INTERNATIONAL JOURNAL · ENGINEERING RESEARCH ·

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

ELSEVIER

SSRN

IJIEMR Transactions, online available on 24th Feb 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-02

Title: **EFFICIENT USER REVOCATION IN CLOUD BY USING IBE**

Volume 08, Issue 02, Pages: 118–123.

Paper Authors

K.NAGA SAILAJA, MR.C.RAVI KISHORE REDDY

Vignan's Lara Institute of Technology & Science

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

EFFICIENT USER REVOCATION IN CLOUD BY USING IBE

K.NAGA SAILAJA[1], MR.C.RAVI KISHORE REDDY[2]
Assistant Professor[1], Department of M.C.A ,Vignan's Lara Institute of Technology & Science
M.C.A Student[2],Department of M.C.A ,Vignan's Lara Institute of Technology & Science

Abstract:
Identity-based encryption (ibe) which simplifies the public key and certificate management at public key infrastructure (pki) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of ibe is the overhead computation at private key generator (pkg) during user revocation. Efficient revocation has been well studied in traditional pki setting, but the cumbersome management of certificates is precisely the burden that ibe strives to alleviate.In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Introduction

Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys. Therefore, sender using IBE does not need to look up public key and certificate, but directly encrypts message with receiver's identity. Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such ciphertext.Though IBE allows an arbitrary string as the public key which is considered as an appealing advantages over PKI, it demands an efficient revocation mechanism. Specifically, if the private keys of some users get compromised, we must provide a mean to revoke such users from system. In PKI setting, revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques [1][2][3]. Nevertheless, the cumbersome management of certificates is precisely the burden that IBE strives to alleviate.As far as we know, though revocation has been thoroughly studied in PKI, few revocation mechanisms are known in IBEsetting. In [4], Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. But this mechanism would result in an overhead load at PKG. In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows.

In 2008, Boldyreva, Goyal and Kumar [5] presented a revocable IBE scheme. Their scheme is built on the idea of fuzzy IBE primitive [6] but utilizing a binary tree data structure to record users' identities at leaf nodes. Therefore, key-update efficiency at PKG is able to be significantly reduced from linear to the height of such binary tree (i.e. logarithmic in the number of users). Nevertheless, we point out that though the binary tree introduction is able to achieve a relative high performance, it will result in other problems: 1) PKG has to generate a key pair for all the nodes onthe path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key. 2) The size of private key grows in logarithmic in the number of users in system, which makes it difficult in private key storage for users. 3) As the number of users in system grows, PKG has to maintain a binary tree with a large amount of nodes, which introduces another bottleneck for the global system.In tandem with the development of cloud computing, there has emerged the ability for users to buy on-demand computing from cloud-based services such as Amazon's EC2 and Microsoft's Windows Azure. Thus it desires a new working paradigm for introducing such cloud services into IBE revocation to fix the issue of efficiency and storage overhead described above. A naive approach would be to simply hand over the PKG's master key to the Cloud Service Providers (CSPs). The CSPs could then simply update all the private keys by using the traditional key update technique [4] and transmit the private keys back to unrevoked users. However, the naive approach is based on an unrealistic assumption that the CSPs are fully trusted and is allowed to access the master key for IBE system. On the contrary, in practice the public clouds are likely outside of the same trusted domain of users and are curious for users' individual privacy. For this reason, a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an untrusted CSP is raised.

In this paper, we introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key-update, leaving only a constant number of simple operations for PKG and eligible users to perform locally. In our scheme, as with the suggestion in [4], we realize revocation through updating the private keys of the unrevoked users. But unlike that work [4] which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decryptability, unrevoked users needs to periodically request on key-update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).Compared with the previous work [4], our scheme does not have to re-issue the whole private keys, but just need to update a lightweight component of it at a specialized entity KU-CSP. We also specify that 1) with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. 2) No secure channel or user authentication is required during key-update between user and KU-CSP.Furthermore, we consider to realize revocable IBE with a semihonest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model [7]. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Existing system:

Upon receiving a keyupdate request on ID, KU-CSP firstly checks whether ID exists in the revocation list RL, if so KU-CSP returns ⊥ and key-update is aborted.In RDoC model, the client is able to interact with multiple servers and it has a right output as long as there exists one server that follows the proposed protocol.This is because we embed a time component into each user’s private key to allow periodically update for revocation, resulting that some additional computations2 are needed in our scheme to initialize this component. Our encryption and decryption is slightly longer than the IBE scheme [4], which is also due to the existence of the time component. The user needs to perform an additional encryption/decryption for this component, rather than just encrypt/decrypt the identity component.

Proposed system:

which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys.we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting.We propose a scheme to offload all the key generation related operations during key-issuing and key-update, leaving only a constant number of simple operations for PKG and eligible users to perform locally. Compared with the traditional IBE definition, the KeyGen, Encrypt and Decrypt algorithms are redefined as follows to integrate time component.proposed a way for users to periodically renew their private keys without interacting with PKG.The authors utilized proxy re-encryption to propose a revocable ABE scheme.

Modules:

1.Client Module
i.Identity-based Encryption Authentication Module.
ii.Public Key Generator Module.
2.Private Key Generator Module.
3.Server Module
i.Graph Module

1.Client Module

i.Identity-based Encryption Authentication Module.

A trustee-based social authentication includes two phases:.

- Registration Phase:
  The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice’s friend list and are appointed as Alice’s trustees.

ii.Public Key Generator Module.

Authentication is essential for securing your account and preventing upload your data encrypted file store from database. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. Identity-based Encryption social authentication systems ask users to select their own trustees without any constraint. In our experiments we show that the service provider can constrain Identity-based Encryption selections via imposing that no users are selected as Identity-based Encryption by too many other users, which can achieve better security guarantees.

2.Private Key Generator.

They are short in storage for both private key at user and binary tree structure at PKG. We specify that in this work we also aim to utilize outsourcing computation technique to deliver overhead computation to KU-CSP so that PKG is able to be offline in keyupdate.

1) It achieves constant efficiency for both computation at PKG and private key size at user;

2) User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP;

3) No secure channel or user authentication is required during key-update between user and KU-CSP.

3.Server Module

Server module first PKG send the key. After check the keyword user key and sever key is matching server approved the file. Not

matching don't data download. This is work main concept of paper. Keyword matching meaning server send the new key from user.
i.Graph module is using how many key in generator in server collection.=

Conclusion:

In this paper, focusing on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-featured: 1) It achieves constant efficiency for both computation at PKG and private key size at user; 2) User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP; 3) No secure channel or user authentication is required during key-update between user and KU-CSP.Furthermore, we consider to realize revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure under RDoC model, in which at least one of the KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs collude, it is unable to help such user re-obtain his/her decryptability.
Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction

References

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation,"
in *Advances in Cryptology – CRYPTO'98*. Springer, 1998.

[2] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in *Financial Cryptography and Data Security*, ser.
Lecture Notes in Computer Science, S. Dietrich and R. Dhamija,
Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.

[3] F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient
certificate validation and revocation," in *Public Key Cryptography*
PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng,
and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947,
pp. 375–388.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the
weil pairing," in *Advances in Cryptology – CRYPTO 2001*, ser.
Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin
/ Heidelberg, 2001, vol. 2139, pp. 213–229.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption
with efficient revocation," in *Proceedings of the 15th ACM conference*
on Computer and communications security, ser. CCS '08. New
York, NY, USA: ACM, 2008, pp. 417–426.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in
Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in
Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg,
2005, vol. 3494, pp. 557–557.

[7] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols

for delegation of computation," Cryptology ePrint Archive, Report
2011/518, 2011.
[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in
Proceedings of the twenty-ninth annual ACM symposium on Theory
of computing, ser. STOC '97. New York, NY, USA: ACM, 1997,
pp. 506–516.
[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource
cryptographic computations," in *Proceedings of the Second international*
conference on Theory of Cryptography, ser. TCC'05. Berlin,
Heidelberg: Springer-Verlag, 2005, pp. 264–282.
[10] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation
of computation," in *Information Theoretic Security*, ser. Lecture
Notes in Computer Science, A. Smith, Ed. Springer Berlin /
Heidelberg, 2012, vol. 7412, pp. 37–61.