International Journal of Engineering & Technology, 7 (4.22) (2018) 241-245

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

De-duplicating Encrypted Data using ABE & ECC for Secured Cloud Environment

Ch Sri Sumanth[1], Y Raja Rajeshwari Reddy[2], N Sandeep Chaitanya[3]

[1]CSE Dept, VNRVJIET
[2] CSE Dept, VNRVJIET
[3]Asst. Professor,CSEDept, VNRVJIET

Abstract

Attribute-Based Encryption (ABE) was widely used in cloud environments, where owner outsource data to cloud service with an encrypted format and share his data with other users with some specific credentials or attributes. In an existing ABE, Data secure deduplication was not involved only attribute based encryption was involved. In our paper, we have used a deduplication technique with a secured data attribute based encryption using ECC(Elliptic Curve Cryptography) in multi cloud setting. Where a duplicate detection is responsible by private cloud and storage space is managed by public cloud. Compared to other systems we have designed data confidentiality with settings of access policy avoiding the share of decryption keys. And also we have created a system that create only one cipher text as per access policy for a plaintext for different owners data with a different access policy and without revealing the plain text to users.

Keywords *: De-duplication, ABE, Security,Multi cloud,ECC.*

1. Introduction

Data providers widely use cloud computing to outsource their data into cloud to share their sensitive data with outers with some credentials only then can download the data. For this owner have to encrypt their data with access policies which is assigned to each user with specific attributes which he can decrypt the encrypted data[1],[2],[3],[4],[5].

The encryption that is done by using this concept is known as Attribute Based Encryption(ABE), where a user have to provide attribute set which is designed by the data provider for a ciphertext which he want to share with the user. So, these attributes are associated with some access policies for each and every ciphertext. However, already existing ABE have failed in secure de-duplication [7]. This provides the scope of saving storage space in cloud inturn it also minimize the bandwidth utilization by only saving one copy of same plaintext by eliminating duplicate copies and this technique was not built in existing system with secured deduplication [8],[9].

In cloud computing ABE and secure deduplication applied extensively to develope cloud environments. Suppose attribute based system support secure de-duplication of data which is encrypted in cloud environments where duplication of data will not be done even though it receives duplicated copies under different access policies.

Consider a data provider Joe, wants to upload a fileM into cloud and he want to share his fileM with other users having specific attributes. For this, Joe encrypt fileM into ciphertext and provide some attributes with access policy A and upload to cloud, users can download who's attributes satisfy the access policy of fileM. Other data provider having the same cipher text for the same file M but different access policy B wants to upload his file. As the file is encrypted, cloud is unable to see that plaintext of both the data providers are same and it will store two copies or fileM twice, it leads to storage space wastage and also most usage of bandwidth for uploading data.

Our Contributions

In this Paper, we are using a different Attribute based storage system (ABSS),where we use a CP-ABE and also we included data Deduplication in a secured manner.The system which is already designed deals with the data confidentiality by a attribute based encryption method used to store data confidentially in the hybrid cloud architecture.We added a method to create the ciphertext with one access policy that the plaintext of that ciphertext will not be revealed. We also use a technique based on the two cryptographic parts, which includes a no idea proof with commitment scheme, inorder to maintain data consistency.

Normally in the existing deduplication system to store the data, the data provider or owner creates a cipher text which as a tag. Then they will uploads the data into cloud with these ciphertext, after that our methodology comes into work, it checks the data provider tag and run the equality checking algorithm, it verify the tag and if the data is identical to any tag the underling plain text of the same file is already stored so it discards this file. In this system there is no standard notion for security in data confidentiality, because if any one correctly guess the tag by some other means or through a computing technique.

To outwit these disincentives, we have designed a system in hybrid cloud[5], in which there is a responsible taking private cloud for tag checking and ciphertext generation and also a public cloud for storing a ciphertexts. By using this architecture semantic security is achieved under the PRV-CDA security policy[8] is accomplished

under large message storage space uploaded in cloud is unpredictable.

2. Literature Survey

"Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues" has been authourised by Michael Armbrust and published by 2012. This paper mainly focuses on the problems of Private cloud and Public cloud environments , which had a lot of challenges to be faced to create our own private cloud and public cloud. This paper is easy enough for anyone to understand meaning of cloud and cloud computing techniques.

"Vendor lock in cloud storage" has been authourised by Abu-Libdeh and published in 2011. This paper describe about the main reason for cost because of arduous data migration. Where the data provider have to download the data from previous cloud and upload it in present cloud. .Advantages of storage cloud mainly used by customers and providers.. Cloud storage inturn creates new risks ,which has to be carefully inspected before make use of technology. The risk that is mainly focused on was vendor lock-in [17

"Multi-Cloud Data Storing Strategy" with Cost Efficiency and High Availability has been authorized by Mansouri and was published in 2013. The scheme provided by the author is to facilitates the client in getting a proof about data integrity, cloud hosting and storage security. Cloud service has been developed rapidly in services based on multi cloud. The main concerns, when moving services into clouds, is capital expenditure. CHARM, propose a novel cost efficient schema for the cost and availability.

"A Survey on Cost-Efficient Multi-Cloud Data Hosting Scheme with High Availability" has been authorised by T. Nandagopal and published in 2016. The scheme provided by the author is to facilitates the client in getting a proof about data integrity, cloud hosting and storage security. Cloud service has been developed rapidly in services based on multi cloud. The main concerns, when moving services into clouds, is capital expenditure. CHARM, propose a novel cost efficient schema for the cost and availability.

"A Novel Approach to security threats and Cost Efficient Data Hosting Of Cloud Data" has been authorised by A. Bessani and published in 2015. In this methodology, It describe about how to fragment the data and store it in the cloud nodes. Each node in cloud store only one fragment data that is of one file. By this if the file is attacked, there will be no loss of complete data. Moreover, each node is placed in different places by using T coloring graph to avoid attackers by guessing the node location.

"A Framework for Accountability and Trust in Cloud Computing" has been authourised by Ryan, Peter Jagadpraman, Miranda.MSiani Pearson, Markus Kirchberg, QianhuiLiang , Bu Sung Lee and published in 2011. Absence of trust in cloud by the clients is a noteworthy obstruction in the reception of distributed computing , so to over come this issue this paper proposes a structure which tends to responsibility in cloud by means of specialized and strategy based approach which can be effortlessly delineated utilizing a cloud responsibility life cycle (CALC).
Paper proposes the understanding of accountability using CALC. Proposes the Abstraction Layers of Accountability. Proposes investigator as opposed to preventive ways to deal with expanding responsibility.[7]

"A View of Cloud Computing" has been authourised by , Rean Griffith, Armbrust, Fox, Joseph, Randy Katz and published in 2010. Cloud Environment is a dream of figuring as an usable and can possibly change the IT business which makes programming more reachable as administration. This paper gives us knowledge of different cloud models and how they contrast from each other. This additionally demonstrates the impediments and development of cloud computing. Points of interest And Disadvantages is profundity clarification of what cloud computing implies concerning cloud suppliers and buyers. Categorizes Snags and Opportunities for Cloud Computing. Provides a generalized study of cloud computing rather than going into specifics.

"Trust mechanisms for cloud computing" has been authourised by Jingwei Huang and David M Nicole and published in 2013.In these surveys the existing mechanisms for enabling trust and point out there limitations. Which then address those limitations by proposing a frame work.
Cloud trust authority (CTA) is one such framework which includes identity service and compliance profiling service . CTA is developed on philosophy of "Trust= Visibility + Control". Points of interest And Disadvantages are as follows; Gives insight on various existing trust mechanisms. Includes SLA and its association with Trust Mechanisms. Each of the instruments tends to one part of trust however not others make full utilization of the least expensive cloud as what replication does. Still more regrettable, this inadequacy will be opened up in the multi-cloud situation where data transmission is for the most part (much) more costly than storage room.

3. Existing System

3.1 System Architecture

Here, we discuss about the concept of secure de-duplication using cipher policy ABS. The engineering of our ABS consists of four actors they are the cloud, information suppliers, attribute authority (AA) and clients. An information supplier needs to provides information in the cloud and inturn offer the same to concerned clients as per the certificates. As per the attributes AA provides the key as per the concerned attributes. [3]

Cloud Environment comprises with Public cloud responsible for information stockpiling and a private cloud which plays out certain calculation, for example, verifying tag. While transferring a file as per the storage demand, every supplier right off the bat makes a T Tag and a mark L related to information, afterward scrambles the information over an arrangement of attributes.

Likewise, every provider creates a record pf with the relation tag T, mark L and the scrambled message ct3, yet this evidence won't be put away anyplace in the cloud and is just utilized amid the checking stage for any recently produced capacity ask. Subsequent to accepting a capacity ask for, the private cloud which initially checks the legitimacy of the verification pf and afterward tests uniformity the new T tag with present tags in scenario framework.

In the event that there is no counterpart for new T tag, in the private cloud environment it includes T tag and the name L, and advances the name and encoded information, to the public cloud (L, ct) for capacity. Something else, let ct0 be the cipher with tag coordinates the present tag and L0 will be the name concerned to ct0, and afterward the private cloud will executes as takes after. ct0 will be the subset of ct in private cloud which essentially disposes of the recent storage ask for; if it is subset in ct0 , In the private cloud

environment the CSP requests that the public CSP supplant and put away combine (L0, ct0) with the recent (L, ct) in which L = L0. If the ct and ct0 are not properly matched, the private CSP generates same plain text by using the cipher recovery concept to yield another cipher with the association of the dual access policies. At the client side, every client can download a thing, and unscramble the cipher uasing ABPK created by AA if and only if present client's attribute set fulfills the entrance structure.

Every client finds the accuracy of unscrambled information utilizing mark, acknowledges the information in the event that it is reliable with the name. Concerning the ill-disposed storage framework, accept that the PR cloud environment "interested yet genuine" to such an extent that it will endeavor to get the scrambled messages however it will sincerely take after the conventions, though the public cloud is doubted to such an extent that it may mess the name and cipher sets produced by the PR cloud. [12]

Another distinction is the PR cloud and the PU cloud is in previous it will not conspire users4, rather the last intrigue the clients. Suspicion is in accordance with this present reality rehearse in which PR cloud is confided in than the PU cloud. So accept information clients may endeavor to get to information past their approved benefits. Notwithstanding endeavoring to get plaintext information from the cloud, malevolent pariahs may likewise confer copy faking assaults as portrayed previously. The cipher strategy ABSF with secure de-duplication comprises of the accompanying concepts:
Algorithm Setup, ABPK age algorithm, KeyGen, algorithm for Encrypt, testing for legitimacy, Test for validity, fairness testing Test for equality, algorithms for re-encryption, Reencode and unscrambling Decrypt algorithm. [1]

Setup algorithm (p, mk). Considering security parameter, yields the PU parameter standards ace PR key mk. AA control KeyGen(p, mk, A) ! skA. Considering the PU parameter standards, the ace mk and set of attributes A for the info, ABPK creates an skA

Encryption algorithm (p, Ma, Att) ! (skT , CpT). considering the PU parameter, M message, entrance structure A with global attribute information, It yields a skT trapdoor key and a CpT = (T, L, ct, pf), with tag T & L , ct is the cipher incorporates message encryption and additionally entrance structure An, and pf relating to T tage, name L cipher ct. CSP controls it. Both skT, CpT sent to PR cloud.[1]

Testing for Legitimacy (p, CpT) private cloud controls it and considering the PU parameter standards, CpT legitimacy testing parses CpT , and yields 1 if pf is a legitimate confirmation or 0 generally. [1]
.
Test for Uniformity It is controlled by PR cloud(p, (T1, L1, ct1), (T2, L2, ct2)) ! 1=0. Taking the public parameter standards and two tuples (T1, L1, ct1) and (T2, L2, ct2) as the information, this correspondence testing algorithm yields 1 if both (T1, L1, ct1), (T2, L2, ct2) are produced by common fundamental message else 0.{21]

Algorithm for Rencryption It is controlled by PR cloud (p, skT , (L, cpt), A0) ! (L, ct0). Considering PU parameter, the skT and a tag, cipher match (L, cpt) and an A0 as the information, it yields another cipher ct0 related with A0 having a similar name L of the ciphertext ct0.

Algorithm for Decryption(p, (L; ct), A, skA) ! M=?. It is controlled by user 4 Considering PU parameter , mark and cipher match (L; cpt) skA related to An as the information, It yields message M for PR key skA fulfills the entrance structure cipher cpt,L is predictable for M, else display in decoding..

4. Proposed System

ABS With Secure De-duplication using ECC

Here we construct ABSS for secure deduplication, analyze its security, and implement using ECC (Elliptic Curve Cryptography)

Let S = (S.E, S.De be a the classical encryption algorithm. Considering a message M & K key We used ABSS With Secure Dedupication techniques[1] and ECC (Elliptic Curve Cryptography) for performing the encryption [2].

Setup algorithm .considering p as the input and gets the data to be transferred which inturn encrypted by ABE using ECC

Key Generation It also takes p, msk(master PR key) set A = fA1; :::;AjAjg of attributes as the input and computes the keys using ECC skA

Algorithm for Encryption. considering p,M 2 M keys from ECC and encrypts the data, generating skT= w, CT = (T, L, cpt, pf)

Test for Validity. considering inputs P,CpT. In order to check cpt, generates the results and cross check the cipher for PU cloud. else CT will be rejected
.
Test for Equality. Considering inputs P (U1;B1) tags, (U2;B2) tags generates o/p 1 for ^e(U1;B2) = ^e(U2;B1).else 0.

Algorithm for Reencryption. choosing p, skT, and cipher to reencrypt the message.

4.1 Elliptic Curve Cryptography (ECC)

Consider ō > 3 be a prime, m, n ϵ Fō fulfill 4m3 + 27n2 ≠ 0. An elliptic curve E over Fō is characterized with the accompanying equation:[2]

y2 = m3 + an + b, (x, y) ϵ F2ō.

Considering the two indistinguishable points the Point doubling technique is utilized for characterizing the expansion activity on the curve, chord and tangent rule. Framing an added substance Abelian group E(Fp) by Considering the ∞(= −∞) as the character component the various points at interminability and the points in the curve. [2]

We consider 5 curves for quick decrease over Fō NIST utilizes a = −3 for effectiveness reasons. The affine coordinate system is utilized for point reversal. As executed in a point of Jocobian systems (x, y) ϵ E(Fō) is spoken to with 3 coordinates (P : Q : R) ϵ F3ō which thusly fulfill x = P/R2 , y = Q/R3.

In the event that ∞ relates to (1 : 1 : 0), and the negative of (P : Q : R) is (P : −Q : R). Point multiplication (PM) used to check the execution time of ECC is spoken to concerning k ϵ R+, Z ϵ E(Fp), kz is the entirety of kZ's with multi point expansion

B. Generation of Digital Signature using ECC
Consider a base point B with a prime request o which is so near p on the curve. The |n| is considered as size of the key and produce Digital Signature (a, b) which is twofold the length of the key 2|n|. ECC-160

can't be utilized now a days, creating the advanced mark with marking ECC-224 can be acknowledged now and again. To get appropriate proficiency in any event ECC-256 ought to be actualized. In this approach the general population key is PU=dg and private key is D ϵ R Z*o is utilized creating advanced mark. [16]

The message process for message m is d = h(m) which is produced by utilizing a safe one-way hash work h(**) which fulfill |e| ≥ |n|[16]
ECCDS Generation
I/P: private key D, digest d

- Consider k ϵ R Z*o
- (x1, y1) = kG
- a = x1 mod o; go to step 1 if a = 0
- b = k−1(e + dr) mod n; go to step 1 if b = 0

O/P: sig. (a, b)

ECCDS Verification
I/P: public key PU, digest d, Digital signature (a, b)

- stop unless a, b ϵ Z*o
- z = b−1 mod n
- v1 = ew mod n, v2 = aw mod n
- (x1, y1) = v1G + v2Q; reject if (x1, y1)=∞
- accept if a = x1 mod n, else reject

O/P: accept/reject

In SHA-256 h(8) is |n| = 256, h(*). By changing the message measure the message digests is sent to the next cloud. Thus the messages are straightforward to the mists and the execution increments directly thinking about the movement. It legitimize the age of mark is fairly that quicker when contrasted with check of mark [16]. So computerized signature age for the propose of security is finished.

4.2. Adaptable Attribute-Based Encryption

Lai et al. displayed crypto crude called versatile CP-ABE, in which a half-trusted intermediary brought in setting of CP-ABE. The intermediary, provides a framework with a trapdoor key, can convert cipher text under one access policy arrangement into an another cipher texts of the same plaintext under a different access strategies without adapting any data about the plaintext amid the procedure of change. Nonetheless, this technique for utilizing a solitary trap door key for cipher texts are very hazardous, as if a single key is bargained, security for framework is completely broken. Antagonistic client utilizing the bargained trap door key recover a cipher for a structure that characteristics fulfill, in this way we can get the plaintext . In addition, the trap door entry produced by the AA[4] which will monitor the unscrambling keys, so it is alluring to decrease vitality for encryption control. Not at all like that in [4], our strategy is coordinated with the main concept that each trap door key will be used to change its concerned cipher. Along these lines, even sooner or later, a trap door keys are included, harm canbe restricted for a single message. For an abnormal state, our method conveys different approach that fabricate versatile CP-ABE frameworks from an alternate perspective.

4.3. De-duplication in Hybrid Cloud(HC) Environment

An inalienable disadvantage in the current ways is to deal with accomplish secure de-duplication that can't fulfill the security for secrecy, for example, semantic security. To take care, a lower security idea called protection under picked conveyance assaults [4] was advanced under the presumption that the info message is adequately capricious. Not quite the same as the current technique for characterizing a lower security idea in the distributed storage framework with secure de-duplication, a cross breed cloud environment design, comprising a couple of open & private mists will be presented in our capacity framework to such an extent that the semantic security ends up noticeably achievable for the general population cloud. This system of twin mists has been generally embraced by and by, where the security of people in general cloud more often than not stands up to more difficulties than that of the private cloud, and subsequently it is alluring to have more grounded information classification insurance at the general population in the side of cloud. Trust that half and half cloud environment engineering is the great way in case of capacity frameworks with de-duplication, where the encoded information is out sourced to the cloud while in the private cloud de-duplication is checked.

5. Conclusion

ABE and ECC(Elliptic Curve Cryptography) has been widely utilized as a part of cloud processing where information providers provides their information to the cloud environment and will include the information to clients having indicated credentials. Then again, deduplication is an essential procedure to spare the storage room and system transfer speed, which disposes of copy duplicates of identical information. Be that as it may, the standard ABE frameworks don't bolster secure deduplication, which makes them expensive to be connected in some business stockpiling administrations. This storage technique is worked in cloud design, in which the private cloud will control the calculation of an open cloud environment which deals with the capacity. In Private cloud environment it is provided including a trap door key which is related to the comparing cipher, with this it can exchange the cipher for more access arrangement in to the cipher of the same plain text under different policies with out considering the plaintext. In the wake of accepting a capacity ask for the private cloud environment which first checks the legitimacy of the upload thing in the joined verification. On the off chance that the verification is substantial, the private cloud environment runs a label coordinating calculation to check whether similar information underlying the ciphertext has been put away. Assuming this is the case, at whatever point it is fundamental, recover the cipher into a cipher of the same plain text on a entrance strategy depending on the access arrangements. This proposed stockpiling framework appreciates two noteworthy points of interest. Right off the bat, it can be utilized to confidentially impart information to different clients by indicating an entrance strategy as opposed to share the key. Also, it accomplishes the concept of semantic security with de-duplication plots just accomplish with a lower security idea.

References

[1] Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud Hui Cui, Robert H. Deng, Yingjiu Li, and Guowei Wu DOI 10.1109/TBDATA.2017.2656120, IEEETransactions on Big Data

[2] N Sandeep Chaitanya “Implementation of Security & Bandwidth Reduction in Multi Cloud Environment ” in IEEE Digital Explore IEEE ISBN: 978-1-5090-5256-1/16/$31.00_c 2016 page no 758-763

[3] N Sandeep Chaitanya “Integrity Verification on Clustered Data using PDP in Cloud Environments” in IRED Journal and the same is presented in Sixth International Conference On Advances in Computing, Electronics and Electrical Technology - CEET 2016. DOI: 10.15224/978-1-63248-109-2-24 Page(s): 145 - 149

[4] N Sandeep Chaitanya “CBP Based Bandwidth Reduction in Secured Clouds” in International Journal of Applied Engineering Research, page no:203-208, ISSN 0973-4562 Vol. 10 No.81 (2015) © Research India Publications; http://www.ripublication.com /ijaer.htm

[5] N Sandeep Chaitanya "Raid Technology for Secured Grid Computing Environments" in IEEE NCC 2012 at IIT Karagpur Print ISBN: 978-1-4673-0815-1 INSPEC Accession Number: 12654144 Digital Object Identifier : 10.1109/NCC.2012.6176738 IEEE Catalog Number: CFP1242J-ART,

[6] N Sandeep Chaitanya "Springer" Ist International Conference on Advances in Computing &Communications(ACC-11) with title "Data Privacy for Grid Systems" A. Abraham et al. (Eds.): ACC 2011, Part IV, CCIS 193, pp. 70–78, 2011. © Springer-Verlag Berlin Heidelberg 2011

[7] D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing / Elsevier, 2014. [Online]. Available: http://www.elsevier.com/books/cloud-storageforensics/ quick/978-0-12-419970-5

[8] K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography: Theory, practice and future research directions," FutureGeneration Comp. Syst., vol. 62, pp. 51–53, 2016.

[9] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics: State-of-the-art and future directions," Digital Investigation, vol. 18, pp. 77–78, 2016.

[10] Y. Yang, H. Zhu, H. Lu, J.Weng, Y. Zhang, and K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

[11] D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.

[12] Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[13] Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneck in the data domain deduplication file system," in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 26- 29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[14] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[15] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, Message-locked encryption for lock-dependent messages," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer, 2013, pp. 374–391.

[16] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. USENIX Association, 2013, pp. 179–194.

[17] M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in Public-Key Cryptography – PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 – April 1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol. 9020. Springer, 2015, pp. 516–538.

[18] S. Bugiel, S. N¨ urnberger, A. Sadeghi, and T. Schneider, "Twin clouds: Secure cloud computing with low latency - (full version)," in Communications and Multimedia Security, 12th IFIP TC 6 / TC 11 International Conference, CMS 2011, Ghent, Belgium, October 19-21,2011. Proceedings, ser. Lecture Notes in Computer Science, vol. 7025. Springer, 2011, pp. 32–44.

[19] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems (extended abstract)," in Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA. ACM, 1985, pp. 291– 304.

[20] M. Fischlin and R. Fischlin, "Efficient non-malleable commitment schemes," in Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, ser. Lecture Notes in Computer Science, vol. 1880. Springer, 2000, pp. 413–431.

[21] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput.Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.