Sixth International Conference on Emerging trends in Engineering and Technology (ICETET'16)
www.ijera.com
ISSN: 2248-9622, pp.71-80

RESEARCH ARTICLE OPEN ACCESS

Secured and Efficiency in Generating Issueing and Updation of Private Key Using Iaas Model

Ms Rameez Fathima.A[1], Mrs Arogya Swarna.S[2]
[1]*II ME CSE S.Veerasamy Chettiar College of Engg and Tech*
[2]*Asso Prof/CSE S.Veerasamy Chettiar College of Engg and Tech hod*

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 certificate 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 rest 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. Time period. But this mechanism would result in an overhead load at PKG. 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 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 untreated CSP is raised. It realizes revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDOC) model finally, we provide extensive experimental results to the efficiency of our proposed construction.This paper is organized as follows. We describe the preliminaries of our scheme. In, we present the system model and security dentition of our scheme. The proposed construction, and its security analyzes is, we propose a security enhanced construction under RDOC model. An extensive experimental result is presented to demonstrate the efficiency.

I. ID-BASED ENCRYPTION

An IBE scheme which typically involves two entities, PKG and users (including sender and receiver is consisted of the following four algorithms.
SETUP: The setup algorithm takes as input a security parameter and outputs the public key and the master key. Note that the master key is kept secret at PKG.
KEYGEN: The private key generation algorithm is run by PKG, which takes as input the master key and user's identity. It returns a private key corresponding to the identity.
ENCRYPT: The encryption algorithm is run by sender, which takes as input the receiver's identity and a message to be encrypted. It outputs the cipher text.
DECRYPT: The decryption algorithm is run by receiver, which takes as input the cipher text and his/her private key. It returns a message or an error. An IBE scheme must satisfy the definition of consistency. Specifically, when the private key generated by algorithm KeyGen when it is given as the input, then Decrypt where Encrypt. The motivation of IBE is to simplify certificate management. For example, when Alice sends an email to Bob at bob company com, she simply encrypts her message using Bob's email address, but does not need to obtain Bob's public key certificate. When Bob receives the encrypted email he authenticates himself at PKG to obtain his private key, and read his email with such a private key.

II. PROBLEM STATEMENT

It present system model for outsourced revocable IBE in Compared with that for typical IBE scheme, a KU-CS is involved to realize revocation for compromised users.
Actually, the KU-CSP can be envisioned as a public cloud run by a third party to deliver basic computing capabilities to PKG as standardized services over the network. Typically,
KU-CSP is hosted away from either users or PKG, but provides a way to reduce PKG computation and storage cost by providing a flexible, even temporary extension to infrastructure. When revocation is triggered, instead of re-requesting private keys from PKG in unrevoked users have to ask the KU-CSP for updating a lightweight component of their private keys. Though many details are involved in KU-CSP's deployment, in this paper we just logically envision it as a computing service provider, and concern how to design secure scheme with an untruth KU-CSP. Based on the system model proposed, we are able to define the outsourced revocable IBE scheme. Compared with the traditional IBE definition, the KeyGen Encrypt and Decrypt algorithms are redefined as follows to integrate time component.
Note that two lists and are utilized in our definition, where records the identities of revoked users and is a linked list for past and current time period.
KeyGen: The key generation algorithm run by PKG takes as input–a master key, an identity, a revocation list and a time list. If, the algorithm is aborted. Otherwise, it sends the private key to user where is the identity component for private key and is its time component for current time period. Additionally, the algorithm sends an outsourcing key to
KU-CSP. Encrypt the encryption algorithm run by sender takes as input–a message, an identity and a time period. It outputs the cipher text.
Decrypt: The decryption algorithm run by receiver takes as input–a cipher text encrypted under identity and time period and a private key. It outputs the original message
If any, otherwise outputs. In addition, two algorithms are defined to realize revocation
At KU-CSP through updating the private keys of unrevoked users. Revoke the revocation algorithm run by PKG takes as input–a revocation list a time list and the set of identities to be revoked. It outputs an updated time period as well as the updated revocation list and time list.
Key Update: The key update algorithm run by KU-CSP takes as input–a revocation list, an identity, a time period and the outsourcing key for identity. It outputs user's updated time component in private key if his identity does not belong to , otherwise, outputs .In discuss user revocation, that is how to deprive users of decrypt ability even if they have been issued their private keys. To this end, we embed a time period into private key.

III. SECURITY DEFINITION

It assumes that KU-CSP in the proposed system model is semi-trusted. Specifically, it will follow our protocol but try to find out as much secret information as possible based on its
Possession. Therefore, two types of adversaries are to be considered as follows.
Type-I adversary. It is defined as a curious user with identity but revoked before time period. Such adversary tries to obtain useful information from cipher text intended for him/her at or after (e.g. time period) through colluding with other users even if they are unrevoked. Therefore, it is allowed to ask for private key including identity component and updated time component for cooperative users. We specify that under the assumption that KU-CSP is semi-trusted, type-I adversary cannot get outsourcing key for any users.
Type-II adversary. It is defined as a curious KU-CSP which aims to obtain useful information from cipher text intended for some target identity at time period. Such Adversary not only possesses of outsourcing keys for all users in the system, but also is able to get user's private key through colluding with any other user with identity. It is noted that to make such attack reasonable we must restrict.

IV. ID-BASED ENCRYPTION WITH SIMPLIFIED REVOCATION IN Iaas MODEL

Having the intuitions above, we are able to define CCA security game for type-I and type-II adversary respectively for our setting. Suppose A is the type- adversary for then, its advantage in attacking the IBE with outsourced revocation scheme E is defined as E A. An identity-based encryption with outsourced revocation scheme is semantically secure against adaptive chosen-cipher text attack (IND-ID-CCA) if no polynomial Bounded adversary has a non-negligible advantage against challenger in security game for both type-I and type-II adversary.
Finally, beyond the CCA security, we also specify that

1) An IBE with outsourced revocation scheme is INDID- CPA secure (or semantically secure against chosen plaintext attack) if no polynomial time adversary has non-negligible advantage in modified games for both type-I and type-II adversary, in which the decryption oracle in both phase 1 and phase 2 is removed.

2) An IBE with outsourced revocation scheme is secure in selective model if no polynomial time adversary has non-negligible advantage in modified games for both type-I and type-II adversary, in which the challenge identity and time period is submitted before setup.

V. EFFICIENT IBE WITH SIMPLIFIED REVOCATION

In order to achieve efficient revocation, we introduce the idea of "partial private key update" into the proposed construction, which operates on two sides: 1) we utilize a "hybrid private key" for each user in our system, which employs an AND gate connecting two sub-components namely the identity component and the time component respectively. is generated by PKG in key-issuing but is updated by the newly introduced KU-CSP in key update In encryption, we take as input user's identity as well as the time period to restrict decryption, more precisely, a user is allowed to perform successful decryption if and only if the identity and time period embedded in his/her private key are identical to that associated with the cipher text. Using such skill, we are able to revoke user's decrypt ability through updating the time component for private key by KU-CSP.

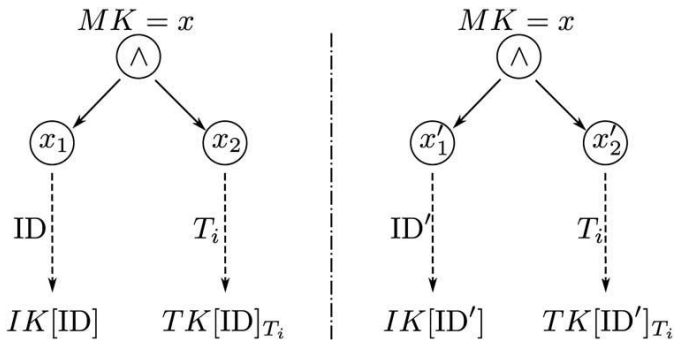
Moreover, we remark that it cannot trivially utilize an identical updated time component for all users because revoked user is able to re-construct his/her ability through colluding with unrevoked users. To eliminate such collusion, we randomly generate an outsourcing key for each identity, which essentially decides a "matching relationship" for the two sub-components. Furthermore, we let KU-CSP maintain a list to record user's identity and its corresponding outsourcing key. In key-update, we can use to update the time component for identity. Suppose a user with identity is revoked at. Even if he/she is able to obtain for identity, the revoked user still cannot decrypt cipher text.

VI. PROPOSED EDIFICE

It present our construction based on as follows.

Setup: The setup algorithm is run by PKG. It selects a random generator G as well as a random integer Z, and sets. Then, PKG picks a random element G and two hash functions G. Finally, output the public key and the master KeyGen For each user's private key request on identity, PKGfirstly checks whether the request identity exists in, if so the key generation algorithm is aborted. Next, PKGrandomly selects Z and sets. It randomly chooses Z, and computes. Then, PKGreads the current time period from (we require that PKG should create current time period firstly if is empty). Accordingly, it randomly selects Z and computes, where and finally output and. Encrypt Suppose a user wishes to encrypt a message under identity and time period. He/She selects a random value Z and computes and Finally, publish the cipher text as Decrypt Suppose that the cipher text is encrypted under and the user has a private key , where and He/She computes Revoke If users with identities in the set are to be revoked at time period, PKG updates the revocation list as as well as the time list through linking the newly created time period onto original list . Finally send a copy for the updated revocation list as well as the new time period to KU-CSP.

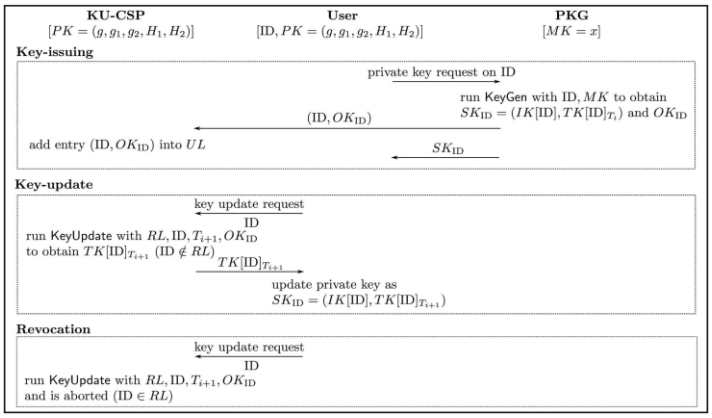
Key Update: Upon receiving a key update request on, KU-CSP firstly checks whether
Exists in the revocation list, if so KU-CSP returns and key-update is aborted. Otherwise, KU-CSP fetches the corresponding entry in the user list Then, it randomly selects Z, and computes and finally,



Finally, we emphasize that the idea behind our construction is to realize revocation through updating the time component in private key. Therefore, the key point is to prevent Revoked user from colluding with other users to re-construct his/her private key. As dealing intuition, such collusion attack is resistant in our proposed construction due to the Random split on for each user. Specifically, as shown in which is an AND gate connecting two sub-components, if two different users call for their private keys, PKG will obtain two random-

ly splits and with the complementary that are used to produce the identity component for and respectively, while the time component is separately generated from and . By the reason that the complementary exists between and as well as and, the identity component and time component should accordingly have a "verification" in private key. With such "verification", even if a curious user obtains time component of other users, he/she cannot forge a valid private key for himself to perform decryption successfully. Key Service Procedures Based on our algorithm construction, as shown in the key service procedures including key-issuing, key-update and revocation in proposed IBE scheme with outsourced revocation work as follows. Key issuing we require that PKG maintains a revocation list and a time list locally. Upon receiving a private key request on, PKG runs Key Gent obtain private key and outsourcing key. Finally, it sends to user and to KUCSP respectively. As described in intuition, for each entry sent from PKG, KU-CSP should add it into a locally maintained user list.

Key-update if some users have been revoked at time period, each unrevoked user needs to send key-update request to KU-CSP to maintain decrypt ability. Upon receiving the request on identity, KU-CSP runs Key Update to obtain. Finally, it sends such time component back to user who is able to update his/her private key a. Revocation. Similar to key update, if a revoked user sends a key-update request on identity, KU-CSP runs



VII. SECURITY SCRUTINY

Theorem:

Suppose that the DBDH assumption holds in G and hash functions and are random oracles. Suppose the adversary makes at most and queries to hash functions, private key, updated key and outsourcing key extraction oracles respectively. We use to denote time cost for single multi-based exponentiation operation in G. Then the proposed IBE with outsourced revocation scheme is secure in the sense of IND-ID-CPA.

Proof:

Assume that an adversary A and A have advantage and in attacking the proposed IBE scheme in the sense of IND-ID-CPA security for type-I and type-II adversary respectively. We will build two simulators S and S that respectively uses A as a sub-algorithm to solve the decisional BDH problem with a non-negligible probability.

Suppose challenger in DBDH problem flips a fair binary coin outside of S and S's view. If, then S and S are given otherwise, for random Z. S and S are asked to output a value as the guess for. Then we provide simulations as follows. Simulation of S against Type-I Adversary Setup: S sets and sends the public key to A. Phase 1: S initializes an empty table list, andanempty set. A is allowed to issue queries in the following types. Query. S randomly picks and maintains a list L to store the answers to the hash oracle. Upon receiving for S performs a check on L . If an entry for the query is found, the same answer will be returned. Otherwise, S randomly selects Z and computes After storing the entry in L, S returns query. S randomly picks and maintains a list L to store the answers to the hash oracle. Upon receiving for, S performs check on L. If an entry for the query is found, the same answer will be returned. Otherwise, S randomly selects Z and computes after storing then try in L, S returns. Private Key query. Upon receiving, S responses in one of the following two ways.

If, S randomly selects Z and attempts to simulate by setting where Z Therefore where and. Moreover, S sets and sends it back to S. If, S randomly selects Z and computes

Where and for Z. Moreover, S sets after adding the entry into, S returns. Updated key query. Upon receiving, S checks whether there exists an entry in if not, S aborts; otherwise, S fetches such entry and responds in the following two cases. If, S selects Z and after setting returns where and If S checks whether if so, S aborts. Otherwise, set for random Z and after setting returns where and Challenge A will submit two challenge messag-

es and as well as and with S checks that whether or if so the security game is aborted. Otherwise, S flips a fair binary coin and returns an encryption of the cipher text is simulated as note that if let then repeated. Guess: A will submit a guess of If S outputs otherwise outputs. We note that since A has the possibility of in submitting for challenge, the security game is finished successfully with the probability of as well. Thus, we have since S guesses when we have if then a sees an encryption of in the successful game. Therefore, we have finally, we have the overall advantage of S in solving DBDH problem as Simulation of S against Type-II Adversary Setup: S performs identically to that in S Phase 1: S empty table list and two empty sets and. A is allowed to issue queries in the following types.

Query. S responses identically to that in S.

Outsourcing key query. Upon receiving, S randomly selects Z and returns after adding into Private Key query. Upon receiving, if there exists such entry in S checks whether, if so S aborts. Otherwise, S sets for Z and computes where and after setting, S returns updated key query. Upon receiving and, if there exists such entry in S computes where and for Z. S continues to check whether, if not it sets finally, return. Challenge will submit two challenge messages and as well as and with and S checks that whether or if so the security game is aborted. Otherwise, S flips a fair binary coin and returns an encryption of the cipher text is simulated as Phase 1 is repeated. Guess: A will submit a guess of If S outputs, otherwise outputs Similar to the analysis presented in the simulation of S against adversary we have the overall advantage of S in solving DBDH problem.

Edifice Under Refereed Allocation Of Computation Representation

In this section, we will attempt to propose a security enhanced construction under the under the recently formalized RDOC model.

VIII. ADVANCED EDIFICE

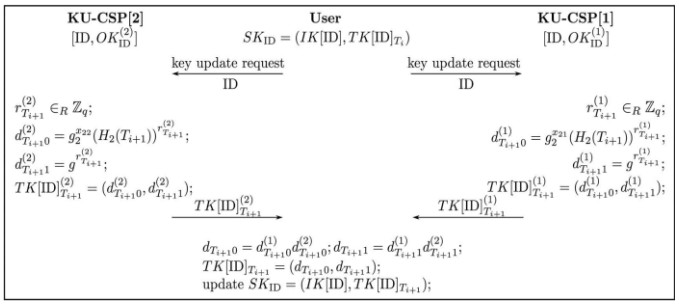
RDOC model originates from the model of refereed games in and is later formalized in and In RDOC model, the client is able to interact with multiple servers and it has a right output as long as there exists one server that follows the proposed protocol. One of the most advantages of RDOC over traditional model with single server is that the security risk on the single server is reduced to multiple servers involved in. As the result of both the practicality and utility, RDOC model recently has been widely utilized in the literature of outsourced computation In order to apply RDOC to our setting, we introduce other independent KU-CSPs. For simplicity, in the rest of paper, we only focused on the case that as shown in Furthermore, we have three requirements in such At least one of the KU-CSPs is honest. Computational complexity at the honest KU-CSP is not much more than the other required performing revocation.PKG's running time would be much smaller than required to directly perform revocation. In figure out that the challenge to realize such advanced construction is to demand that and cannot be leaked at the same time. To achieve this goal, we randomly split into and which will be separately used by the two KU-CSPs to produce partial time component and after receiving the two partial time components, user performs a production.

System model with two KU-CSPs.

To make a combination and obtains the final updated key (i.e. time component for private key Since the setup, encryption and decryption phases operate exactly as before, we will introduce the Key Combine algorithm and only provide the key generation and revocation for the advanced construction as follows.

Keygen: The algorithm is presented similar to that in our proposed construction. The only difference is that PKG does not directly send to KU-CSP, but makes a further random split on to obtain and with Finally, PKG sends to -the KU-CSP.

Key Update: Upon receiving the key update request on the KU-CSP checks whether Exists in the revocation list if so the key update is aborted. Otherwise, it fetches the corresponding entry in the user list and computes. Finally send the updated partial time component back to user. Key Combine: Upon receiving and , user performs a key combination by computing and as the paradigm shown in to obtain . Finally update as



IX. SECURITY SCRUTINY

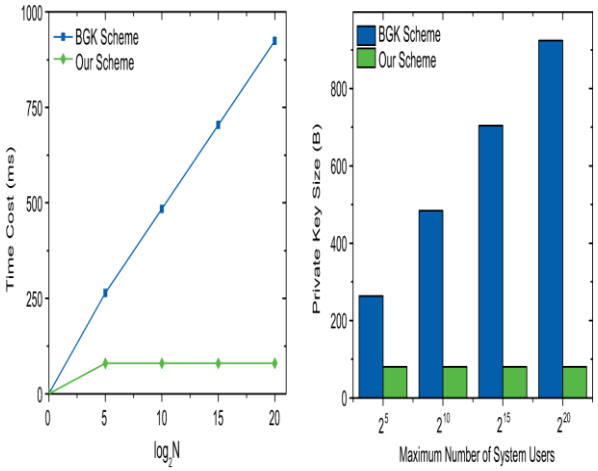
As a stronger adversary model, RDOC captures much more meaning beyond the "honest-but-curious" sense, that is curious user is allowed to cooperate with at most servers if

Servers are involved. To accommodate to this case, we modify the private key oracle slightly to adapt to a pair of outsourcing keys and introduce another outsourcing key extraction oracle for Type-I adversary as follows. It is noted that the challenger is required to maintain an empty set to restrict adversary accessing the whole outsourcing key for some identity. This coincides with the assumption that at least one of the KU-CSPs is honest. Private key extraction oracle. Upon receiving private key request on challenger runs to obtain the private key and a pair of outsourcing keys After adding the entry into return Outsourcing key extraction oracle. Upon receiving the partial outsourcing key request on to the the KU-CSP, challenger firstly checks whether If so the oracle is aborted. Otherwise, if there exists an entry in after setting return .The advanced construction is secure in the sense of IND-ID-CPA in random oracle under the assumption that DBDH problem is intractable.

Proof Since the proof technique is quite similar to that used in the proof of theorem 1, we would only provide a sketch here Suppose the advantage and in attacking the proposed advanced construction in the sense of IND-ID-CPA for type-I and type-II adversary respectively. Then, we are to provide two simulators S and S to simulate two games (i.e. CPA security game for type-I and type-II adversary) between challenger and adversary. We specify that comparing with single KU-CSP adversary model it allows collusion between curious user and either of the KU-CSPs here. Correspondingly, comparing with the simulators in the proof of S is identical and S needs to simulate another outsourcing key extraction oracle. In the additional outsourcing key extraction oracle, upon receiving the input S firstly examines that whatever is queried. If so, the oracle is aborted since A is not allowed to collude with both of the KU-CSPs. Otherwise A fetches the entry in and returns back to adversary.

TABLE 1
Efficiency Comparison for Stages in Revocable IBE

	Our Scheme	IBE without Revocation [4]
Setup	83.764 ms	80.233 ms
Key-Issuing	40.369 ms	20.121 ms
Encryption	39.840 ms	24.595 ms
Decryption	21.278 ms	10.285 ms
Key-Update	10.300 ms[1]	—-



(a) Responding Time for Single Key Generation Request

(b) Private Key Size

X. PERFORMANCE EVALUATION

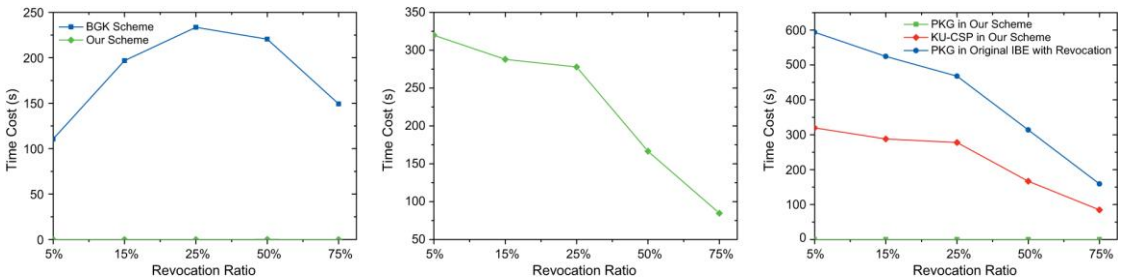
In this section, we will provide a thorough experimental evaluation of the construction proposed in We build our tested by using 64-bit M2 high-memory quadruple extra large Linux servers in Amazon EC2 platform as KU-CSP, and a Linux machine with Intel(R) Core(TM)2 Duo CPU clocked at 2.40 GHz and 2 GB of system memory as the

User and PKG. Note that in all the evaluations, the groups G and G are selected in 160-bit and 512-bit length respectively.

XI. INFERENCE

Firstly, we aim to evaluate the efficiency of our outsourced revocable scheme by comparing the total time taken during each stage with the original IBE which does not consider revocation. We examine the time cost of executing individual stage by the both schemes. It is not surprising to see that our scheme takes more time because we consider the revocability issue. Note that our scheme shares the same setup algorithm with the IBE scheme. Our key-issuing stage is relative longer than that in the IBE scheme. This is because

We embed a time component into each user's private key to allow periodically update for revocation, resulting that some additional computation are needed in our scheme to initialize this component. Our encryption and decryption is slightly longer than the IBE scheme. This is also due to the existence of the time component the user needs to additional encryption/decryption for this component, rather than just encrypt/decrypt the identity component. To sum up, our revocable scheme achieves both identity based encryption/decryption and revocability without introducing significant overhead compared to the original IBE scheme our execution time is still within millisecond



(a) Key Update at PKG

(b) Key Update at KU-CSP

(c) Key Update Comparison with [4]

Alternative IBE

Introduced by and firstly implemented by Boney and Franklin as well as, IBE has been researched intensively in cryptographic community. On the aspect of construction, these first schemes were proven secure in random oracle. Some subsequent systems achieved provable secure in standard model under selective-ID security or adaptive-ID security .Recently, there have been multiple lattice-based constructions for IBE systems on

revocable IBE, there is little work presented. As mentioned before, Boney and Franklin's suggestion is more a viable solution but impractical. Hanaoka et al. Proposed a way for users to periodically renew their private keys without interacting with PKG. However the assumption required in their work is that each user needs to possess a tamper-resistant hardware device. Another solution is mediator-aided revocation In this setting there is a special semi-trusted third party called a mediator who helps users to decrypt each cipher text. If an identity is revoked then the mediator is instructed to stop helping the user. Obviously, it is impractical since all users are unable to decrypt on their own and they need to communicate with mediator for each decryption. Recently, Lin et al. Proposed a space efficient revocable IBE mechanism from non-monotonic Attribute-Based Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where the number of revoked users is.

As far as we know, the revocable IBE scheme presented by Boldyreva et al. remains the most effective solution right now. Liberty and Vergnaud improved Boldyreva's construction to achieve adaptive-ID security. Their work focused on security enhanced, but inherits the similar disadvantage as Boldyreva's original construction. As we mentioned before they are short in storage for both private key at user and binary tree structure at PKG.

XII. OTHER TECHNIQUE

Another work related to us originates from Yu et al. The authors utilized proxy re-encryption to propose a revocable ABE scheme. The trusted authority only needs to update master key according to attribute revocation status in each time period and issue proxy re-encryption key to proxy. Comparisons in key update (Case: system users). Key-Update in BGK Scheme in Varying System Users servers. The proxy servers will then re-encrypt cipher text using the re-encryption key to make sure all the unrevoked users can perform successful decryption. We specify that a third party service provider is introduced in both Yu et al and this work. Differently, Yu et al.utilized the third party (work as a proxy) to realize revocation through re-encrypting cipher text which is only adapt to the special application that the cipher text is stored at the third party. However, in our construction the revocation is realized through updating private keys for unrevoked users at cloud service provider which has no limits on the location of cipher text.

XIII. CLOUD COMPUTING

Cloud Computing is the latest term encapsulating the delivery of computing resources as a service. It is the current iteration of utility computing and returns to the model of "renting" resources. Leveraging cloud computing is today, the defector means of deploying internet scale systems and much of the internet is tethered to a large number of cloud Service providers. In this paper, the KU-CSP provides computing service in the Infrastructure as a service (IaaS) model, which provides the raw materials of cloud computing, such as processing, storage and other forms of lower level network and hardware resources in a virtual, on demand manner via the Internet. Differing from traditional hosting services with which physical servers or parts thereof are rented on a monthly or yearly basis, the cloud infrastructure is rented as virtual machines on a per-use basis and can scale in and out dynamically, based on customer needs. Such on-demand scalability is enabled by the Some other works about outsourced ABE include. Especially outsourced the encryption in ABE with the map-reduce technique in cloud computing. Zhang et al. proposed a novel outsourced image recovery service architecture, which exploits different domain technologies and takes security, efficiency, and design complexity into consideration from the very beginning of the service flow.

XIV. 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) Non secure channel or user authentication is required during key-update between user and KU-CSP.

Furthermore, we consider realizing 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 decrypt ability. 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). New York, NY, USA: Springer, 1998, pp. 137–152.
[2]. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, S. Dietrich and R. Dhamija, Eds. Berlin, Germany: Springer, 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'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, vol. 2947, pp. 375–388.
[4]. D. Boney and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.
[5]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Computer Security (CCS'08), 2008, pp. 417–426.
[6]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 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, Rep. 2011/ 518, 2011 [online]. Available: http://eprint.iacr.org/2011/518.
[8]. U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Anna. ACM Sump theory Computer (STOC'97), 1997, pp. 506–516.
[9]. S. Rosenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography (TCC'05), 2005, pp. 264–282.
[10]. R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, A. Smith, Ed. Berlin, Germany: Springer, 2012, vol. 7412, pp. 37–61.
[11]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in Proc. 17th Eur. Sump. Res. Computer. Security (ESORICS), 2012, pp. 541–556.
[12]. M. J. Attalla and K. B. Firkin, "Securely outsourcing linear algebra computations," in Proc. 5th ACM Sump. Inf. Computer Security (ASIACCS'10), 2010, pp. 48–59.
[13]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology (CRYPTO), G. Blakely and D. Chum, Eds. Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.
[14]. C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, B. Horary, Ed. Berlin/ Heidelberg: Springer, 2001, vol. 2260, pp. 360–363.
[15]. R. Canetti, S. Halevy, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology (EUROCRYPT'03), E. Balham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646.
[16]. D. Boney and X. Boyne, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'04), C. Cachin and J. Camelish, Eds. Berlin, Germany: Springer, 2004, vol. 3027, pp. 223–238.
[17]. D. Boney and X. Boyne, "Secure identity based encryption without random oracles," in Advances in Cryptology (CRYPTO'04), M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206.
[18]. B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.
[19]. C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464. [20] C. Gentry, C. Pokier, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proc. 40th Anna. ACM Sump.Theory Computer (STOC'08), 2008, pp. 197–206.
[20]. S. Agrawal, D. Boney, and X. Boyden, "Efficient lattice in the standard model," in Advances in Cryptology (EUROCRYPT'10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.
[21]. D. Cash, D. Hofheinz, E. Kilts, and C. Pokier, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology (EUROCRYPT 10), H. Gilbert, Ed Berlin, Germany: Springer, 2010, vol. 6110, pp. 523–552.
[22]. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in Advances in Cryptology (ASIACRYPT'05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.
[23]. D. Boney, X. Ding, G. Studio, and C. Wong, "A method for fast revocation of public key certificates and security capabilities," in Proc. 10th USENIX Security Sump., 2001, pp. 297–308.
[24]. B. Liberty and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in Proc. 22nd Anna. Sump. Principles Distribute. Compute., 2003, pp. 163–171.

[25]. H. Lin, Z. Cao, Y. Fang, M. Zhou, and H. Zhu, "Houghton design space efficient revocable IBE from non-monotonic ABE," in Proc. 6th ACM Sump. Inf. Computer. Communed. Security (ASIACCS'11), 2011, pp. 381–385.
[26]. B. Liberty and D. Vergnaud, "Adaptive-id secure revocable identity based encryption," in Topics in Cryptology (CT-RSA'09), M.Fechlin, Ed. Berlin, Germany: Springer, 2009, vol. 5473, pp. 1–15.
[27]. S. Yu, C. Wang, K. Ran, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ACM Sump. Inf. Computer. Communed. Security (ASIACCS'10), 2010, pp. 261–270.
[28]. D. Chum and T. P. Pedersen, "Wallet databases with observers," in
[29]. Proc 12th Anna. Int. Cryptology Conf. Adv. Cryptology (CRYPTO'92), 1993, pp. 89–105.
[30]. M. J. Attalla, K. Pintzopoulos, J. R. Rice, and E. E. Safford, "Secure outsourcing of scientific computations," in Trends in Software Engineering, M. V. Zelkowitz, Ed. New York, NY, USA: Elsevier, 2002, vol. 54, pp. 215–272.