IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 8 (August. 2018), ||V (III) || 12-21

Identity Based Encryption in Cloud Computing With Outsourced Revocation Using Ku-CSP

Dr.Chinthagunta Mukundha[1], Bhanu Chandar[2],
[1]*Associate Professor,Dept of IT, Sreenidhi Institute of Science & Technology,Hyderabad*
[2]PG Student, *Dept of IT, Sreenidhi Institute of Science & Technology, Hyderabad*
Corresponding Author: Dr.Chinthagunta Mukundha

ABSTRACT: Identity-based encryption (IBE), which easier to do or understand the public key and certificate management at public key infrastructure (PKI) is an important one of two or more available possibilities, to public key encryption.one of the main efficiency drawbacks of IBE suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. But this technique would result in an overhead load at PKG.All the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys.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 validity for all transactions, which will become a bottleneck for IBE system as the number of users develop, We propose a scheme to offload all the key generation related operations during key-issuing and key-update, leaving only a uniform number of simple operations for PKG and qualified users to perform locally,Our outline doesn't have to re-generate the whole private keys, but we should update an ability component of it at a characterized entity KU-CSP With the provision of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is permitted to be not connected after sending the revocation list to KU-CSP, No secure channel or user action is required during key-update between user and KU-CSP. Furthermore, we propose another construction which is secure under the recently formalized refereed delegation computation model. Finally, we provide extent experimental results in an efficient way.

KEYWORDS: Identity-based encryption(IBE), Outsourced, Revocation, KU-CSP, Cloud-computing

---

Date of Submission: 04-08-2018 Date of acceptance: 18-08-2018

I. INTRODUCTION

This study to focus on identity-based encryption understand the public key and certificate management at public key infrastructure(PKI) is an important one or more available possibilities. We bring outsourcing activity into IBE demonstration of review and endorsement the protected meaning of outsourced revocable IBE out of the blue to the best of our insight.We propose a plan to offload all the key age-related tasks amid key-issuing and key-refresh, leaving just a consistent number of basic activities for PKG and qualified clients to perform locally. In our plan, we understand renouncement through refreshing the private keys of the unrevoked clients. Subsequently, keeping in mind the end goal to keep up decode capacity, unrevoked clients' needs to intermittently ask for on key-refresh for time part to a recently presented substance named Key Update Cloud Service Provider (KU-CSP). we don't need to re-issue the entire private keys, however simply need to refresh a lightweight part of it at a specific element KU-CSP. With the guide of KU-CSP, the client needs not to contact with PKG in key-refresh, at the end of the day, PKG is permitted to be disconnected in the wake of sending the disavowal rundown to KU-CSP. No safe channel or client validation is required amid key-refresh amongst client and KU-CSP.

When a large number of users call for their private keys, it mayover-burden the quality specialist. Additionally, key management mechanism, key revocation in particular, is necessary in a secure and scalable ABE system.

In the majority of existing ABE scheme, the repudiation of any single private key requires key-refresh at a quality specialist for the rest of the unrevoked keys which share normal attributes with the one to be denied. characteristic expert.

In addition,all of these heavy tasks centralized at authority side would make it an efficiency bottleneck in the access control system. going at eliminating the most overhead estimation at both the characteristic specialist and the client sides, an outsourced ABE conspire is prescribed that sponsorships outsourced decryption and also enables appointing key generation.In addition, it is observed that when experiencing commercial cloud computing services, the CSPs may be selfish in order to save its computation or bandwidth, which may cause results returned incorrectly Keeping in mind the end goal to manage this issue, checkability is done on comes about came back from both KGSP and DSP.

When using public-key cryptography over the Internet, the main issue is the ability to associate the right public-keys to the right individuals/organizations. The overall strategy for doing so is as follows. In its simplest form, we assume one or more trusted Certificate-Authority (CA) centers which initially run the signature key generation algorithm to compute its own public and secret keys. Each CA holds its secret key under great security but widely distributes.

Furthermore, we consider to realizing 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.In this manner, key-update proficiency at PKG can be fundamentally decreased from straight to the stature of such paired tree (i.e. logarithmic in the quantity of clients). By the by, we bring up that however the parallel tree acquaintance is capable with accomplish a relative superior, it will bring about different issuesNevertheless, 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 on the 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 quantity of clients in framework develops, PKG needs to keep up a double tree with a lot of hubs, which presents another bottleneck for the worldwide framework. Pair with the improvement of distributed computing.

II. RELATED WORK

i) Fast Digital Identity Revocation

Computerized characters are fundamental for business, private and government utilization of the web. Eg: they requirement for on-line shopping, business-to-business exchanges, on-line managing an account code validation, organization inside personalities, The U.S. Government, NIST, the U.S. Mail station, Visa and Master Card, some real banks, and privately-owned businesses like VeriSign, SIAC, IBM, GTE, and Microsoft are for the most part assembling computerized personality foundations. While the general plan of every one of these plans is comparative, and depends on open key cryptography and Certificate Authority administrations, In 1995, S. Micali proposed a rich strategy for character denial which requires next to no correspondence amongst clients and verifiers in the framework. they found that, plot by lessening the general CA to catalog correspondence, while as yet keeping up the same minor clients to seller correspondence. To lessens the CA to catalogs correspondence costs significantly. It can be prove that the normal day by day cost is propositional to at most (R/365) log (365 N/R) this lessening the picked up at the costs of an expansive correspondence prerequisite for the verifier. This exclusive expanding the normal day by day correspondence cost of the CA by a factor [7].

ii) Certificate Revocation Using Fine Grained Certificate Space Partitioning

A certificate is a digitally signed statement binding the key holder’s name to a public key and various other feature. At the point when an endorsement is issued, the CA announces the timeframe for which the authentication is legitimate.However, there may be situations when the certificate must unusual to be declared invalid prior to its expiration date. Each partition contains the status of a set of certificates, our scheme is more efficient than the three well known certificate revocation techniques: CRL, CRS and CRT. Our scheme aims to something the right balance between CA to directory communication costs and query costs by carefully selecting the number of partitions. certification Revocation List (CRL) is the first and the least difficult strategy for declaration denial. it is generally perceived [Mic97, Goy04, Riv98] that CRLs are too exorbitant and can't give a decent level of auspiciousness, Certificate Revocation System (CRS) [Mic96, Mic97, Mic02] was presented by Micali and could answer the client inquiries with extraordinary productivity [1].The main problem with CRS is that it is not suitable in case of a distributed query answering system, The CA to directory communication is too high shoot the overall cost of the system [NN98, ALO98]. Aiello et al [ALO98] proposed an improvement to CRS aimed at decrease this communication but their approach had problems, Certificate Revocation Tree (CRT) [Koc98] is the third well known technique for certificate revocation. Though the CA to directory communication is very low, the query cost is too high again shoot up the overall cost of the system, The above approach may be worth analyze in environments where the number of directories or updates per day is high. This is because it may reduce the CA to directory communication costs which are quite high in such environments, though at the price of increasing the query costs [1].

iii) Private And Cheating-Free Outsourcing Of Algebraic Computations

We Give Protocols For Thesecure And Private Outsourcing Of Straight Variable Based Math Calculations, That Expert A Customer To Safely Outsource Broad Arithmetical Calculations To Two Remote Servers, Such That The Servers Learn Nothing About The Customer's Private Input Or The Result Of The Computation And Any Attempted Corruption Of The Answer By The Servers Is Identify The Presence With

High Probability. Large-Scale Problems In The Physical And Life Sciences Are Being Radically By Internet Computing Technologies, Such Of Techniques For Computational Outsourcing In A Privacy-Preserving And Cheating-Resilient Manner, In Future Work We Will Extend These Results To Different Algebraic Structures, Such As The Closed Semi As Grid Computing, A Weak Computational Device, Once Connected To Such A Grid, Is No Longer Limited By Its Slow Speed, Small Local Storage, Two Major Impediments To The Use Of "Computational Outsourcing" Are (I) The Fact That The Data In Question Is Often Influences, (Ii) The Quality Of The Computed Answers, Which Is Often Poor (E.G., In Seti Random Answers Afflict Around 40% Of The Computations). This Provide The Design -Ring Ones That Arise In Activity Programming And In Graph Algorithms[3].

iv) Secure And Practical Outsourcing Of Linear Programming In Cloud Computing

The privacy cheating discouragement" Sec-cloud" is used for courage the greater aspects of security. Although the cloud computing is being used to obtain large-scale computations to the cloud, data privacy has become a major issue, the modern cryptographic techniques in secure outsourcing along with the research work, which has been proposed in past years has been presented, which is used for the activities non-demand network access to the shared pool of the computing a stock which is having the greater efficiency as well as large computational power. Basic advantage of cloud computing is that it is having the benefits of centralized large computational power, space and efficiency, so that the customers/clients can outsource their complex problem to the cloud for computation, they have also presented several real time problems for secure outsourcing of complex matrix multiplication and quadrature scientific computations. They have also mentioned the possibility of leakage of confidential and private information. Atallah and Li presented an efficient protocol to securely outsource the sequence comparisons between two servers to overcome the problem of computing using the edit distance between two sequences. Today, data privacy and security become an essential part of various cloud-based applications, multiparty computation scenarios etc. Due to lack of computational resources, clients need to direct their computational problem parameters to cloud, in this area and the general architecture of secure outsourcing linear programming problems in cloud computing. The problem identification in this area has also discussed in this paper and have given the future research directions [14].

v) Attribute Based Data Sharing With Attributes Revocation

In CP-ABE, every client is related with an arrangement of properties and information are encoded with get to structures on characteristics. A client can unscramble a ciphertext if and just if his qualities fulfill the ciphertext get to structure, Specifically, we settle this testing issue by considering more pragmatic situations in which semi-trustable on-line intermediary servers are accessible. When contrasted with existing plans, our proposed arrangement empowers the expert to disavow client properties with insignificant exertion. The present processing innovations have pulled in an ever-increasing number of individuals to store their private information on outsider servers either for simplicity of sharing or for cost sparing. At the point when individuals appreciate the focal points these new innovations and administrations realize, their worries about information security additionally emerge. Normally, individuals might want to make their private information just open to approved clients. Much of the time, it is likewise attractive to give separated access administrations with the end goal that information get to arrangements are characterized over client properties/parts. Sahai and Waters first presented qualities-based encryption (ABE) for encoded get to control. In an ABE framework, both the client mystery key and the ciphertext are related with an arrangement of characteristics. One fascinating future work is to join a safe calculation strategy with our development to ensure the trustworthiness of intermediary servers. Another heading for future work is to enable intermediary servers to refresh client mystery key without unveiling client property data [2].'

vi) Security In Cloud Using Cipher text Policy Attributes-Based Encryption With Check ability

(CP-ABE) is considered as a standout amongst the most appropriate plan for information get to control in distributed storage. In spite of that the current Outsourced ABE arrangements can offload some serious processing intensive to an outsider, the unquestionable status of results came back from the outsider presently can't seem to be tended to. Going for handling the test over, another Secure Outsourced ABE framework is proposed, which underpins both secure outsourced key-issuing and decoding. In ABE framework, clients' private keys and ciphertext marked with sets of spellbinding characteristics and access arrangements separately, and a specific key can unscramble a specific ciphertext just if related qualities and approach are coordinated. Up to this point, there are two sorts of ABE having been proposed: key-approach quality-based encryption (KPABE) and ciphertext-arrangement trait-based encryption (CP-ABE). In KP-ABE, the entrance strategy is doled out in private key, while, in CP-ABE, it is determined in ciphertext, Identity-Based Encryption (IBE) enables a sender to encode a message to a character without access to an open keys endorsement. The capacity to do open key encryption without declarations has numerous useful applications. The client denial should be possible by means of the intermediary encryption system together with the CP-ABE calculation. Another

outsourced ABE conspire is recommended that at the same time bolsters outsourced key-issuing and unscrambling. With the guide of KGSP and DSP, this plan accomplishes consistent effectiveness at both specialist and client sides. At the point when encryption gives information privacy, it likewise incredibly constrains the adaptability of information activity. To address this issue, it is expected to join ABE with cryptographic natives, for example, accessible encryption, private data recovery and homomorphic encryption to empower calculations on encoded information without decoding [21].

vii) Efficient Identity-Based Threshold Decryption Scheme From Bilinear Pairings

Identity based (ID-based) cryptography was proposed by Shamir in 1984 to simplify key management and remove the public key certificates. In ID-based cryptography, the identity of a user, such as his/her e-mail address, is taken as the public key and so the certificate for requirements the public key is not needed. The first practical ID-based encryption (IBE) scheme was proposed in 2001 by Boneh and Franklin, which was proved to be secure against showing chosen ciphertext attack in random oracle model. Since then, in the so-called identity-based cryptography field, many ID-based cryptographic schemes have been proposed. Extension First, our IBTD scheme is very suitable, when the user wants to share his private key out among a number of decryption servers in such a way that any committee member can successfully decrypt the ciphertext Second, our IBTD scheme can be used as a building block to construct a mediated ID-based encryption scheme. The idea is to split a private key associated with the receiver Bob's ID into two parts, and give one share to Bob and the other to the Security Mediator (SEM). Third, since the main computation is the common group operations in the group G or GT and only very few pairings are involved during the decrypting procedure, our IBTD scheme is very efficient and hence is suitable for some resource-restricted applications. We proposed a new identity-based threshold decryption (IBTD) scheme from bilinear pairings. With this scheme, the user can by himself distribute the private key among 17 decryption servers, without bothering PKG in the sharing procedure. It uses much less bilinear pairings than other IBTD schemes in the involved algorithms [10].

viii) **Secure Identity Based Encryption Without Random Oracles**

(IBE) provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number. The corresponding private key can only be generated by a Private Key Generator (PKG)who has knowledge of a master secret. it is only recently that the first working implementations were proposed. Boneh and Franklin [BF01, BF03] defined a security model for identity-based encryption and gave a construction based on the Bilinear Diffie-Hellman (BDH) problem. Extension Hierarchical identities weresecure and private outsourcing of straight variable based math calculations, that specialist a customer to safely presented by Horwitz and Lynn [HL02], and a Hierarchical IBE (HIBE) was first built by Gentry and Silverberg [GS02] in the arbitrary prophet show. The IBE arrangement of sums up normally to give a semantically secure HIBE under an adaptively picked personality assault (IND-ID-CPA) without arbitrary prophets source broad arithmetical calculations to two remote serversoracles A recent result of Canetti et al. [CHK04] gives an efficient way to build a chosen ciphertext IBE (IND-ID-CCA) from a chosen plaintext 2-HIBE (IND-ID-CPA). Thus, by the previous paragraph, we obtain a full chosen identity, chosen ciphertext IBE (IND-ID-CCA) that is provably secure without random oracle We can extend our IBE system to handle identities ID $\in \{0, 1\} *$ (as opposed to ID $\in \{0, 1\}$ w) by first hashing ID using a collision resistant hash function $H\tilde{} : \{0, 1\} * \rightarrow \{0, 1\}$ w prior to key generation and encryption. r, the present system is not very practical and mostly serves as an existence proof. It is still a wonderful problem to find a practical IBE system with a tight security reduction without random oracles, based on Decision BDH or a comparable assumption [13].

III. SYSTEM MODEL

IDENTITY REVOCATION

At the point when an open key, together with a termination date, is marked by a CA, there remains a hazard. That is, a client's private key and endorsement might be stolen/traded off, or an organization's private key and certificate might be held by a previous representative. Without a technique for declaration disavowal, these keys might be utilized by unapproved parties.

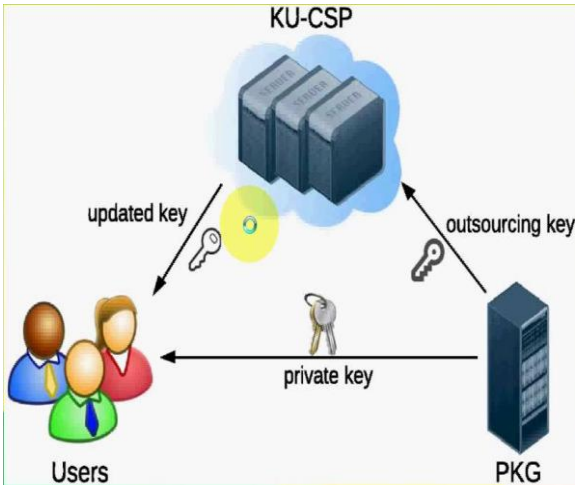

Fig : Identity Based Encryption

Similarly, as with charge cards, periodic denial is an unavoidable truth. As per a few appraisals, around 10% of open keys will generally be denied before they lapse [1]. Along these lines, an essential component of any CA plan (or progressive system) is its repudiation methodology. Notice, that with repudiation, the above straightforward setting turns out to be more required, since now to confirm that some open key is substantial, one must not just watch that it has been marked by the best possible CA, yet in addition that is has not been renounced. (In addition, if there should be an occurrence of CA pecking order, one must guarantee that the CA open key has not been repudiated either). Therefore, the meaning of one's personality relies upon the disavowal governs in a fundamental way. In this paper, we broaden an exquisite strategy for doing repudiations. Before we clarify our approach, let us audit the plan goals and past work done on this issue.

With a specific end goal to accomplish productive disavowal, we present the possibility of "incomplete private key refresh" into the proposed development, which works on two sides: 1) We use a "mixture private key" for every client in our framework, which utilizes an AND door interfacing two sub-parts in particular the character segment IK and the time segment TK individually. IK is created by PKG in key-issuing yet TK is refreshed by the recently presented KU-CSP in key-refresh; 2) In encryption, we take as information client's character ID and in addition the day and age T to confine unscrambling, all the more unequivocally, a client is permitted to perform fruitful decoding if and just if the personality and era inserted in his/her private key are indistinguishable to that related with the ciphertext. Utilizing such aptitude, we can repudiate client's decode capacity through refreshing the time part for private key by KU-CSP.

IV. OUTSOURCING

Homomorphic Encryption : This is a special form of encryption that allows the computations to be performed on ciphertext itself, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. There are numerous partially homomorphic cryptosystems as well as fully homomorphic cryptosystems. Fully homomorphic encryption(FHE) is considered to be more secure than partially homomorphic encryption.

Partially Homomorphic Encryption: A cryptosystem is thought as halfway homomorphic in the event that it shows either added substance or multiplicative homomorphism property, yet not both. A few cases are - RSA(based on multiplicative homomorphism), Palliser(based on added substance homomorphism), El Gamal(based on multiplicative homomorphism)

Fully Homomorphic Encryption: A cryptosystem is thought as fully homomorphic if it manifests both additive and multiplicative homomorphism property. The first (and currently only) before-mentioned system is a lattice-based cryptosystem which was in 2010, proposed and developed by Craig Gentry.[15] FHE is considered as far more powerful and a great way to secure the outsourced data in an efficient manner Ring Homomorphism: Let, P and Q are rings a function

$f : P \rightarrow Q$ will be ring homomorphism if $\forall x1, x2 \in P$.

—$f(x1 + x2) = f(x1) + f(x2)$

—$f(x1 * x2) = f(x1) * f(x2)$

—$f(1P) = 1Q$

Outsourcing computation to entrusted workers" the author R. Gennaro [4] said that, the work is based on the crucial (and somewhat surprising) observation that Yao's Garbled Circuit Construction. In other words,

we can have adapted Yao's construction to allow a client to outsource the computation of a function on a single input. More specifically, in the preprocessing stage the client garbles the circuit C according to Yao's construction. Then in the "input preparation" stage, the client reveals the random labels associated with the input bits of x in the garbling. This allows the worker to compute the random labels associated with the output bits, and from them the client will reconstruct F(x). If the output bit labels are sufficiently long and random, the worker would not be able to guess the labels for an incorrect output, and therefore the client is assured that F(x) is the correct output.

KEY UPDATE AND CLOUD SERVICE PROVIDER

Cloud service providers (CSP) are companies that offers network services, infrastructure, or business applications in the cloud. The cloud services are hosted in a data center than can be accessed by companies' individuals using network connectivity. KU-CSP receives all files from the data owner and store all files on cloud. Check the data integrity in the cloud and inform to end user about the data integrity. Send request to PKG to update the private key of the user based on the date parameter. KU-CSP List all files on cloud, List all the. Updated private key based on the date component and user name, List all File attackers and File Receive Attackers.

PKG

(public key generator):key generator is the way toward creating keys in cryptography. A key is utilized to encode and decode whatever information is being scrambled/unscramble. Present day cryptographic frameworks incorporate symmetric key calculation, (for example, DES and AES) and open key calculation, (for example, RSA). Symmetric-key calculations utilize a solitary shared key; keeping information mystery requires keeping this key mystery. Open key calculations utilize an open key and a private key Receive ask for from the clients to produce the key in view of their special name, Store all keys in light of the client names. Check the username and afterward give the private key to exact end client. Record Receiver on the off chance that they endeavor to hack document in the cloud server and unrevoked the client in the wake of refreshing the private key for the comparing document in light of the client.

Model

The model for IBE consists of an authority that generates a single master public key mpk for all its users, along with a master secret key msk. To encrypt a message, one needs to know the master public key mpk and the receiver's identity id, which can be any string. A user with identity id obtains a secret key skid from the authority (typically after proving his identity in some way). He can use this secret key to decrypt messages sent to him.

Formally, an IBE scheme consists of four ppt algorithms:

- Setup(1,n) outputs a master public key mpk and master secret key msk. This algorithm is executed once by the authority when setting up the system.
- Ext(msk, id) outputs a secret key for every user based on his id. Since only the authority should have access to msk, this algorithm is executed only by the authority after checking a user's identity
- Encryption (mpk, id, m) outputs a ciphertext corresponding to a message m.
- Dec(skid, c) decrypts a ciphertext and outputs a message.

Security Definition

Here we present a formal definition of the notion of IND-CPA security for an IBE scheme. The intuition behind this definition is that a message encrypted to a particular "target" identity id∗ (chosen by the adversary) should remain secret, even if the adversary gets the secret keys for a polynomial number of other identities that are different from id∗.

Definition 1.1. An IBE scheme is IND-CPA-secure if: mpk, E(·), C0 (id*,m0,m1) c ≈ mpk, E(·), C1 (id* , m0, m1) , where (mpk, msk) ← Setup, and E(id) returns Ext(msk, id), except if queried on id∗ in which case it returns ⊥. Furthermore, for an id∗ different from all prior queries to E, the oracle C b (id∗ , m0, m1), returns Enc(mpk, id∗ , mb), defines id∗ as the target identity, and terminates.

The definition can be strengthened in various ways, such as adding chosen-ciphertext security. In such a definition the adversary would additionally get a decryption oracle for the identity id∗ that it is allowed to query on any string except for the challenge ciphertext that was output by C_b.

Background

Throughout this paper we will let N be a Blum integer, i.e., N = pq for primes p and q that are both 3 modulo 4. We use QR ∗ N to denote the set of quadratic residues modulo N. We use a p = a p−1/2 = ±1 mod p to denote the Legendre symbol. (The symbol itself is defined as an integer, not a quantity modulo p).

A natural generalization of the Legendre symbol is the Jacobi symbol, defined as a pq = a p · a q . Note that −1 p = −1 q = −1, hence −1 N = 1 for a Blum integer N. That is, −1 ∈ J ∗ N but is a non-square. Also note that ab N = a N · b N , by the multiplicative property of the Legendre symbol. Finally, we define J ∗ N = a∈ Z ∗ N | a N = 1 , which is a multiplicative subgroup of Z ∗ N . The following claim can be established easily.

Claim 2.1 ; Given a and N (in binary), we can efficiently compute a N without knowing the factoring of N. Proof. The following reciprocity laws can be proved with some effort. We omit their proofs. for odd a and N, a N = N a · (−1) a−1 2 · N−1 2 (2.1) for any N, −1 N = (−1) N−1 2 (2.2) 2 N = (−1) N2−1 8.

For any even number a, we can reduce the problem to the case when a is odd by using equation (2.3). Using equations (2.1) and (2.2) we can iteratively reduce a or N until one of them becomes eauls to 1, when a N can be calculated trivially. The overall algorithm and its complexity is analogous to Euclid's algorithm for finding the gcd of two numbers.

We also present another claim that would be useful in the following section:

Claim 2.2. |QR∗ N | = 1 2 |J N |. Proof. Let a ∈ Z ∗N . Note that a ∈ QR∗ N iff a p = a q = 1, so |QR∗ N | = (p − 1)(q − 1)/4. Also, a ∈ J ∗ N iff a p = a q = ±1, so |J ∗ N | = (p−1)(q−1

2. The security of Cocks' IBE is based on the following assumption which was proposed in the seminal work of Goldwasser and Micali on public-key encryption.

Conjecture 2.3 (Quadratic Residuosity Assumption). For a modulus generation S. or S, hN ← S(1∗), a ← QR∗ N i c ≈ hN ← S(1∗), a ← J ∗ N \ Q

Ni In words, the assumption says that given N, it is hard to distinguish between a random quadratic residue and a random quadratic non residue with Jacobi symbol 1. Note that it is crucial that the element have Jacobi symbol 1, otherwise the tuples could be distinguished trivially by computing the Jacobi symbol a N using Cl

2.1 Interlude: Goldwasser-Micali Encryption:

Scheme As a warm-up to the IBE, we briefly recall the original application of the quadratic residuosity assumption to standard public-key encryption. The Goldwasser-Micali scheme for message space {0, 1} is defined as follows.

• Gen(1n): Generate a Blum integer pk = N as a public key with known factorization sk = (p

• Enc(N, b ∈ {0, 1}): Choose r ← Z ∗ N and output the encryption of b as c = r 2 · (−1)b mod N.

• Dec(sk = (p, q), c): Return m = 0 if c ∈ QR∗ N , and return 1 otherwise. This test can be done efficiently by testing whether both c p = 1 and c q = 1.The proof of security follows directly from Conjecture 2.3, which yields the following theorem.

Theorem 2.4: Under QRA, the Goldwasser-Micali scheme is IND-CPA-secure.

The Cocks IBE Scheme

In this section we define Cocks' IBE scheme and prove its security. To begin, we give a basic public key encryption scheme that works relative to a modulus N, but where decryption can be performed without needing the factorization of N. Instead, decryption will only require knowledge of a square root of a user's public key. Looking ahead, the factorization of N will be the master secret key of the system, which will allow the authority to extract a secret key for any user. Later in Section 3.2, we will convert this PKE into an IBE scheme.

3.1 Warm-Up: Public-Key Encryption Scheme

The PKE is for the message space {±1}, and is defined by the following algorithms, which are all implicitly provided with the modulus N.

• Gen(1n): Generate secret key sk = r ← Z ∗ N and public key pk = r 2 = a ∈ QR∗ N ⊆ Z ∗ N .

• Enc(a, m ∈ {±1}): Choose uniformly random t ∈ Z ∗ N such that t N = m. (This can be done by repetition, since the probability of success for a random choice of t is 1/2.) Output the ciphertext c = t + a/t mod N.

• Dec(r, c): Output c+2r N

From inspection it is not immediately apparent that decryption is correct, but the following claim establishes that this is so

Claim 3.1.. For any r ∈ √ a mod N and any message m ∈ {±1}, we have Dec(r, Enc(a, m)) =m.
Proof. Let t be the random value chosen by Enc where t N = m. The claim follows from the equations given below
. c + 2r N = t + r 2/t + 2r N · t N 2 = t 2 + r 2 + 2rt N · t N = (t + r) 2 N · t N = t N
In the remainder of this section we will argue that the above scheme is IND-CPA secure under the QRA by showing that if the public key pk = a is instead an element of J ∗ N \ QR∗N , then the encryption algorithm Enc is "lossy," i.e., the distributions of Enc(a, +1) and Enc(a, −1) are identical. The following claim establishes this lossy property. Following the claim, we easily prove that this lossiness property implies IND-CPA security.

Claim 3.2. If pk = a ∈ J ∗ N \ QR∗N , then Enc(a, +1) ≡ Enc(a, −1).
Proof. Note that a p = a q = −1. Let c = t + a/t (for some t ∈ Z ∗N) be some fixed ciphertext that could be output by Enc(a, ·). For this fixed c and public key a, consider all solutions t to this equation c = t + a/t. Let t = t0 ∈ Z ∗ N be an arbitrary such solution. Written using the Chinese remainder representation of Z ∗N , there are a total of four solutions:
• ht0 mod p;t0 mod qi has Jacobi symbol t0 N . • ha/t0 mod p;t0 mod qi has Jacobi symbol −1 · t0 N , because a/t0 p = a p t0 p −1 = −1 t0 p .
• ht0 mod p; a/t0 mod qi has Jacobi symbol −1 · t0 N , for similar reasons.
• ha/t0 mod p; a/t0 mod qi has Jacobi symbol t0 N.
Hence, Pr [Enc(a, 1) = c] = Pr [Enc(a, −1) = c], and the proof is complete.
Corollary 3.3 Under the QRA, the basic Cocks public-key encryption scheme is IND-CPA secure
Proof. By the QRA, composition lemma, and Claim 3.2, we have the follow
N, a ← QR∗N ,Enc(a, +1)i c ≈ hN, a ← J ∗ N \ QR∗ N , Enc(a, +1)I ≡ hN, a ← J ∗ N \ QR∗N ,Enc(a, −1)I c ≈ hN, a ← QR∗N ,Enc(a, −1)).

Making It Identity-Baseded We make the scheme identity-based in the random oracle model. Let H : {0, 1} ∗ → J ∗ N be modelled as a truly random function, which will maps identities to public keys in the basic scheme. (Note that such a function can be obtained from a random function H0{0, 1} ∗ → {0, 1} by using the random output bits of H0 to sample from J ∗N .) There is only one subtlety: we cannot detect whether the output of the hash function H is a "proper" or "lossy" public key. The solution is to encrypt (using independent randomness) to both a0 = H(id) and a1 = −H(id), both of which have Jacobi symbol 1, and exactly one of which is a quadratic residue (because −1 ∈ J ∗ N \ QR∗
• Setup(1n) chooses a Blum integer mpk = N = pq as the master public key, and lets msk = (p, q) be the master secret key.
• ExtH(msk, id) lets a0 = H(id) and a1 = −1 · H(id). It returns rid ∈ Z ∗ N as a random square root of a0 or a1, whichever is a quadratic residue
• EncH(mpk = N, id, m ∈ {±1}) lets a0 = H(id) and a1 = −1·H(id), and outputs c0 = Enc(a0, m) and c1 = Enc(a1, m) where Enc(·, ·) is the encryption algorithm of the basic scheme as defined in Section 3.1
• Dec(skid = √ ab, c = (c0, c1)) outputs Dec(skid, cb), where Dec(·, ·) is the decryption algorithm of the basic scheme as defined in Section 3.1.

We now provide an outline of the proof of security for the above scheme; a good exercise is to fill in the details carefully. In order to prove security, we need to give a simulator S(N, a) that attempts to solve the QR problem using an adversary for the IBE scheme. The simulator must provide an msk, and answer oracle queries H(·) and extraction queries Extmsk(·) for arbitrary identities (but without knowing the msk!). The basic idea is that S sets msk = N, and "programs" the random oracle H so that it knows a random square root for ±H(id) for all but a single H(id∗) := ±a, where id∗ is a randomly chosen query to H that S "guesses" will be the adversary's declared target identity. If S does happen to guess this identity correctly, then it prepares a challenge ciphertext by using the basic scheme to encrypt two opposite bits in random order (i.e., either +1, −1 or −1, +1) under a and −a, respectively. Note that by the lossiness property, such a ciphertext is distributed identically as either Enc(id∗ , +1) or Enc(id∗ , −1), depending on whether a or −a is a quadratic residue. Based on whether the adversary identifies the ciphertext as an encryption of +1 or −1, then, the simulator answers whether a ∈ QR∗ N or not.

Description of Scheme

The Sakai–Kasahara scheme allows the encryption of a message to an receiver with a specific identity, . Only the entity with the private key, , associated to the identity, , will be capable of decrypting the message.

As part of the scheme, both the sender and receiver must trust a Private Key Generator (PKG), also known as a Key Management Server (KMS). The purpose of the PKG is to create the receiver's private key, , associated to the receiver's identity, . The PKG must securely deliver the identity-specific private key to the receiver, and PKG-specific public parameter, , to all parties. These distribution processes are not considered as part of the definition of this cryptographic scheme.

Preliminaries

The scheme uses two multiplicative groups E and G It is assumed:

- The Diffie-Hellman problem is hard in **E**. Meaning that given two members of the group P and Q, it is hard to find [**x]** such that**P=Q.**
- The Diffie-Hellman problem is hard in **G**. Meaning that given two members of the group **g** and **t**, it is hard to find **x** such that**gX=t**
- There is a bilinear map, a Tate-Lichtenbaum pairing**e(,)**, from E to G. This means that for a**P** member of**E** and for**g=e(P,P)** a member of **G**: **e(P,[X].P)=e([x].P,P)=e(P,P)^{x}=g^{x}**

Frequently, **E** is a supersingular elliptic curve, such as**E: y^{2}=x^{3} -3x**(over a finite field of prime order**P**). A generator of **P** primeorder**q** is chosen in**E** . The group**G** is the image due to the pairing of the group generated by**P** (in the extension field of degree 2 of thefinite field of order p).

Two hash functions are also required**H$_1$**, and**H$_2$**. **H$_1$**. outputs a positive integer,**x** , such that**1< x < q**.**H$_2$** outputs bits, where isthe length of the message **M**.

Key Generation

The PKG has a master secret**z**where **1 < z < q**and a public key**Z = [z].P**which is a point on **E.** The PKG generates the privatekey,**K$_U$** , for the user with identity**ID$_U$** as follows:

K$_U$

Encryption

To encrypt a non-repeating message**M** , the sender requires receiver's identity**ID$_U$**, and the public PGK value**Z** . The sender performsthe following operation.

1. Create:**id = H1(ID$_U$)**

2.The sender generates using**r = H$_1$(M||id)**

3. Generate the point **R** in**E**:

R = [**r**].([**id**]. **P** + **Z**

4. Create the masked message:

S =M+ H$_2$(g^{r})

5. The encrypted output is **(R,S)**

Note that messages may not repeat, as a repeated message to the same identity results in a repeated ciphertext. There is an extension tothe protocol should messages potentially repeat.

Decryption

To decrypt a message encrypted to**ID$_U$**, the receiver requires the private key**K$_U$**, from the PKG and the public value**Z**. The decryptionprocedure is as follows:

1. Compute**id = H$_1$(ID$_U$)**

2. Receive the encrypted message: (**R,S)**.

3. Compute:**w = e(R,K$_U$)**

4. Extract the message:

M = S+ H$_2$(w)

5. To verify the message, compute**r =H$_1$(M||id)**, and only accept the message if:

[r].([id].P + Z = R

Demonstrationof Algorithmic Correctness

The following equations demonstrate the correctness of the algorithm

W = e (R,K$_U$) = e([r]. ([id]. P + Z), K$_U$)=e([r].([id]. P + [z]. P),K$_u$) = e([r(id + z)]. P, K$_u$)

By the bilinear property of the map:

W = e([r(id + z)]. P, K$_u$) = e([r(id + z)]. P [ ].P) = e(P,P) =g^{r}

As a result:

S + H$_2$ **(w) = (M + H$_2$(g^{r})) + H$_2$(w) = M**

V. CONCLUSION

We introduced outsourcing computation into IBE and propose a revocable conspire in which the disavowal tasks are designated to CSP. With the guide of KU-CSP, the proposed conspire is full-included:1) It accomplishes steady effectiveness for both calculation at PKG and private key size at client; 2) User needs not to contact with PKG amid key-refresh, as it were, PKG is permitted to be disconnected subsequent to sending the disavowal rundown to KU-CSP; 3) No protected channel or client validation is required amid key-refresh amongst client and KU-CSP.

REFERENCES

[1]. 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.

[2]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 261–270.

[3]. D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. 6th Annu. Conf. Privacy Security Trust (PST'08), 2008, pp. 240–245.

[4]. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Security (SEC'11), 2011, pp. 34–34.

[5]. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proc. 8th Int. Conf. Netw. Service manage., 2012, pp. 37–45.

[6]. D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'04), C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer, 2004, vol. 3027, pp. 223–238.

[7]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Cryptology – CRYPTO'98.

[8]. D. Boneh and M. Franklin, "Identity encryption from the well pairing," in Advances in Cryptology.

[9]. 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.

[10]. Wei Gaoa,b, Guilin Wangc , Kefei Chena , Xueli Wangd , Guoyan Zhang Efficient identity-based threshold decryption scheme from bilinear pairings:

[11]. R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation, " Cryptology e-Print Archive, Report 2011/518, 2011.

[12]. J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in Proc. 18th Eur. Symp. Res. Comput. Security (ESORICS), 2013, pp. 592–609

[13]. Dan Boneh∗ Xavier Boyen† Secure Identity Based Encryption Without Random Oracles

[14]. C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2011, pp. 820–828.

[15]. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Security (SEC'11), 2011, pp. 34–34.

[16]. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proc. 8th Int. Conf. Netw. Service manage., 2012, pp. 37–45.

[17]. J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryption of attribute-based encryption with map-reduce," in Information and Communications Security. Berlin, Heidelberg: Springer, 2012, vol. 7618, pp. 191–201.

[18]. S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography (TCC'05), 2005, pp. 264–282.

[19]. 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.

[20]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.

[21]. Security in cloud using ciphertext policy attributes-based encryption with checkability

[22]. M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 48–59.

Dr.Chinthagunta Mukundha "Identity Based Encryption in Cloud Computing With Outsourced Revocation Using Ku-Csp." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 8, 2018, pp. 12-21.