6-5 Revocable Identity-Based Encryption

Keita EMURA

In this paper, we introduce revocable identity-based encryption (RIBE). In the usual identity-based encryption, any value, e.g., e-mail address or machine number, can be a public key, and it is expected to be applied to new-generation network. Remark that, a secret key can be computed for any value, and therefore it seems difficult to revoke secret keys. To circumvent this problem, Boldyreva, Goyal, and Kumar (ACM CCS 2008) proposed the first RIBE scheme. We pointed out that decryption key exposure resilient was not considered in the Boldyreva et al. scheme, and proposed the first RIBE scheme with decryption key exposure resilient. Moreover, we showed a decryption key exposure attack against the Boldyreva et al. scheme. We also introduce hierarchical RIBE, RIBE with rejoin functionality, and application to searchable encryption.

1 Introduction

Identity-based encryption (IBE) is a public key encryption that any values, e.g., mail address, name, and so on, can be public keys. Though public key certificates are required in conventional public key encryption schemes since public keys are random values, no such a certificate is required in IBE. An authority called key generation center (KGC) issues a secret key for each identity ID, and the secret key can decrypt ciphertexts generated by ID as the public key. The first IBE scheme was proposed by Boneh and Franklin[1]. They considered how to revoke secret keys, where, for a time period T, KGC issues secret keys of identitiy ID||T if a user who has ID is not revoked on time T. In this system, a time T is also indicated as a part of a public key, and users who do not have legitimate secret keys on time T can be revoked. On drawback is the cost of KGC since KGC needs to re-issue O(N-R) size secret keys for each T where N is the number of users and R is the number of revoked users. Thus, this scheme is not scalable. To circumvent this problem, Boldyreva et al.[2] proposed revocable IBE (RIBE) explained in Fig 1. Each user is issued a (long-term) secret key sk_{ID} by KGC as in IBE. A ciphertext is generated by using not only the corresponding ID but also a time period T. KGC generates key update information ku_T on time T, and broadcast it (i.e., no secure channel is required). If a user is not revoked, then the user can compute a decryption key $dk_{ID,}$T from sk_{ID} and $ku_{T.}$ By applying a framework of broadcast encryption which we call Complete Subtree (CS)[3], the size of ku_T can be O(Rlog(N/R)).

2 Decryption key exposure resistance

In the papers[4][5], we pointed out that the security model of Boldyreva et al. does not capture decryption key exposure resistance though it is captured by the security model of Boneh-Franklin. In this section, we introduce decryption key exposure resistance. As a remark, the Boneh-Franklin paper does not mention decryption key exposure resistance.

In the usual security model of IBE, an adversary chooses the challenge identity ID*, and it is required that no information of plaintext is revealed from a ciphertext computed by using ID* as its public key. Moreover, the adversary is allowed to obtain secret keys of any identity except ID*. In RIBE, the adversary chooses not only ID* but also the challenge time period T*, and it is required that no information of plaintext is revealed from a ciphertext computed by using ID* and T* as its public key. The

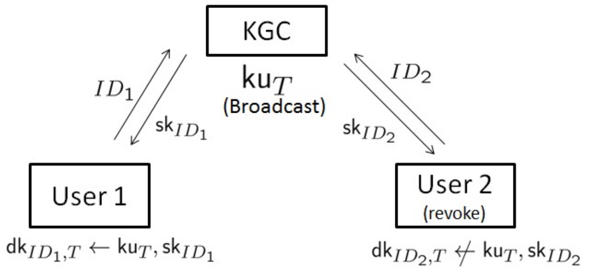
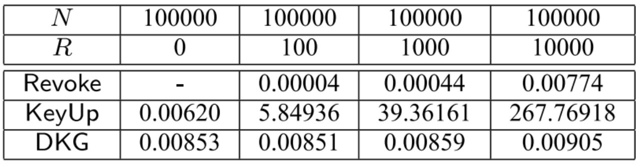

KGC
ku_T
(Broadcast)
ID_1
sk_{ID_1}
ID_2
sk_{ID_2}
User 1
User 2
(revoke)
$dk_{ID_1,T} \leftarrow ku_T, sk_{ID_1}$
$dk_{ID_2,T} \not\leftarrow ku_T, sk_{ID_2}$

Fig. 1 A framework of RIBE

adversary is required either the adversary does not obtain sk_{ID^*} or the adversary obtains sk_{ID^*} but ID* is revoked on time T*. In the security model of Boldyreva et al., the adversary is not allowed to obtain a decryption key $dk_{ID,T}$ (ID,T)≠(ID*,T*). We pointed out that the Boneh-Franklin scheme is still secure even if the adversary is allowed to obtain $dk_{ID,T}$ (ID,T)≠(ID*,T*) but the Boldyreva et al. scheme becomes insecure. Since the Boneh-Franklin scheme is not scalable, we also proposed the first scalable RIBE scheme with decryption key exposure resistance. See[4][5] for details.

Next, we introduce an implementation result by using the PBC library[6] in Fig.2. Revoke is an algorithm that adds ID of revoked users and its auxiliary information on a revocation list, KeyUp is an algorithm that generates kuT, and DKG is an algorithm that generates a decryption key $dk_{ID,T}$ from sk_{ID} and $ku_{T.}$

Though the cost of the Revoke algorithm linearly depends on the number of revoked user R, the cost is quite efficient. The cost of the KeyUp depends on the size of ku_T, i.e, O(Rlog (N/R)). But this algorithm needs to be run by KGC only once for each T, and the cost seems reasonable. The DKG algorithm is run by each user, and its cost does not depend on R, and is efficient in practice.



N	100000	100000	100000	100000
R	0	100	1000	10000
Revoke	-	0.00004	0.00044	0.00774
KeyUp	0.00620	5.84936	39.36161	267.76918
DKG	0.00853	0.00851	0.00859	0.00905

Fig. 2 Implementation Result (Unit：Second) [4]

3 Other schemes

In this section, we introduce an extension of RIBE, hierarchical RIBE and RIBE with re-join, and application of RIBE to searchable encryption. In IBE, a single KGC issues secret keys for each user. This structure can be extended by introducing hierarchy of KGC. The hierarchic is represented by a tree structure, and a parent node has a role of KGC of its children nodes. We proposed hierarchical IBE with revocation (RHIBE)[7][8][10]–[13]. In RIBE, no re-join functionality after revocation is defined, and therefore other ID needs to be used if the corresponding secret key is revoked[9]. However, we can consider a case that ID is difficult to be changed, e.g., biometrics, it seems desirable to use the same ID even after revocation. According to this motivation, we proposed RIBE with rejoin functionality. As a well-known result, searchable encryption can be constructed from IBE. By employing revocation functionality, we proposed searchable encryption with keyword revocation[14].

4 Conclusion

We introduce revocability in the IBE context. IBE is recognized as a useful tool for constructing other cryptographic primitives. As we proposed searchable encryption with keyword revocation in [14], we can expect that revocation functionality could be applied for adding functionality to other primitives. In addition to this, there is a room for improvement the security level and efficiency of RHIBE. We would like to circumvent these problems.

References

1. Dan Boneh and Matthew K. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM J. Comput. 32(3), pp.586–615, 2003.
2. Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar, "Identity-based encryption with efficient revocation," ACM Conference on Computer and Communications Security 2008, pp.417–426, 2008.
3. Dalit Naor, Moni Naor, and Jeffery Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," CRYPTO 2001, pp.41–62, 2001.
4. Jae Hong Seo and Keita Emura, "Revocable Identity-Based Cryptosystem Revisited: Security Models and Constructions," IEEE Trans. Information Forensics and Security 9(7), pp.1193–1205, 2014.
5. Jae Hong Seo and Keita Emura, "Revocable Identity-Based Encryption Revisited: Security Model and Construction," Public Key Cryptography 2013, pp.216–234, 2013.
6. The PBC (pairing-based cryptography) library, available at http://crypto.stanford.edu/pbc/.
7. Jae Hong Seo and Keita Emura, "Revocable hierarchical identity-based encryption," Theor. Comput. Sci. 542, pp.44–62, 2014.
8. Jae Hong Seo and Keita Emura, "Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption," CT-RSA 2013, pp.343–358, 2013.
9. Jae Hong Seo and Keita Emura, "Revocable Identity-Based Encryption with Rejoin Functionality," IEICE Transactions 97-A(8), pp.1806–1809, 2014.
10. Jae Hong Seo and Keita Emura, "Revocable hierarchical identity-based encryption via history-free approach," Theor. Comput. Sci. 615, pp.45–60, 2016.
11. Jae Hong Seo and Keita Emura, "Revocable Hierarchical Identity-Based Encryption: History-Free Update, Security Against Insiders, and Short Ciphertexts," CT-RSA 2015, pp.106–123, 2015.
12. Keita Emura, Jae Hong Seo, and Taek-Young Youn, "Semi-Generic Transformation of Revocable Hierarchical Identity-Based Encryption and Its DBDH Instantiation," IEICE Transactions 99-A(1), pp.83–91, 2016.
13. Jae Hong Seo and Keita Emura, "Adaptive-ID Secure Revocable Hierarchical Identity-Based Encryption," IWSEC 2015, pp.21–38, 2015.
14. Keita Emura, Le Trieu Phong, and Yohei Watanabe, "Keyword Revocable Searchable Encryption with Trapdoor Exposure Resistance and Regenerateability," TrustCom 2015, pp.167–174, 2015.

Keita EMURA, Ph.D.

Senior Researcher, Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography