathbb{K}$, generate a public key $pk = (Z^{x_1}, g^{x_2})$ and a private key $sk = (x_1, x_2)$, where $x_1, x_2 \in_R \mathbb{Z}_p$.
- $rk_{i\to j} \leftarrow$ ReKey: Given $sk_i = (x_{i1}, x_{i2})$ for user i (the delegator) and $pk_j = (Z^{x_{j1}}, g^{x_{j2}})$ for user j (the delegatee), user i calculates the transformation key $rk_{i\to j} = g^{x_{i1}x_{j2}} \in \mathbb{G}_1$.
- $c_i \leftarrow$ Encrypt: To encrypt a plaintext $m \in \mathbb{G}_2$ under the public key $pk_i = (Z^{x_{i1}}, g^{x_{i2}})$ for user i, selects a random $s \in_R \mathbb{Z}_p$ and calculates a ciphertext as follows.
  - First-Level: Compute and output $c_{x,1} = (Z^{x_{i1}s}, mZ^s)$, which can only be decrypted by user i. The first-level ciphertext $c_{i,1}$ can only be decrypted by the delegator.
  - Second-Level: Compute and output $c_{i,2} = (g^s, mZ^{x_{i1}s})$, which can only be decrypted by user i or the delegatees. The second-level ciphertext $c_{i,2}$ can be decrypted by the delegator and his delegatee.
- $c_{i\to j} \leftarrow$ ReEncrypt: A second-level ciphertext under the public key of the delegator can be transformed into a first-level ciphertext under the public key of the delegatee with the transformation key $rk_{i\to j}$. Given a re-encryption key $rk_{i\to j} = g^{x_{i1}x_{j2}}$ for $i \to j$ and a delegator's second-level ciphertext $c_{i,2} = (g^s, mZ^{x_{i1}s})$, the proxy computes $e(g^s, g^{x_{i1}x_{j2}}) = Z^{x_{i1}x_{j2}s}$. Then it produces the re-encryption ciphertext $c_{i\to j} = (Z^{x_{i1}x_{j2}s}, mZ^{x_{i1}s}) = (Z^{x_{j2}s'}, mZ^{s'})$ where $s' = x_{i1}s$.
- $m' \leftarrow$ Decrypt: On input sk_i and a ciphertext c_i for user i on message *m*,
  - Given a first-level ciphertext $c_{i,1}$ for user i and her own private key sk_i, user i returns $m' = mZ^s/(Z^{x_{i1}s})^{(x_{i1})^{-1}}$.
  - Given a second-level ciphertext $c_{i,2}$ for user i and her own private key $x_{i1} \in sk_i$, user i returns $m' = mZ^{x_{i1}s}/e(g^s, g)^{x_{i1}}$.

In this scheme, the re-encryption key $rk_{i\to j} = (g^{x_{j2}})^{x_{i1}} = g^{x_{i1}x_{j2}}$ is generated non-interactively by the delegator (e.g user i) with his own private key x_{i1} and the delegatee (e.g user j)'s public key $g^{x_{j2}}$. Then the delegator is responsible for delivering the re-encryption key to the proxy via a secure channel. Compared with Blaze *et al.*'s bidirectional and multi-use re-encryption key [6], this scheme is unidirectional and single-use since it is computationally infeasible for the proxy to obtain the re-encryption key $rk_{j\to i}$ from any other re-encryption keys without user j's delegation. Furthermore, the re-encrypted ciphertext $c_{i\to j}$ cannot be re-encrypted by ReEncrypt algorithm any more.

Ateniese [12]-2 is a PRE scheme based on bilinear pairings. The Encrypt algorithm contains the first-level encryption and the second-level encryption, where the proxy can only transform a second-level ciphertext under the delegator's public key into a first-level ciphertext under the delegatee's public key. Meanwhile, the construction of a re-encryption key makes Ateniese [12]-2 non-transitive and collusion-resistant due to

the fact that x_i cannot be recovered from $g^{x_{i1}x_{j2}}$ under the discrete logarithm assumption.

C. Comparisons

In this subsection, several representative PRE schemes are compared in terms of properties, performance and security in Table II, III and Table IV respectively. In our comparisons, the complexity of highly efficient operations such as multiplication or addition in group, conventional hash function and XOR operation are omitted. We denote by P a pairing operation, by S a scalar multiplication in $\mathbb{G}_1$, by E a exponentiation in $\mathbb{G}_2$; Sig and Vfy denote the one-time signature and verification, respectively; Enc and Dec denote the symmetric encryption and decryption respectively; k, k_1 and k_2 denote a security parameter, the bit-length of $\{0,1\}^{k_1}$ and $\{0,1\}^{k_2}$, respectively; $|\mathbb{G}|$, $|\mathbb{G}_1|$, $|\mathbb{G}_2|$ and $|\mathbb{Z}_p|$ denote the bit-length of an element in $\mathbb{G}$, $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{Z}_p$, respectively; $|k_s|$ and $|\sigma_s|$ denote the bit-length of one-time signing key and signature; $|T|$ denotes the bit-length of the timestamp; $|\mathcal{M}|$ denotes the bit-length of message $m \in \mathbb{M}$; $|Sym_{Enc}|$ denotes the bit-length of the one-time symmetric encryption ciphertext; $|N|$, $|N_x|$ and $|N_y|$ denote the safe-prime modulus; RO and ST denote the random oracle model and the standard model, respectively.

In Table II, "weak" means that the proxy cannot obtain the delegator's private key but the underlying encrypted message through the collusion attacks. It is obvious that none of the existing schemes can meet all properties simultaneously since each PRE scheme is proposed to be suitable for different application scenarios. In view of the heavy computational cost of bilinear pairing, it is also easy to see that the pairing-free PRE schemes gain better efficiency than other schemes. In addition, the works of Deng *et al.* [29] and Chow *et al.* [36] outperform other PRE schemes. Particularly, their schemes not only have more efficient Encrypt/Decrypt algorithms but also have more compact key length and ciphertext length. Meanwhile, we observe that the existing schemes, which are provable secure without random oracles, are all constructed based on bilinear pairings. Compared with [30, 43, 46], Canetti *et al.*'s scheme [15] is the optimal one in terms of computation cost, key length and ciphertext length.

IV. Extensions

In this section, we first described the proxy re-signature, the signature counterpart of PRE, with respect to the syntax, security model and properties. After that, the extensions and applications of PRE schemes are also presented.

A. Proxy Re-Signature

The primitive of proxy re-signature (PRS), which was also introduced by Blaze *et al*. in their seminar work [6], allows a semi-trusted proxy to transform a signature from the delegatee into a signature from the delegator on the same message. However, the proxy cannot sign arbitrary message on behalf of either the delegatee or the delegator. A multi-use and bidirectional PRS scheme has also been presented in [6]. Since the introduction of the PRS primitive, there was no follow-ups until the work by Ateniese and Hohenberger [14] in 2005. In [14], they first formalized the definition of security for the PRS scheme, known as the AH model, and then proposed three concrete proxy re-signature schemes based on bilinear pairing with proven security. Similar to PRE schemes, PRS has attracted a lot of attention from then on. In particular, Shao *et al*. [74] proposed an identity based multi-use and bidirectional proxy re-signature scheme, and Libert and Vergnaud [75] proposed a multi-use and unidirectional scheme based on the *l*-FlexDH assumption. Shao *et al.* [76] presented unidirectional ID-based proxy re-signature scheme along with the security proof in the random oracle model. Recently, Tian *et al.* [77] constructed an identity-based PRS scheme based on lattices assumptions.

1) Syntax of Proxy Re-Signature: According to [14], the definition of an unidirectional PRS scheme is described as follows.

Definition 5 (Proxy Re-Signature Scheme): A PRS scheme consists of the following polynomial time algorithms: KeyGen, ReKey, Sign, ReSign and Verify.

- KeyGen: On input a security parameter $k \in \mathbb{K}$, user i runs this algorithm to generate its public/private key pair (pk_i, sk_i).
- ReKey: On input a key pair (pk_i, sk_i) for user i and a key pair (pk_j, sk_j) for user j (sk_j is optional), the re-encryption key generation algorithm ReKey is performed by user i to output a re-encryption key $rk_{i\to j}$. Since the re-encryption key $rk_{i\to j}$ enables to transform user i's signature into user j's signature, thus user j acts as the delegator and user i acts as the delegatee.
- Sign: On input a message $m \in \mathcal{M}$ and its own private key sk_i, user i performs this algorithm to compute a corresponding signature σ_i.
- ReSign: On input a signature σ_i from user i and a re-signature key $rk_{i\to j}$, this algorithm is executed by the proxy to generate a re-signed signature $\sigma_{i\to j}$, if $\mathsf{Verify}(pk_i, m, \sigma_i) = 1$ holds; Otherwise, this algorithm returns an error symbol $\perp$ indicating σ_i is invalid.
- Verify: On input a public key pk_i of user i, the message $m \in \mathcal{M}$ and a corresponding signature σ_i, a verifier performs this algorithm to check the validity of this signature. If $\mathsf{Verify}(pk_i, m, \sigma_i)$ holds, it returns 1; otherwise, returns 0.

Correctness. Generally, a triple of (KeyGen, Sign, Verify) are identical to those in normal signature scheme. For any message $m \in \mathcal{M}$ and any key pairs $(pk_i, sk_i), (pk_j, sk_j) \leftarrow \mathsf{KeyGen}(k)$, PRS should satisfy the following conditions of correctness:

$$\mathsf{Verify}(pk_i, m, \mathsf{Sign}(m, sk_i)) = 1,$$
$$\mathsf{Verify}(pk_j, m, \mathsf{ReSign}(\mathsf{ReKey}(pk_i, sk_i, pk_j, sk_j), \mathsf{Sign}(m, sk_i))) = 1.$$

2) Security Model for PRS: Generally, a normal sense of existential unforgeability [78] is considered for a digital signature in the sense that the adversary should not be able to generate a valid signature on any message even though this adversary can obtain signatures on any messages it wishes

TABLE II
THE PROPERTY COMPARISON OF PRE SCHEMES

Schemes	Properties								
	Unidirectional	Multi-use	Key-private	Transparent	Key-optimal	Non-interactive	Non-transitive	Temporary	Collusion-resistant
Blaze [6]	×	✓	×	✓	✓	×	×	×	×
Ateniese [12]-1	✓	×	✓	✓	✓	✓	✓	×	weak
Ateniese [12]-2	✓	×	✓	✓	✓	✓	✓	×	weak
Ateniese [13]	✓	×	✓	✓	✓	✓	✓	✓	weak
Canetti [15]-1	×	✓	×	✓	✓	×	×	×	×
Canetti [15]-2	×	✓	×	✓	✓	×	×	×	×
Libert [30]-1	✓	×	✓	×	✓	✓	×	×	✓
Libert [30]-2	✓	×	✓	×	✓	✓	×	✓	✓
Deng [29]	×	×	✓	×	✓	×	×	×	×
Shao [31]-1	✓	×	✓	✓	×	✓	✓	×	✓
Shao [31]-2	✓	×	✓	✓	×	✓	✓	✓	✓
Chow [36]	✓	×	✓	✓	✓	✓	✓	×	✓
Canard [73]	✓	×	✓	✓	✓	✓	✓	×	✓
Shao [43]	✓	✓	✓	×	✓	✓	✓	×	✓
Isshiki [46]	✓	×	✓	×	✓	✓	✓	×	✓

TABLE III
THE COMPUTATIONAL OVERHEAD COMPARISON OF PRE SCHEMES

Schemes	Computational Cost				Pairing Free?
	Encrypt	Decrypt_1	ReEncrypt	Decrypt_2	
Blaze [6]	$2S$	S	S	S	✓
Ateniese [12]-1	$S+2E$	$P+E$	P	P	×
Ateniese [12]-2	$S+2E$	$P+E$	P	P	×
Ateniese [13]	$S+2E$	$P+E$	P	P	×
Canetti [15]-1	$P+3S+E+\mathsf{Sig}$	$5P+S+\mathsf{Vfy}$	$4P+S+\mathsf{Vfy}$	$5P+S+\mathsf{Vfy}$	×
Canetti [15]-2	$P+3S+E+\mathsf{Sig}$	$5P+S+\mathsf{Vfy}$	$4P+S+\mathsf{Vfy}$	$5P+S+\mathsf{Vfy}$	×
Libert [30]-1	$P+5S+E+\mathsf{Sig}$	$3P+S+E+\mathsf{Vfy}$	$2P+4S+\mathsf{Vfy}$	$5P+S+E+\mathsf{Vfy}$	×
Libert [30]-2	$P+5S+E+\mathsf{Sig}$	$3P+S+E+\mathsf{Vfy}$	$2P+4S+\mathsf{Vfy}$	$5P+S+E+\mathsf{Vfy}$	×
Deng [29]	$3S$	$4S$	$3S$	$2S$	✓
Shao [31]-1	$5S$	$5S$	$4S$	$4S$	✓
Shao [31]-1	$5S$	$5S$	$4S$	$4S$	✓
Chow [36]	$3S$	$4S$	$3S$	$4S$	✓
Canard [73]	$7S+\mathsf{Sig}$	$7S$	$4S+\mathsf{Vfy}$	$7S$	✓
Shao [43]	$P+2S+2E+\mathsf{Sig}$	$3P+3S+E+\mathsf{Vfy}$	$6P+6S+3E+\mathsf{Sig}+\mathsf{Vfy}$	$9P+7S+3E+3\mathsf{Vfy}$	×
Isshiki [46]	$P+7S+\mathsf{Enc}$	$5P+S+E$	$4P+5S+\mathsf{Enc}$	$8P+3S+E+\mathsf{Dec}$	×

TABLE IV
THE STORAGE OVERHEAD AND SECURITY COMPARISON OF PRE SCHEMES

Schemes	Key Length			Ciphertext Length		Security
	Public Key	Private Key	Re-Encryption Key	Original	Transformed	
Blaze [6]	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$2\lvert\mathbb{Z}_p\rvert$	IND-$\text{CCA}_{0,0}$, RO, CDH
Ateniese [12]-1	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert$	$2\lvert\mathbb{G}_2\rvert$	IND-$\text{CCA}_{0,0}$, RO, q-DBDHI
Ateniese [12]-2	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	$2\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+3\lvert\mathbb{G}_2\rvert$	$2\lvert\mathbb{G}_2\rvert$	IND-$\text{CCA}_{0,0}$, RO, e-DBDH
Ateniese [13]	$2\lvert\mathbb{G}_1\rvert$	$2\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+3\lvert\mathbb{G}_2\rvert$	$2\lvert\mathbb{G}_2\rvert$	IND-$\text{CCA}_{0,0}$, RO, DBDH
Canetti [15]-1	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	IND-$\text{CCA}_{2,0}$, RO, m-DBDH
Canetti [15]-2	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	IND-$\text{CCA}_{2,2}$, ST, DBDH
Libert [30]-1	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}_1\rvert$	$4\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	$4\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	IND-$\text{CCA}_{1,2}$, ST, 3-qDBDH
Libert [30]-2	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}_1\rvert$	$4\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert+\lvert T\rvert$	$4\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert+\lvert T\rvert$	IND-$\text{CCA}_{1,2}$, ST, 4-qDBDH
Deng [29]	$\lvert\mathbb{G}\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$2\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_p\rvert+k_1+k_2$	$\lvert\mathbb{G}\rvert+k_1+k_2$	IND-$\text{CCA}_{2,2}$, RO, CDH
Shao [31]-1	$3\lvert N^2\rvert$	$2\lvert N^2\rvert+\lvert\mathbb{Z}_p\rvert$	$\lvert N_x^2\rvert+2\lvert N_y^2\rvert+k_1$	$\lvert\mathcal{M}\rvert+3\lvert N_x^2\rvert+2k$	$\lvert\mathcal{M}\rvert+3\lvert N_x^2\rvert+2\lvert N_y^2\rvert+k_1$	IND-$\text{CCA}_{2,2}$, RO, DDH
Shao [31]-2	$3\lvert N^2\rvert$	$2\lvert N^2\rvert+\lvert\mathbb{Z}_p\rvert$	$\lvert N_x^2\rvert+2\lvert N_y^2\rvert+k_1$	$\lvert\mathcal{M}\rvert+3\lvert N_x^2\rvert+2k$	$\lvert\mathcal{M}\rvert+3\lvert N_x^2\rvert+2\lvert N_y^2\rvert+k_1$	IND-$\text{CCA}_{2,2}$, RO, DDH
Chow [36]	$2\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_p\rvert+k_1+k_2$	$2\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_p\rvert+k_1+k_2$	$2\lvert\mathbb{G}\rvert+2k_1+2k_2$	IND-$\text{CCA}_{2,1}$, RO, CDH
Canard [73]	$2\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{Z}_p\rvert$	$4\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_p\rvert$	$3\lvert\mathbb{G}\rvert+3k_1+3k_2$	$2\lvert\mathbb{G}\rvert+3k_1+3k_2$	IND-$\text{CCA}_{2,0}$, RO, CDH
Shao [43]	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{Z}_p\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+2\lvert\mathbb{Z}_p\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	$\lvert\mathcal{M}\rvert+2\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert k_s\rvert+\lvert\sigma_s\rvert$	$\lvert\mathcal{M}\rvert+6\lvert\mathbb{G}_1\rvert+5\lvert\mathbb{G}_2\rvert+2\lvert\mathbb{Z}_p\rvert+2\lvert k_s\rvert+2\lvert\sigma_s\rvert$	IND-$\text{CCA}_{2,1}$, ST, 2-ABDHE
Isshiki [46]	$3\lvert\mathbb{G}_1\rvert$	$2\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{G}_1\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert\mathbb{Z}_p\rvert$	$2\lvert\mathbb{G}_1\rvert+\lvert Sym_{Enc}\rvert$	IND-$\text{CCA}_{2,2}$, ST, 6-AmDBDH

during the attack. The security model for unidirectional proxy re-signatures formalized by Ateniese and Hohenberger [14] includes both *external attack* and *internal attack*. The former attack attempts to capture the attacks mounted by the parties excluding the proxy and any delegation parties. The latter attack attempts to simulate the attack launched by a party inside the system such as the proxy, another delegation partner, or some collusion between them. In this way, the security model for proxy re-signature mainly includes *external security* and *internal security*.

Suppose there are *n*+1 users with key pairs (pk_i, sk_i) for $i \in \{0, 1, \cdots, n\}$, without loss of generality, we assume the adversary attempts to forge the signature under the public key of user indexed by 0; we first define the oracles that an adversary has access to:

- $\mathcal{O}_{Sign}(j, m)$: On input an index $0 \leq j \leq n$ and a message $m \in \mathcal{M}$, the signature generation oracle $\mathcal{O}_{Sign}(j, m)$ returns the output of $\mathsf{Sign}(sk_j, m)$.
- $\mathcal{O}_{ReKey}(i, j)$: On input two distinct indices $1 \leq i, j \leq n$, the re-signature key generation oracle $\mathcal{O}_{ReKey}(i, j)$ returns the output of $\mathsf{ReKey}(pk_i, sk_i, pk_j, sk_j)$.
- $\mathcal{O}_{ReSign}(i, j, m, \sigma)$: On input two distinct indices $1 \leq i, j \leq n$, a message *m* and a signature σ, the re-signature generation oracle $\mathcal{O}_{ReSign}(i, j, m, \sigma)$ returns the output of $\mathsf{ReSign}(\mathsf{ReKey}(pk_i, sk_i, pk_j, sk_j), \sigma, pk_i, m)$.

External Security aims to protect a user from adversaries outside the system (i.e., excluding the proxy and any delegation partners). This is the proxy equivalent of strong existential unforgeability under adaptive chosen-message attack where an external adversary $\mathcal{A}_{ext}$ cannot create a new signature even for a previously signed message [79] by accessing to $\mathcal{O}_{Sign}$ and $\mathcal{O}_{ReSign}$. For some applications, it may also make sense to only require the standard notion of existential unforgeability where a forgery must be on a new message [78].

Definition 6 (External Security): A proxy re-signature scheme is secure against external adversaries $\mathcal{A}_{ext}(k)$ if the probability of winning the following experiment is a negligible function of k.

Experiment $\mathbf{Exp}_{\mathcal{A}_{ext}}(k)$:

$$(pk_i, sk_i) \leftarrow \mathsf{KeyGen}(k)_{i\in\{0,\cdots,n\}}$$
$$(m, \sigma) \leftarrow \mathcal{A}_{ext}^{\mathcal{O}_{\mathsf{Sign}}(\cdot,\cdot),\mathcal{O}_{\mathsf{ReSign}}(\cdot,\cdot,\cdot,\cdot)}(\{pk_i\}_{i\in\{0,\cdots,n\}})$$

$\mathcal{A}_{ext}$is said to win this experiment if and only if

$$(m, \sigma) \notin \mathcal{L}_{ext} \quad \text{and} \quad \mathsf{Verify}(pk_0, m, \sigma) = 1$$

where $\mathcal{L}_{ext}$ is defined as the list of items (m, σ) where $\mathcal{A}_{ext}$ has obtained a signature σ on the message m by querying $\mathcal{O}_{Sign}(0, m)$ and $\mathcal{O}_{ReSign}(\cdot, 0, m, \cdot)$.

The aim of the *Internal Security* is to simulate the attack mounted by a rogue proxy and/or delegation partner (who may be colluding). Intuitively, internal attacks allow accesses to $\mathcal{O}_{Sign}$ and $\mathcal{O}_{ReKey}$ and there are three guarantees to make: *Limited Proxy*, *Delegatee Security* and *Delegator Security*.

In the security notion of *Limited Proxy*, if the delegator and the delegatee are both honest, then the proxy neither produces signatures for the delegator unless the message was first signed by one of her delegatees, nor create any signatures for the delegatee.

Definition 7 (Limited Proxy Security): A proxy re-signature scheme is secure against limited proxy adversaries $\mathcal{A}_{pro}(k)$ if the probability of winning the following experiment is a negligible function of *k*.

Experiment $\mathbf{Exp}_{\mathcal{A}_{pro}}(k)$:

$$(pk_i, sk_i) \leftarrow \mathsf{KeyGen}(k)_{i\in\{0,\cdots,n\}}$$
$$(m, \sigma) \leftarrow \mathcal{A}_{pro}^{\mathcal{O}_{\mathsf{Sign}}(\cdot,\cdot),\mathcal{O}_{\mathsf{ReKey}}(\cdot,\cdot)}(\{pk_i\}_{i\in\{0,\cdots,n\}})$$

$\mathcal{A}_{pro}$is said to win this experiment if and only if

$$(m, \sigma) \notin \mathcal{L}_{pro} \quad \text{and} \quad \mathsf{Verify}(pk_0, m, \sigma) = 1$$

where $\mathcal{L}_{pro}$ is defined as the list of items (m, σ) where $\mathcal{A}_{pro}$ has obtained a signature σ on the message m by querying $\mathcal{O}_{Sign}(\star, m)$, for $\star = 0$ or any $\star$ where $\mathcal{O}_{ReKey}(\star, 0)$ has been queried.

In the security notion of *Delegatee Security*, if the delegatee is honest, then he is "safe" from a colluding delegator and proxy. That is, they cannot produce any signatures on his behalf.

Definition 8 (Delegatee Security): A proxy re-signature scheme is delegatee secure against collusion of delegator and proxy adversaries $\mathcal{A}_{dtee}(k)$ if the probability of winning the following experiment is a negligible function of *k*.

Experiment $\mathbf{Exp}_{\mathcal{A}_{dtee}}(k)$:

$$(pk_i, sk_i) \leftarrow \mathsf{KeyGen}(k)_{i\in\{0,\cdots,n\}}$$
$$(m, \sigma) \leftarrow \mathcal{A}_{dtee}^{\mathcal{O}_{\mathsf{Sign}}(0,\cdot),\mathcal{O}_{\mathsf{ReKey}}(\cdot,t)}(pk_0, \{pk_i, sk_i\}_{i\in\{1,\cdots,n\}})$$

$\mathcal{A}_{dtee}$is said to win this experiment if and only if

$$(m, \sigma) \notin \mathcal{L}_{dtee} \quad \text{and} \quad \mathsf{Verify}(pk_0, m, \sigma) = 1$$

where $t \neq 0$ and $\mathcal{L}_{dtee}$ is defined as the list of items (m, σ) where $\mathcal{A}_{dtee}$ has obtained a signature σ on the message m by querying $\mathcal{O}_{Sign}(0, m)$.

Finally, in the security notion of *Delegator Security*, if the delegator is honest, then she is "safe" from a colluding delegatee and proxy. That is, the colluding delegatee and proxy cannot produce strong signatures on her behalf.

Definition 9 (Delegator Security): A proxy re-signature scheme is delegator secure against collusion of delegatee and proxy adversaries $\mathcal{A}_{dtor}(k)$ if the probability of winning the following experiment is a negligible function of *k*.

Experiment $\mathbf{Exp}_{\mathcal{A}_{dtor}}(k)$:

$$(pk_i, sk_i) \leftarrow \mathsf{KeyGen}(k)_{i\in\{0,\cdots,n\}}$$
$$(m, \sigma) \leftarrow \mathcal{A}_{dtor}^{\mathcal{O}_{\mathsf{Sign}}(0,\cdot),\mathcal{O}_{\mathsf{ReKey}}(\cdot,\cdot)}(pk_0, \{pk_i, sk_i\}_{i\in\{1,\cdots,n\}})$$

$\mathcal{A}_{dtor}$is said to win this experiment if and only if

$$(m, \sigma) \notin \mathcal{L}_{dtor} \quad \text{and} \quad \mathsf{Verify}(pk_0, m, \sigma) = 1$$

where σ is an untransformed signature which is outputted by the Sign algorithm instead of ReSign, and $\mathcal{L}_{dtor}$ is defined as the list of items (m, σ) where $\mathcal{A}_{dtor}$ has obtained a signature σ on the message m by querying $\mathcal{O}_{Sign}(0, m)$.

The above model covers almost all types of forgeries for proxy re-signatures, but it omits one type of forgeries that the delegatee may aim to produce signatures on behalf of the delegator without colluding with the proxy. For example, for the transformation path: user $i \rightarrow$ the proxy $\rightarrow$ user j. User i may attempt to produce a transformed signature on

a message on behalf of user j without the transformation of the proxy. This situation is not allowed in the proxy re-signature schemes with private re-signature key, since user j has delegated his signing rights via proxy but not to user i directly. The schemes suffering from this attack cannot be used in most of the applications of PRS listed in [6]. Hence, in [80], Shao *et al.* proposed a clearer and simpler security model based on the Ateniese and Hohenberger security model for an unidirectional proxy re-signature scheme with private re-signature key.

B. Special PRE Schemes

1) The Conditional-based Formulation: Despite PRE has been applied to many practical scenarios already, it is non-trivial to deploy ordinary PRE schemes in the environments where the conditional transformation is necessary. To meet this requirement, Weng *et al.* [33] proposed the definition of conditional proxy re-encryption (C-PRE). In this PRE paradigm, the re-encryption key contains a partial re-encryption key $rk_{i\to j}$ and a conditional key $ck_{i\to j}$. The proxy is allowed to make a transformation from user i's ciphertext into user j's ciphertext if and only if user i's ciphertext meets a specific condition set by herself. In general, the definition of C-PRE are described as follows, where the KeyGen, ReKey and Decrypt algorithms are omitted since these algorithms are identical to those in the typical PRE schemes.

- C-ReKey: On input user i's private key sk_i and a specific condition ω, the conditional key generation algorithm C-ReKey is run by user i to generate a conditional key $ck_{i\to j}$.
- Encrypt: User i executes this encryption algorithm by inputting a plaintext message $m \in \mathcal{M}$, a public key pk_i and a condition ω set by user i. Then it outputs the ciphertext $c_i \in \mathcal{C}$ associated with ω under the public key pk_i.
- ReEncrypt: Take as input user i's ciphertext c_i associated with ω under pk_i, the partial re-encryption key $rk_{i\to j}$ and the conditional key $ck_{i\to j}$ associated with ω, this algorithm is implemented by the proxy to produce a re-encrypted ciphertext $c_{i\to j} \in \mathcal{C}'$ for user j.

As described above, both $rk_{i\to j}$ and $ck_{i\to j}$ are needed by the proxy to perform ciphertext transformations from user i (the delegator) into user j (the delegatee). It is impossible for the proxy to transform user i's ciphertext associated with the specific condition ω which is not available. Hence, in a C-PRE scheme, the delegator has a fine-grained and flexible control on ciphertext transformations by releasing proper conditional keys.

2) The Type-based Formulation: Type-based proxy re-encryption (T-PRE) is a novel notion presented by Tang *et al.* [81]. It is designed for scenarios requiring fine-grained ciphertext transformations. In a T-PRE scheme, the plaintext messages are divided into different types and the proxy is only allowed to re-encrypt a subset of the delegator's ciphertext associated with type t. The ciphertext associated with type t can be regarded as a type-based ciphertext which enables to be re-encrypted by the proxy. Furthermore, there exists a regular ciphertext which cannot be transformed. The changes in T-PRE are described as follows.

- T-ReKey: Besides user i's and user j's key pairs, this algorithm should also take as input a message type t associated with the message $m \in \mathcal{M}$ to generate a type-based re-encryption key $rk^t_{i\to j}$.
- Encrypt$_t$: Take as input user i's public key pk_i, a message $m \in \mathcal{M}$ and a message type t associated with the message $m \in \mathcal{M}$, this algorithm is performed by user i to output a type-based ciphertext c^t_i.
- Encrypt: On input a message $m \in \mathcal{M}$ and user i's public key pk_i, the regular encryption algorithm outputs a regular ciphertext c_i.
- ReEncrypt: On input a type-based re-encryption key $rk^t_{i\to j}$, a message type t and a type-based ciphertext c^t_i, this algorithm is performed by the proxy to produce the re-encrypted ciphertext $c_{i\to j}$ which is a regular ciphertext.
- Decrypt$_t$: For a type-based ciphertext, this algorithm is run by inputting a type-based ciphertext c^t_i, a message type t and user i's private key sk_i. It outputs a message $m \in \mathcal{M}$ or the error symbol $\perp$ indicating c^t_i is invalid.
- Decrypt: For a regular ciphertext, this algorithm is run by inputting a regular ciphertext c_i for user i and the corresponding private key sk_i. It outputs a message $m \in \mathcal{M}$ or the error symbol $\perp$ indicating c is invalid.

In the above description of the T-PRE, the message type *t* is usually embedded in the type-based ciphertext c^t_i as a label of this ciphertext.

3) The Searchable Formulation: Shao *et al.* [40] presented the notion of proxy re-encryption with keyword search (S-PRE). As a motivating exmaple, in an encrypted e-mail environment, S-PRE allows an e-mail server as the proxy with a searchable re-encryption key to transform a encrypted keyword ω under pk_i for user i into the same encrypted keyword under pk_j for user j. Moreover, with a trapdoor from user j (the delegatee), only user j's e-mail server can test whether or not the e-mail delegated from user i (the delegator) includes certain keywords. The e-mail server cannot learn any information from the e-mails. Generally, a S-PRE scheme consists of the following algorithms.

- Trapdoor: On input a private key sk_i for user i and a keyword ω, this algorithm is run by user i to generate a trapdoor $T_{i,\omega}$ associated with the keyword ω. The trapdoor should be sent to a designated tester.
- Encrypt: On input a public key pk_i for user i, a message $m \in \mathcal{M}$ and a keyword ω extracted from message m, it generates a ciphertext $c_i \in \mathcal{C}$ associated with the keyword ω under the public key pk_i.
- Test: On input a public key pk_j, a re-encrypted ciphertext $c_{i\to j}$ and the trapdoor $T_{j,\omega}$ for user j, this algorithm is run by a tester designated by user i to test whether or not $c_{i\to j}$ contains the keyword ω. It returns 1 if $\omega = \omega'$ and 0 otherwise. (ω' denotes the keyword of the ciphertext $c_{i\to j}$.)

C. Applications Using PRC

1) Data Sharing in Cloud Computing: Despite the abundant resource provided by the cloud computing, data owners'

concerns about the privacy of their outsourced data such that these data can only be accessed by the authorized parties become the main obstacles impede cloud computing from spread adoption, especially if the cloud server is only semi-trusted. As described in Section I, proxy re-encryption is a promising candidate to enable secure data sharing in the cloud computing. In view of the special translation of PRE, Wu *et al.* [82, 69] constructed a certificateless-based PRE scheme and applied this scheme to secure data sharing in the cloud computing environment. In their protocol, the approach of hybrid encryption is adopted by enjoying the merits of public key encryption and symmetric encryption together. Concretely, the shared data is encrypted by a symmetric encryption algorithm with the data encryption key (DEK). Then, the DEK is encrypted using the asymmetric encryption under the public key of the data owner. After receiving the ciphertext of the DEK, PRE is used by the cloud server to transform the encrypted DEK into the encryption that can only be decrypted by the granted recipient's private key. Then the recipient can download the encrypted data from the cloud and use the DEK for decryption.

To realize fine-grained access control on encrypted data and secure data sharing, Yu *et al.* [66] proposed a secure data sharing protocol in the cloud by integrating the techniques of key policy attribute-based encryption (KP-ABE), PRE and lazy re-encryption. More specifically, they associate each data file with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. To enforce this kind of access control, they utilize KP-ABE to encrypt data encryption keys of data files. Such a construction enjoys fine-grained access control immediately but suffers from heavy computation overhead and cumbersome online burden mainly caused by the operation of user revocation. To resolve this challenging issue and make the construction suitable for cloud computing, they uniquely combine PRE with KP-ABE and enable the data owner to delegate most of the computation intensive operations to cloud servers without disclosing the underlying encrypted file. Such a construction allows the data owner to control access of his data files with a minimal overhead. Furthermore, they take advantage of the lazy re-encryption technique and allow cloud servers to aggregate computation tasks of multiple system operations. Their protocol also has salient properties of user access privilege confidentiality and user secret key accountability.

To deal with the user revocation and fine-grained access control, Liu *et al.* [50] presented a time-based PRE scheme such that a user's access right expires automatically after a predetermined period of time. In this circumstance, re-encryption keys can be generated off-line and delivered to the cloud server in time by the data owner, which ensures that the revoked user cannot access the future data and avoids potential security risks caused by the retard of producing re-encryption keys. In their scheme, each data is associated with two access tree structures, which indicate a set of attribute and a set of time periods, respectively. The access time structure represents the valid time of the access right for a cloud user, who should be identified by the attribute-based access tree. To enable the transformation, a root private key should be shared by the data owner and the cloud serve during the initial stage. Then, with the root private key, the cloud server can deal with the updating of access time tree for a certain data after getting the time of the data access request. As a result, given the re-encryption keys, the cloud server can transform the data owner's ciphertext into the data recipients' ciphertext and only the data recipients whose attributes meet the access control tree and access rights meet the access time tree are enabled to decrypt corresponding re-encrypted ciphertext.

2) Encrypted Email Forwarding: In the encrypted email forwarding system, the email containing sensitive information should be encrypted under the recipient's public key before being sent to this recipient. After that, only the legitimate recipient is able to decrypt this email using his/her own private key. However, sometimes it is necessary for the recipient delegate his colleague to check the emails on behalf of himself in case this recipient is on a journey or cannot access the Internet. It is unwise for the recipient to disclose his own private key to the colleague directly. However, there was no suitable cryptographic primitive to solve this problem effectively and securely until the PRE primitive was proposed. By utilizing the PRE primitive in a encryption email system, the granted recipient first generates a re-encryption key using his own private key and the delegatee's public key, and delegates this key to a email server. Then relying on the PRE scheme the email server can achieve transformations from the recipient's encrypted emails into the delegatee's encrypted emails without disclosing any information. Finally, the delegatee can check the delegator's encrypted emails conveniently with his own private key. Crucially, the private key for the recipient is protected from being disclosed in this email system.

3) Digital Rights Management: The digital rights management (DRM) is developed to prevent digital contents from being copied and redistributed illegally by binding a digital content and a unique license together. In such a DRM system, the value of digital content can be protected by bounding digital content to a license such that the content can only be accessed under the terms stated by the license. However, most DRM systems cannot support inter-operation due to the lack of standardization. Therefore, it is non-trivial for the consumers to read the content they have purchased on the device of their choice. In order to achieve inter-operability among different DRM systems, Taban *et al.* [7] introduced the primitive of PRS and PRE into DRM. Taban *et al.* added a domain interoperability manager (DIM) with capabilities of signature and ciphertext transformations to the traditional DRM system. With leveraging additional delegations, DIM is allowed to transform the encrypted digital content along with its licence for device A into ones on the same digital content for device B without disclosing any information. In this way, the digital content can be accessed from different devices under the protection of DRM.

4) Vehicular Ad Hoc Networks: By enabling vehicles to communicate with other vehicles or roadside units (RSUs) via the equipped on-board units (OBUs) communication devices, vehicular ad hoc networks (VANETs) can be formed to offer a more efficient and comfortable driving experience. Generally, VANETs includes a top trusted authority (TA), the immobile

RSUs at the roadside, and the moving vehicles equipped with OBUs. Despite its attracting characteristics, the communication trust and privacy issues in VANET should be carefully addressed in view of the open-medium nature of wireless communications and the high-speed mobility of the OBUs. To ensure the authentication of the disseminated message in VANETs, a naive approach for the OBU is to issue a signature on the message before broadcasting this message. Upon receiving a message along with the corresponding signature, the receiver (i.e., the RSU or other OBUs) first verifies the validity of the signature and then forwards this message/signature pair again. However, during this process a malicious adversary (e.g. RSU, or malicious OBUs) may trace the OBU's private information such as identity and location privacy. To address the trust and privacy issues in VANETs, Xiong *et al.* [9] put forward an authentication protocol with privacy preservation by using a single-use PRS scheme. In their authentication protocol, the RSU is able to transform a signature from a OBU into another signature from TA on the traffic message without revealing any private information of the OBU. This conceals the real identity of the OBU from malicious adversary.

V. Related Work

By considering the rich achievements in the field of PRE, it is somewhat surprising that none of the comprehensive survey has been proposed till now. In 2012, Cao [83] presented a monograph focusing on the modern cryptography including the topic of PRE. This monograph focuses more on the specific security models and constructions, while we are interested in looking at the PRE primitive in a more systematic manner. In 2013, Inbarani *et al.* [84] surveyed a variety of PRE techniques roughly. This survey does not sufficiently highlight features particular to PRE schemes. Moreover, the syntax, security models and design philosophy are omitted in their survey.

VI. Future Work and Conclusion

As a promising primitive to secure the data sharing in the cloud computing, PRE has captured a lot of concern due to the delegation function of decryption. In this paper, we reviewed the state-of-the-art of the PRE by investigating the design philosophy, examining the security models, and comparing the efficiency of existing schemes. Furthermore, the potential applications and extensions of PRE have also been discussed. There are some possible interesting problems in this research field that need further investigation.

1) One direct open problem of PRC is how to design a generic framework which can transform the ordinary encryption/signature to proxy re-encryption/re-signature.
2) Bearing the quantum computing in the mind, it is natural to construct PRC schemes based on the lattice-based cryptography or multi-variable public key cryptosystem.
3) Finding the efficient PRE schemes with full security is also an open problem since most of the existing PRE schemes can only achieve selective security.
4) Identifying new scenarios where the decryption/signing rights of the resource-limited users can be delegated to the resource-abundant proxy by adapting the existing PRC schemes to feature with special properties can be regarded as another open problem.

Acknowledgment

This work is partially supported by National Natural Science Foundation of China under Grant Nos. 61003230, 61370026 and 61300191 and the National High Technology Research and Development Program of China (863) under Grant 2015AA016007.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in *33rd International Convention on Information and Communication Technology, Electronics and Microelectronics*. IEEE, 2010, pp. 344–349.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, no. 1, pp. 69–73, 2012.

[4] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 556–568, 2012.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[6] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology–EUROCRYPT'98*. Springer, 1998, pp. 127–144.

[7] G. Taban, A. A. Cárdenas, and V. D. Gligor, "Towards a secure and interoperable drm architecture," in *Proceedings of the ACM Workshop on Digital Rights Management*. ACM, 2006, pp. 69–78.

[8] S. Lee, H. Park, and J. Kim, "A secure and mutual-profitable drm interoperability scheme," in *Proceedings of IEEE Symposium on Computers and Communications*. IEEE, 2010, pp. 75–80.

[9] H. Xiong, Z. Chen, and F. Li, "Efficient privacy-preserving authentication protocol for vehicular communications with trustworthy," *Security and Communication Networks*, vol. 5, no. 12, pp. 1441–1451, 2012.

[10] T. Yang, H. Xiong, J. Hu, Y. Wang, W. Xin, Y. Deng, and Z. Chen, "A traceable privacy-preserving authentication protocol for vanets based on proxy re-signature," in *8th International Conference on Fuzzy Systems and Knowledge Discovery*, vol. 4. IEEE, 2011, pp. 2217–2221.

[11] Y.-R. Chen, J. Tygar, and W.-G. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in *IEEE International Conference on Computer Communications*. IEEE, 2011, pp. 1952–1960.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proceedings of the 2005 Symposium on Network and Distributed System Security*, 2005.

[13] ——, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC'06)*, vol. 9, no. 1, pp. 1–30, 2006.

[14] G. Ateniese and S. Hohenberger, "Proxy re-signatures: new definitions, algorithms, and applications," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*. ACM, 2005, pp. 310–319.

[15] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 185–194.

[16] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1786–1802, 2011.

[17] J. Weng, R. H. Deng, S. Liu, and K. Chen, "Chosen-ciphertext secure bidirectional proxy re-encryption schemes without pairings," *Information Sciences*, vol. 180, no. 24, pp. 5077–5089, 2010.

[18] E. Kirshanova, "Proxy re-encryption from lattices," in *Public Key Cryptography–PKC'14*. Springer, 2014, pp. 77–94.

[19] N. David, A. Isaac, and L. Javier, "Ntrureencrypt: An efficient proxy re-encryption scheme based on ntru," in *Proceedings of the 10^{th} ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15)*. ACM, 2015, pp. 179–189.

[20] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in *Advances in CryptologyłCRYPTO'98*. Springer, 1998, pp. 26–45.

[21] D. Nunez, I. Agudo, and J. Lopez, "A parametric family of attack models for proxy re-encryption," in *IEEE 28th Computer Security Foundations Symposium (CSF 2015)*. IEEE, 2015, pp. 290–301.

[22] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in *Topics in Cryptology–CT-RSA'09*. Springer, 2009, pp. 279–294.

[23] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology–CRYPTO'85*. Springer, 1985, vol. 196, pp. 10–18.

[24] M. Jakobsson, "On quorum controlled asymmetric proxy re-encryption," in *2nd International Workshop on Practice and Theory in Public Key Cryptography*. Springer, 1999, pp. 112–121.

[25] A.-A. Ivan and Y. Dodis, "Proxy cryptography revisited," in *Proceedings of the 2003 Symposium on Network and Distributed System Security*, 2003.

[26] R. Canetti, H. Krawczyk, and J. B. Nielsen, "Relaxing chosen-ciphertext security," in *Advances in Cryptology–CRYPTO'03*. Springer, 2003, pp. 565–582.

[27] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proceedings of the 5th International Conference on Applied Cryptography and Network Security*. Springer, 2007, pp. 288–306.

[28] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology–CRYPTO'01*. Springer, 2001, pp. 213–229.

[29] R. H. Deng, J. Weng, S. Liu, and K. Chen, "Chosen-ciphertext secure proxy re-encryption without pairings," in *Proceedings of the 7th International Conference on Cryptology and Network Security*. Springer, 2008, pp. 1–17.

[30] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in *Public Key Cryptography–PKC'08*. Springer, 2008, pp. 360–379.

[31] J. Shao and Z. Cao, "Cca-secure proxy re-encryption without pairings," in *Public Key Cryptography–PKC'09*. Springer, 2009, pp. 357–376.

[32] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*. ACM, 2009, pp. 276–286.

[33] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*. ACM, 2009, pp. 322–332.

[34] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional proxy re-encryption with chosen-ciphertext security," in *Proceedings of the 12th International Conference on Information Security*. Springer, 2009, pp. 151–166.

[35] J. Weng, M. Chen, Y. Yang, R. Deng, K. Chen, and F. Bao, "Cca-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles," *Science China Information Sciences*, vol. 53, no. 3, pp. 593–606, 2010.

[36] S. S. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient unidirectional proxy re-encryption," in *Progress in Cryptology–AFRICACRYPT'10*. Springer, 2010, pp. 316–332.

[37] T. Matsuda, R. Nishimaki, and K. Tanaka, "Cca proxy re-encryption without bilinear maps in the standard model," in *Public Key Cryptography–PKC'10*. Springer, 2010, pp. 261–278.

[38] C. Sur, C. D. Jung, Y. Park, and K. H. Rhee, "Chosen-ciphertext secure certificateless proxy re-encryption," in *Proceedings of the 11th International Conference Communications and Multimedia Security*. Springer, 2010, pp. 214–232.

[39] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology–ASIACRYPT'03*. Springer, 2003, pp. 452–473.

[40] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576–2587, 2010.

[41] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-

encryption without random oracles," in *Proceedings of the 10th International Conference on Information Security*. Springer, 2007, pp. 189–202.

[42] J. Weng, Y. Zhao, and G. Hanaoka, "On the security of a bidirectional proxy re-encryption scheme from pkc 2010," in *Public Key Cryptography–PKC'11*. Springer, 2011, pp. 284–295.

[43] J. Shao, P. Liu, Z. Cao, and G. Wei, "Multi-use unidirectional proxy re-encryption," in *IEEE International Conference on Communications*. IEEE, 2011, pp. 1–5.

[44] G. Hanaoka, Y. Kawai, N. Kunihiro, T. Matsuda, J. Weng, R. Zhang, and Y. Zhao, "Generic construction of chosen ciphertext secure proxy re-encryption," in *Topics in Cryptology–CT-RSA'12*. Springer, 2012, pp. 349–364.

[45] J. Shao, P. Liu, and Y. Zhou, "Achieving key privacy without losing cca security in proxy re-encryption," *Journal of Systems and Software*, vol. 85, no. 3, pp. 655–665, 2012.

[46] T. Isshiki, M. H. Nguyen, and K. Tanaka, "Proxy re-encryption in a stronger security model extended from ct-rsa2012," in *Topics in Cryptology–CT-RSA'13*. Springer, 2013, pp. 277–292.

[47] L. Fang, W. Jiandong, G. Chunpeng, and R. Yongjun, "Fuzzy conditional proxy re-encryption," *SCIENCE CHINA Information Sciences*, vol. 56, no. 5, pp. 1–13, 2013.

[48] J. Zhang, Z. Zhang, and Y. Chen, "Pre: Stronger security notions and efficient construction with non-interactive opening," *Theoretical Computer Science*, vol. 542, no. 0, pp. 1–16, 2014.

[49] H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys," in *Proceedings of the 13th International Conference on Cryptology and Network Security*. Springer, 2014, pp. 20–33.

[50] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Information Sciences*, vol. 258, pp. 355–370, 2014.

[51] T. Fei, L. Hongda, and J. Chang, "Multi-hop unidirectional proxy re-encryption from multilinear maps," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 98, no. 2, pp. 762–766, 2015.

[52] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices." in *Advances in Cryptology–Eurocrypt'13*, vol. 7881. Springer, 2013, pp. 1–17.

[53] D. Hua, W. Qianhong, Q. Bo, S. Willy, L. Joseph, and S. Wenchang, "Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data," in *Proceedings of the 10^{th} ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15)*. ACM, 2015, pp. 393–404.

[54] Z. Yunya, D. Hua, W. Qianhong, Q. Bo, L. Jianwei, and D. Yong, "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," *Future Generation Computer Systems*, p. in press, 2015.

[55] W. K. Koo, J. Y. Hwang, and D. H. Lee, "Security vulnerability in a non-interactive id-based proxy re-encryption scheme," *Information Processing Letters*, vol. 109, no. 23, pp. 1260–1262, 2009.

[56] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in *IEEE International Conference on Communications*. IEEE, 2011, pp. 1–5.

[57] Y. Ren, D. Gu, S. Wang, and X. Zhang, "Hierarchical identity-based proxy re-encryption without random oracles," *International Journal of Foundations of Computer Science*, vol. 21, no. 06, pp. 1049–1063, 2010.

[58] K. Emura, A. Miyaji, and K. Omote, "An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system," in *7th European Workshop on Public Key infrastructures, Services and Applications*. Springer, 2011, pp. 77–92.

[59] J. Zhang and X. A. Wang, "Security analysis of a multi-use identity based cca-secure proxy re-encryption scheme," in *Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems*. IEEE, 2012, pp. 581–586.

[60] H. Wang, Z. Cao, and L. Wang, "Multi-use and unidirectional identity-based proxy re-encryption schemes," *Information Sciences*, vol. 180, no. 20, pp. 4042–4059, 2010.

[61] J. Shao, "Anonymous id-based proxy re-encryption," in *Proceedings of the 17th Australasian Conference on Information Security and Privacy*. Springer, 2012, pp. 364–375.

[62] J. Shao and Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption," *Information Sciences*, vol. 206, pp. 83–95, 2012.

[63] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in *1st International Conference on Pairing-Based Cryptography-Pairing 2007*. Springer, 2007, pp. 247–267.

[64] C. Ling and C. N. Calvin, "Provably secure ciphertext policy abe," in *ACM Conference on Computer and Communications Security 2007*. ACM, 2007, pp. 456–465.

[65] S. Luo, J. Hu, and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption," in *Proceedings of the 12th International Conference on Information and Communications Security*. Springer, 2010, pp. 401–415.

[66] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proceedings of IEEE International Conference on Computer Communications*. IEEE, 2010, pp. 1–9.

[67] ——, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ACM, 2010, pp. 261–270.

[68] B. Libert and J.-J. Quisquater, "On constructing certificateless cryptosystems from identity based encryption," in *Public Key Cryptography–PKC'06*. Springer, 2006, pp. 474–490.

[69] L. Xu, X. Wu, and X. Zhang, "Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with

public cloud," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*. ACM, 2012, pp. 87–88.

[70] H. Guo, Z. Zhang, J. Zhang, and C. Chen, "Towards a secure certificateless proxy re-encryption scheme," in *Proceedings of the 7th International Conference on Provable Security*. Springer, 2013, pp. 330–346.

[71] K. Yang, J. Xu, and Z. Zhang, "Certificateless proxy re-encryption without pairings," in *Proceedings of the 16th International Conference on Information Security and Cryptology*. Springer, 2014, pp. 67–88.

[72] Z. Qin, S. Wu, and H. Xiong, "Strongly secure and cost-effective certificateless proxy re-encryption scheme for data sharing in cloud computing," in *Big Data Computing and Communications*. Springer, 2015, pp. 205–216.

[73] S. Canard, J. Devigne, and F. Laguillaumie, "Improving the security of an efficient unidirectional proxy re-encryption scheme," *Journal of Internet Services and Information Security*, vol. 1, no. 2, pp. 140–160, 2011.

[74] J. Shao, Z. Cao, L. Wang, and X. Liang, "Proxy re-signature schemes without random oracles," in *Progress in Cryptology–Indocrypt'07*. Springer, 2007, pp. 197–209.

[75] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*. ACM, 2008, pp. 511–520.

[76] S. Jun, W. Guiyi, L. Yun, and X. Mande, "Unidirectional identity-based proxy re-signature," in *IEEE International Conference on Communications (ICC 2011)*. IEEE, 2011, pp. 1–5.

[77] M. Tian, "Identity-based proxy re-signatures from lattices," *Information Processing Letters*, vol. 115, no. 4, pp. 462–467, 2015.

[78] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[79] J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," in *Advances in Cryptology–Eurocrypt'02*. Springer, 2002, pp. 83–107.

[80] J. Shao, M. Feng, B. Zhu, Z. Cao, and P. Liu, "The security model of unidirectional proxy re-signature with private re-signature key," in *Proceedings of the 15th Australasian Conference on Information Security and Privacy*. Springer, 2010, pp. 216–232.

[81] Q. Tang, "Type-based proxy re-encryption and its construction," in *Progress in Cryptology–INDOCRYPT 2008*. Springer, 2008, pp. 130–144.

[82] X. Wu, L. Xu, and X. Zhang, "Poster: a certificateless proxy re-encryption scheme for cloud-based data sharing," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 869–872.

[83] Z. Cao, *New Directions of Modern Cryptography*. CRC Press, 2012.

[84] W. S. Inbarani, G. Shenbagamoorthy, and C. K. C. Paul, "Proxy re-encryption schemes for data storage security in cloud-a survey," *International Journal of Engineering Research and Technology*, vol. 2, no. 1, 2013.

Zhiguang Qin is a professor in the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC). He received his PH.D. degree from UESTC in 1996. His research interests include information security and computer network.

Hu Xiong received his Ph.D. degree in the School of Computer Science and Engineering from UESTC in 2009. He is currently an associate professor in the School of Information and Software Engineering, UESTC. His research interests include cryptographic protocols and network security.

Shikun Wu received his B.S. degree in the School of Computer Science and Engineering, Anhui University of Science and Technology (AUST) in 2013. He is currently pursuing his M.S. degree in the School of Information and Software Engineering, UESTC. His research interests include cryptographic protocols and network security.

Jennifer Batamuliza received her B.S. Degree in School of Computer Engineering, Kigali Institute of Science and Technology (KIST) in 2012. She is currently pursuing her M.S. degree in the School of Computer Science and Engineering, UESTC. Her research interests include cryptographic protocols and network security.