A Survey on Cloud Storage Auditing Free Through Denial-Based Encryption Attribute

1 B.THRIVENI 2 D.RAJA REDDY

Abstract— Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

1 INTRODUCTION

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed, including .Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant [8]. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies [9], [10]. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lavabit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to

shut down its email service .Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called deniable encryption, first proposed in . Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data1.

In this work, we describe a deniable ABE scheme for

1. Some papers divide this role into service providers and trusted key managers. More specifically, one is for cloud service operation, while the other is for key management and is assumed to be trusted. In this work we use cloud storage providers for both functions for simplicity. Further, this is also a common case in practice. Note that it is not difficult to apply our scheme to an architecture that has these two different roles defined. cloud storage services. We make use of ABE characteristics for securing

stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme [4]. We enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

2. Our Contributions

In this work, we construct a deniable CP-ABE scheme that can make cloud storage services secure and auditfree. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability. All data are encrypted into the multidimensional space. Only with the correct composition of dimensions is the original data obtainable. With false composition, ciphertexts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. We make use of composite order bilinear groups to construct the multidimensional space. We also use chameleon hash functions to make both true and fake messages convincing. Our deniable ABE has the advantages described below over previous deniable encryption schemes.

• **Blockwise Deniable ABE**. Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case. To solve this problem, O’Neil et al. designed a hybrid encryption scheme that simultaneously uses symmetric and asymmetric encryption. They use a deniably encrypted plan-ahead symmetric data encryption key, while real data are encrypted by a symmetric key encryption mechanism. This reduces the repeating number from the block size to the key size. Unlike those techniques used in previous deniable encryption schemes, we build two encryption environments at the same time, much like the idea propose. We build our scheme with multiple dimensions while claiming there is only one dimension. This approach removes obvious redundant parts. We apply this idea to an existing ABE scheme by replacing prime order groups with composite order groups. Since the base ABE scheme can encrypt one block each time, our deniable CPABE is certainly a blockwise deniable encryption scheme. Though the bilinear operation for the composite order group is slower than the prime order group, there are some techniques that can convert an encryption scheme from composite order groups to prime order groups for better computational performance.

• **Consistent Environment**. Most of the previous deniable encryption schemes are inter-encryption independent. That is, the encryption parameters should be totally different for each encryption operation. If two deniable encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility. For example, once coercers get private keys, which are the most common receiver proofs, these keys should be convincing not only under some particular files, but also under all related stored data. Otherwise, the coercers will know that these keys are fake; however, all proposed schemes only provide convincing proofs for particular transmissions. The deniability of our scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, we can construct the released fake key to decrypt normal ciphertexts correctly.

• **Deterministic Decryption**. Most deniable encryption schemes have decryption error problems. These errors come from the designed decryption mechanisms. The concept of our deniable scheme is different than these schemes described above. Our scheme extends a pairing ABE, which has, the coercers will know that these keys are fake; however, all proposed schemes only provide convincing proofs for particular transmissions. The deniability of our scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, we can construct the released fake key to decrypt normal ciphertexts correctly. This reduces the repeating number from the block size to the key size. Unlike those techniques used in previous deniable encryption schemes, we build two encryption environments at the same time, much like the idea propose. We build our scheme with multiple dimensions while claiming there is only one dimension. This approach removes obvious redundant parts.

We apply this idea to an existing ABE scheme by replacing prime order groups with composite order groups. Since the base ABE scheme can encrypt one block each time, our deniable CPABE is certainly a blockwise deniable encryption scheme. Though the bilinear operation for the composite order group is slower than the prime order group, there are some techniques that can convert an encryption scheme from composite order groups to prime order groups for better computational performance. deterministic decryption algorithm, from the prime order group. The sender proof is still inter-independent, because receiver proofs are related to user keys whereas sender proofs are related to random for encryption composite order group. The decryption algorithm in our scheme is still deterministic; therefore, there is no decryption errors using our scheme.

3. Organization

In additional to this introductory section, we introduce preliminaries used in this paper. We formally define deniable CP-ABE and its properties. We show how to set up a basic deniable CPABE scheme and prove security, deniability and other features of our scheme. We transform our basic scheme from composite order groups to prime order groups. We then enhance our scheme to be chosen ciphertext attack (CCA) secure, we implement our deniable schemes and evaluate their performance. Finally, we present our conclusions.

3.1 Chameleon Hash

The idea behind the chameleon hash scheme was first Introduced. Just like other common secure hash functions, a chameleon hash scheme has two key properties, namely **collision resistance** and **semantic security**. Further, a chameleon hash scheme also provides **collision forgery** with a predetermined trapdoor. The input of a chameleon hash includes two parts, one being input message m and the other random string r. The random string r is used to provide a chance to adapt the message for the hash value. The definitions of the three aforementioned requirements, **collision resistance**, **semantic security** and **collision forgery**, are listed below.

4 DEFINITION

4.1 Deniable CP-ABE Scheme

Deniable encryption schemes may have different properties and we provide an introduction to many of these properties below.

- ***ad hoc deniability vs. plan-ahead deniability*****:** The former can generate a fake message (from the entire message space) when coerced, whereas the latter requires a predetermined fake message for encryption. Undoubtedly, all bitwise encryption schemes are adhoc.

• ***sender-, receiver-, and bi-deniability***: The prefix here in each case implies the role that can fool the coercer with convincing fake evidence. In sender-deniable encryption schemes and receiver-deniable schemes, it is assumed that the other entity cannot be coerced. Bi-deniability means both sender and receiver can generate fake evidence to pass third-party coercion.

• ***full deniability vs. multi-distributional deniability***: A fully deniable encryption scheme is one in which there is only one set of algorithms, i.e., a keygeneration algorithm, an encryption algorithm and so on. Senders, receivers and coercers know this set of algorithms and a sender and a receiver can fool a coercer under this condition. As for multidistributional deniable encryption schemes, there are two sets of algorithms, one being a normal set, while the other is a deniable set. The outputs of algorithms in these two sets are computationally indistinguishable. The normal set of algorithms cannot be used to fool coercers, whereas the deniable set can be used. A sender and a receiver can use the deniable algorithm set, but claim that they use the normal algorithm set to fool coercers..

• ***interactive encryption vs. non-interactive encryption***: The difference between these two types of encryption is that the latter scheme does not need interaction between sender and receiver. According to the above definitions, the ideal deniable encryption scheme is *ad hoc*, *full*, *bi-deniability* and *noninteractive deniability*; however, there is research focused on determining the limitations of the deniable schemes. In Nielsen stated that it is impossible to encrypt unbounded messages by one short key in non-committing schemes, including deniable schemes. Since we want our scheme to be blockwise deniable with a consistent encryption environment, we design our scheme to be a plan-ahead deniable encryption scheme.

4.2 Security Proof

To prove that our deniable encryption scheme is secure requires this scheme to be a valid encryption scheme. For a multi-distributional deniable encryption scheme, it is only necessary to prove the security from the normal algorithm set. That is, we only need to prove the security of a scheme composed of the following four algorithms **Setup**, **KeyGen**, **Enc**, and **Dec**. As for the deniable algorithms, since deniable keys and ciphertexts are indistinguishable from normal keys and ciphertexts, which will be proved in the next subsection, deniable algorithms will be treated as normal algorithms which are proved to be secure.

4.3 Deniability Proof

To prove the deniability of our CP-ABE scheme, we must show (M,C, PE, PD) and (M′,C′, P′ E, P′ D) are indistinguishable. Since M,C,PE,PD are pairwise independent because of the security property.

4.4 Decryption Errors

In section 1, we described why most deniable schemes may cause decryption errors. Most of these schemes claim their decryption error rates are small or negligible, but they cannot ensure that there are no errors whatsoever in their schemes. In our scheme, a receiver uses a one-way function with a signature to obtain the true message. Both the one-way function and the signature are generated by the sender. That is, the sender can avoid any decryption errors in encryption.

5 DENIABLE CP-ABE CONSTRUCTION FROM PRIME ORDER BILINEAR GROUP

In the previous section, we described how to design adeniable CP-ABE scheme with composite order bilinear groups for building audit-free cloud storage services. Composite order bilinear groups have two attractive properties, namely **projecting** and **cancelling**, defined by Freeman in. We make use of the cancelling property for building a consistent environment; however, Freeman also pointed out the important problem of computational cost in regard to the composite order bilinear group. The bilinear map operation of a composite order bilinear group is much slower than the operation of a prime order bilinear group with the same security level. That is, in our scheme, a user will spend too much time in decryption when accessing files on the cloud. To make composite order bilinear group schemes more practical, Freeman converted into prime order schemes. Meiklejohn et al. showed that both projecting and cancelling cannot be simultaneously achieved in prime order groups.

6 PERFORMANCE EVALUATION

In this section, we evaluate the performance of our idea by implementing two deniable schemes: the composite order scheme and the prime order simulation scheme. We compare them with the Waters scheme. We use the Pairing Based Cryptography (PBC) library for cryptographic operations. Our experiments focus on one block encryption/decryption. A large file can be divided into multiple blocks, and all blocks can be protected by one secret s. Because GT multiplication and H are lightweight operations, we use one-block encryption/decryption to evaluate the performance. The composite order scheme is undoubtedly the most time consuming scheme; its performance is almost unacceptable for practical applications. The reason for this poor performance is that all arithmetic and pairing operations are executed in a group much larger than those for the other two schemes. As for the prime order simulation scheme, it takes little time to get the deniability feature from the Waters scheme and therefore, the prime order simulation scheme is suitable to be distributed to cloud storage services for the deniability feature.

CONCLUSIONS

In this work, we proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy.

REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Eurocrypt*, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in *Public Key Cryptography*, 2011, pp. 53–70.

[5] A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in *Crypto*, 2012, pp. 199–217.

[6] S. Hohenberger and B. Waters, “Attribute-based encryption with fast

decryption," in *Public Key Cryptography*, 2013, pp. 162–179.

[7] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds." *IEEE T. Cloud Computing*, pp. 172–186, 2013.

[8] Wired. (2014) Spam suspect uses google docs; fbi happy. [Online]. Available: http://www.wired.com/2010/04/cloud-warrant/

[9] Wikipedia. (2014) Global surveillance disclosures (2013present). [Online]. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)

[10] ——. (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden

[11] ——. (2014) Lavabit. [Online]. Available: http://en.wikipedia. org/wiki/Lavabit

[12] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in *Crypto*, 1997, pp. 90–104.

[13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Eurocrypt*, 2010, pp. 62–91.

[14] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R`afols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, 2012.

[15] M. D¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in *Eurocrypt*, 2011, pp. 610–626.

[16] A. O'Neill, C. Peikert, and B. Waters, "Bi-deniable public-key encryption," in *Crypto*, 2011, pp. 525–542.

[17] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in *WPES*, 2010, pp. 31– 42.

AUTHOR'S PROFILE:

1.B.THRIVENI
Thriveni0305@gmail.com

2.D.RAJA REDDY
ASSISTANT PROFESSOR

raajaareddy@gmail.com