International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Identity-Based Encryption with Revocation of Outsourced In Cloud Computing

Amer Jaber Khazaal Almatwari

NIZAM COLLEGE (AUTONOMOUS) OSMANIA UNIVERSITY, HYDERABAD.

amerjaber7818@Gmail.com

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.

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 $\perp$ 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.

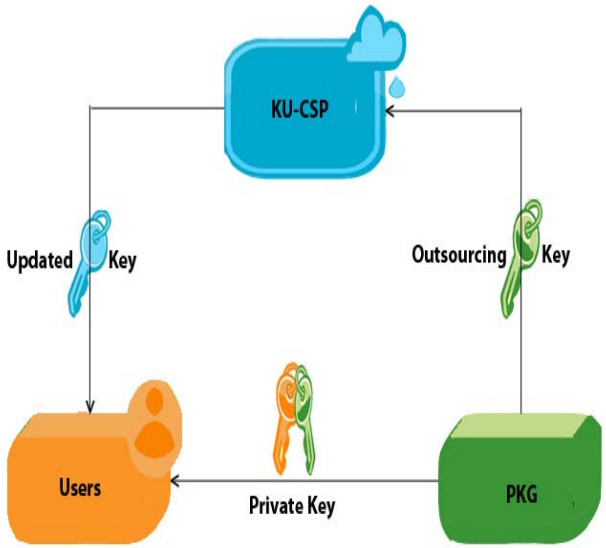
we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting.

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.



Conclusion:

Delegating key revocation successfully achieved by KU-CSP , and the key complexity also overcome and PKG will outsource keys to the KU-CSP, when ever key revocation will occur the user has to get new updated key from KU-CSP instead of PKG.

References:

[1] C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in Proceedings of the 40th annual ACM symposium on Theory of computing, ser.

STOC '08. New York, NY, USA: ACM, 2008, pp. 197–206.

[2] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe in the standard model," in Advances in Cryptology EUROCRYPT 2010, ser. Lecture Notes in Computer Science, H. Gilbert, Ed. Springer Berlin / Heidelberg, 2010, vol. 6110, pp. 553–572.

[3] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology EUROCRYPT 2010, ser. Lecture Notes in Computer Science, H. Gilbert, Ed. Springer Berlin / Heidelberg, 2010, vol. 6110, pp. 523–552.

[4] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in Advances in Cryptology - ASIACRYPT 2005, ser. Lecture Notes in Computer Science, B. Roy, Ed. Springer Berlin / Heidelberg, 2005, vol. 3788, pp. 495–514.

[5] D. Boneh, X. Ding, G. Tsudik, and C. Wong, "A method for fast revocationofpublickeycertificatesandsecurity capabilities,"in 10th USENIX Security Symposium, 2001, pp. 297–308.

[6] B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," pp. 163–171, 2003. [26] H. Lin, Z. Cao, Y. Fang, M. Zhou, and H. Zhu, "How to design space efficient revocable ibe from non-monotonic abe," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 381–385.

[7] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identitybased encryption," in Topics in Cryptology CT-RSA 2009, ser. Lecture Notes in Computer Science, M. Fischlin, Ed. Springer Berlin / Heidelberg, 2009, vol. 5473, pp. 1–15.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM SymposiumonInformation,ComputerandCommunicationsSecurity, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 261–270.

[9] D. Chaum and T. P. Pedersen, "Wallet databases with observers," in Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '92. London, UK, UK: Springer-Verlag, 1993, pp. 89–105.

[10] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," in Trends in Software Engineering, ser. Advances in Computers, M. V. Zelkowitz, Ed. Elsevier, 2002, vol. 54, pp. 215 – 272.

[11] 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.

[12] 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.

AMER JABER KHAZAAL ALMATWARI

MSCIS From NIZAM COLLEGE (AUTONOMOUS)
OSMANIA UNIVERSITY, HYDERABAD.

9676945382 , amerjaber7818@Gmail.com