ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

Isolation -Protect Alternate Re-Encryption for Records Allocation in Cloud Computing

S.Kavitha [1], C.K. Hemantha Rama [2]

M.Tech, Department of Computer Engineering, Sree Rama Engineering College, Tirupati, A.P, India[1]

Assistant Professor, Department of Computer Engineering, Sree Rama Engineering College, Tirupati, A.P, India[2]

ABSTRACT: we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication. 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 semitrusted 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.

I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources [2], [3]. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. To protect data privacy and combat unsolicited accesses in the cloud and beyond, sensitive data, for example, e-mails, personal health records, photo albums, tax documents, financial transactions, and so on, may have to be encrypted by data owners before outsourcing to the commercial public cloud [4]; this, however, obsoletes the traditional data utilization service based on plaintext keyword search. The trivial solution of downloading all the data and decrypting locally is clearly impractical, due to the huge amount of bandwidth cost in cloud scale systems. Moreover, aside from eliminating the local storage management, storing data into the cloud serves no purpose unless they can be easily searched and utilized. Thus, exploring privacypreserving and effective search service over encrypted cloud data is of paramount importance.
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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

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.

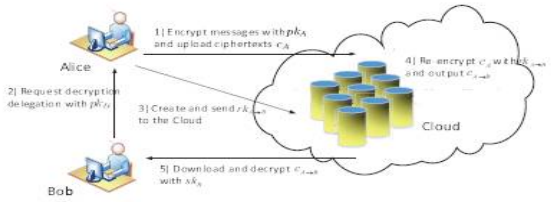

Fig. 1. Secure Data Sharing with PRE in Cloud Computing.

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.

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

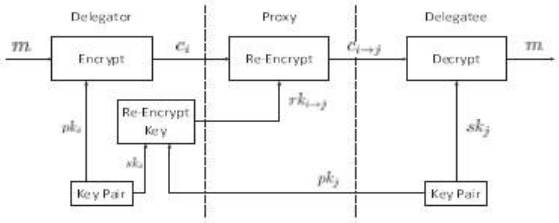

Fig. 2. The intuition of Proxy Re-Encryption Primitive.

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, INDCCA1 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 INDCPA 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.

III. SURVEYING PROXY RE-ENCRYPTION SCHEMES

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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

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.

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 identitybased 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.

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 attributebased PRE (AB-PRE), where the delegator associated with some specified attributes could freely allow a proxy to reencrypt a ciphertext with respect to a certain access policy to another encryption under a different access policy.

***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.

B. 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 G1, by E a exponentiation in G2; Sig and Vfy denote the one-time signature and verification, respectively; Enc and Dec denote the symmetric encryption and decryption respectively; k, k1 and k2 denote a security parameter, the bit-length of {0, 1}k1 and {0, 1}k2, respectively; |G|, |G1|, |G2| and |Zp| denote the bit-length of an element in G, G1, G2 and Zp, respectively; |ks| and |σs| denote the bit-length of one-time signing key and signature; |T | denotes the bit-length of the timestamp; |M| denotes the bit-length of message m ∈M; |SymEnc| denotes the bit-length of the one-time symmetric encryption ciphertext; |N|, |Nx| and |Ny| denote the safe-prime modulus; RO and ST denote the random oracle model and the standard model, respectively.

IV. EXTENSIONS

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.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

B. SPECIAL PRE SCHEMES

1) The Conditional-based Formulation: Despite PRE has been applied to many practical scenarios already, it is nontrivial 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 $rk_{i\rightarrow j}$ and a conditional key $ck_{i\rightarrow j}$. 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. 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 semitrusted. 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.

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.
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.

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.

V. 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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

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.

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 inCryptology–EUROCRYPT'98*. Springer, 1998, pp. 127– 144.

[7] G. Taban, A. A. C´ardenas, 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 mutualprofitable 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 privacypreserving 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 reencryption 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 chosenciphertext 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, "Chosenciphertext 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 publickey 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, "Keyprivate 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 Practiceand 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.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

[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 reencryption,"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, "Chosenciphertext 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 chosenciphertext 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 chosenciphertext 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 chosenciphertext 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 reencryption 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, "Chosenciphertext
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 reencryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576–2587, 2010.