Elliptic Curve Cryptography Digital Signature Algorithm For Privacy-Preserving Public Auditing For Shared Data In The Cloud

Vanitha. M[1]
Assistant Professor,
Department of Information Technology
Sri Eshwar College of Engineering,
e-mail: vanitham87@gmail.com

K. Subramani[3]
Technology Lead,
Infosys Limited,
Mysore ,
e-mail: subramani_k@gmail.com

Jayapratha. T[2]
Assistant Professor,
Department of Information Technology
Sri Eshwar College of Engineering,
e-mail: itzbtechengineer@gmail.com

Pradeepa. T[4]
Research Scholar,
Department of Computer Science
Sri Ramakrishna College of Arts and Science for Women
e-mail: tdeepu1991@gmail.com

***Abstract*—** Cloud computing becomes one of the emerging technology on now a days to share and manage their data in organization , because of its forcefulness, small communication cost and everywhere environment. Privacy preservation concern in the cloud computing becomes arise several security challenges since information stored in the cloud data is easily outsourced anywhere at any time. To manage this privacy preservation in cloud computing several number of the mechanism have been proposed in earlier work to permit both data owners and public verifiers toward proficiently audit cloud information integrity without leakage information from cloud server. But major issue of the existing works becomes these methods is that unavoidably disclose secret data to free verifiers. In order to overcome this problem in this paper presents novel privacy-preserving elliptic curve digital signature cryptography methods data integrity with the purpose to maintain public auditing on shared information stored which is stored in the cloud computing database. In the proposed methods digital signature are created to each data owner in the cloud computing environment and attain data integrity confirmation for shared information between one cloud data owner to third party auditor. In our proposed data integrity Elliptic Curve Cryptography Digital Signature Algorithm, the individuality of the signer on every one chunk in shared information is reserved privately secure manner by creation elliptic curve based private key from public verifiers. Further improve accuracy of the privacy preservation for shared information in the cloud computing proposed ECCDSA perform manifold auditing tasks parallel. The experimentation results of the proposed ECCDSA based multiple data auditing task shows that higher efficiency and higher data integrity while performing auditing task, it can be compared with existing public auditing methods.

Keywords- *Cloud Computing, Data Auditing Task, Elliptic Curve Cryptography Digital Signature Algorithm (ECCDSA), Access control, Data security.*

*****

I. INTRODUCTION

Cloud computing is new emerging technology to manage system resources be make available vigorously using Internet. It is a focus for substantial awareness and concentration from together academic world and business. Conversely, it has to face some of the few challenges earlier to apply them to real life time applications. First of all, information privacy must be assured. Since the individual perceptive information is stored in cloud database, privacy risks would rise considerably. Unconstitutional users might moreover be capable to interrupt someone's information. Secondly, individual information is next to hazard since one's individuality is legitimate according to his personal information. As people are attractive additional worried regarding their confidentiality these days, the privacy-preservability is very significant. If possible, someone authority should not distinguish some client's individual information. It should not be flexible in the case of protection violation since some part of the structure is cooperating through attackers.

Privacy concerns occur at any time perceptive information is outsourced to the cloud. Through using encryption, the cloud server is prohibited from learning substance in the cloud computing outsourced databases. However how can we also avoid a confined administrator from learning substance in the cloud computing outsourced databases. And how can we evade situation such as: employees via cloud applications may perhaps study additional than it is required to carry out their individual responsibility.

The reliability of information in cloud storage, conversely, is subject to uncertainty and examination, as information stored in the cloud preserve simply be vanished ,due to the unavoidable hardware/ software malfunction and human mistake [1-2]. To formulate this substance still worse, cloud service providers might be indisposed to notify users concerning these information errors in regulate to preserve the character of their services and evade losing profits [3]. So, the reliability of cloud information must be confirmed earlier than any information exploitation, such as exploration or computation exceeding cloud information [4].

The most important motivation is that the amount of cloud information is huge in common. Downloading the complete cloud information to confirm information integrity, especially less computation cost and communication resources becomes difficult. Besides, numerous use of cloud information does not essentially necessitate users to download the entire cloud information to restricted devices [5]. Since cloud providers, such as Amazon, be able to suggest users computation services

straightforwardly on large-scale information that previously be present in the cloud.

In addition, several numbers of works [6]–[9] have been proposed to generate additional data privacy requirements to exist strongly and proficiently confined in cloud computing environment [10]–[12]. These methods weakness to preserve individuality confidentiality on public information throughout public auditing determination expose important secret information to public verifiers. In order to safe guard cloud user secret information, it is necessary and very significant to protect individuality confidentiality from public verifier and third party auditor (TPA) during unrestricted auditing. In order to solve above mentioned privacy preservation issue in cloud computing data on shared information, through proposing elliptic curve cryptography digital signature algorithm public auditing cloud computing data mechanism. More specifically, proposed system make use of the concepts of the elliptic curve cryptography digital signature algorithm thus number of key and signatures are generated to each data owner in the cloud computing environment, therefore that a public verifier is capable to authenticate the reliability of shared information without retrieving the entire information. The proposed ECCDSA perform manifold auditing tasks concurrently and improve the effectiveness of data confirmation for manifold auditing tasks in cloud data auditing task.

II. BACKGROUND KNOWLEDGE

The conventional approach designed for examination of information appropriateness is to recover the complete information from the cloud, and subsequently authenticate information integrity by proposing data integrity methods such as MD5 [13]. Positively, this traditional method is capable to effectively verify the exactness of cloud information. But major problem is that improving the effectiveness for these methods still becomes more doubt [14] in cloud computing information environment. These methods also extended to public data task to confirm the verification of the data owner [15] and cloud data also in cloud computing environment. Though, a new-fangled important privacy problem is that outflow of individuality confidentiality to public verifiers [15].

The conventional approach designed for examination of information appropriateness is to recover the complete information from the cloud, and subsequently authenticate information integrity by proposing data integrity methods such as MD5 [13]. Positively, this traditional method is capable to effectively verify the exactness of cloud information. But major problem is that improving the effectiveness for these methods still becomes more doubt [14] in cloud computing information environment. These methods also extended to public data task to confirm the verification of the data owner [15] and cloud data also in cloud computing environment. Though, a new-fangled important privacy problem is that outflow of individuality confidentiality to public verifiers [15].

Sahai as well as Waters proposed a new type of IBE – Fuzzy Identity-Based Encryption [16], which is known as Attribute-Based Encryption (ABE). During their work, individuality is viewed, since a set of descriptive attribute. Dissimilar from the IBE, everywhere the decrypter possibly will decrypt significance if as well as only if his identity is accurately equivalent as what specific by the encrypter, this fuzzy IBE enable decryption condition are 'identity overlaps' more than a pre-set threshold among one specified by encrypter, the single belong toward decrypter. Though, this category of threshold-based method was restricted designed for common classification since threshold base semantic cannot communicate a common condition.

Key-Policy Attribute-Based Encryption (KP-ABE) [17] as well as Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [18], are future by Goyal et al. as well as Bethencourt et al. correspondingly overcome the abovementioned disadvantage of fuzzy IBE. It look equivalent, although ciphertext as well as key structures are completely dissimilar, as well as decision of encryption policy is prepared through different parties.

Kubiatowicz et al. [19] explain structural design for encrypted determined storage during Cloud called OceanStore; Sadeghi et al. [20] explain a procedure throughout usage of a tamper-proof hardware token. This method applies toward a cloud service supplier which is base scheduled trust compute platform. An additional project is from Pearson et al. ([21], [22]) to facilitate combine several of preceding techniques. The key suggestion for mostly establishment of a Privacy Manager, as well as responsibility represented as a result of a Trusted Platform Module.

III. PROPOSED STOCHASTIC GRADIENT FOR FCM ALGORITHM BASED ON ONLINE KERNEL LEARNING

In this work presents a novel ECCDSA based public data auditing system for preserving privacy in cloud computing for stored information. The proposed method make use of the concept of the elliptic curve based digital signature method and verifiably at random also proposed in ECCDSA to assurance with the intention of the TPA to remove the trouble of cloud user from the deadly and probably perform exclusive auditing task. The cloud computing storage parameters ECCDSA consist of a suitably chosen elliptic curve defined over a finite field F_p of feature , and base of $G \in E(F_{pc}$,it is specified to group of cloud user ,procedure for generating random elliptic curves for each cloud user also mentioned in the following sections and it also verified through the generation of the number ,also meeting cloud user requirements that simultaneously hold numerous examination sessions beginning different users in favor of their outsourced information files in a group way designed for better efficiency.

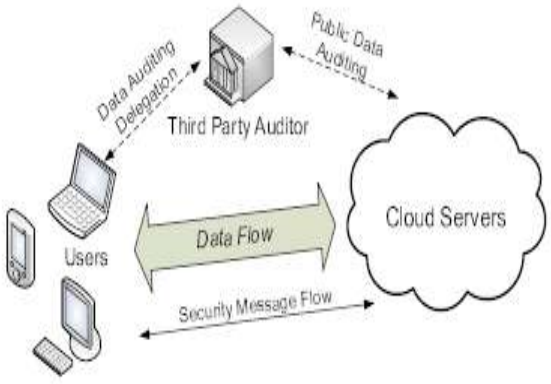

Figure 1. The architecture of cloud data storage service

The general architecture of the cloud storage environment for retrieving a copy of the whole to the cloud users is shown in Figure 1. The privacy preservation requirements of the cloud

user need to follow the following steps to satisfy the batch public auditing task.

1) Public auditability: to permit TPA to confirm the appropriateness of the cloud data on demand without recover a duplication of the whole data of cloud users.
2) Storage space suitability: to make sure with the intention of present exists no corrupting cloud server so as to can pass the TPA's audit not including indeed storing users' data together.
3) Privacy-preserving: to make sure with the purpose of the TPA cannot originate users' data substance from the information collected throughout the auditing procedure.
4) Batch auditing: to permit TPA through protected and well-organized auditing ability to manage through manifold auditing delegation beginning probably huge amount of diverse users concurrently.
5) Lightweight: to permit TPA to execute auditing through smallest amount of communication cost and time complexity.

A. *Domain Parameters*

In order to formulate simple interoperability, a number of limits are positioned on the fundamental field size for private key for cloud user and the illustration of the data attribute elements as . Furthermore, to keep away from a number of explicit well-known attacks, limits are positioned on the elliptic curve. A practical method to safeguard cloud user data against unauthorized cloud user and some special kind of curves might be exposed in the future, is to choose the elliptic curve at arbitrary focus to the condition with the intention of . A curve can be chosen verifiably at random through decide the general parameters of the elliptic SHA-1 function according to a number of pre-specified process. To review, domain parameters for each cloud user in the cloud computing environments using the following conditions are comprised of:

1. Private key size for cloud data owner is represented as , where either , an odd prime, or ;
2. An suggestion of cloud user attributed information as (field representation) and it is represented in the form of
3. Choose a bit string that contains less 160 bits.
4. Two attribute elements of the cloud user as which describe the elliptic curve over .
5. Two attribute elements of the cloud user in a group as in which define a group as f prime order
6. The order of the point with and cofactor

B. *Generating an Elliptic Curve Verifiably at Random*

This section describes the technique with the purpose to generating a random number to each cloud user data or information based on the elliptic curve verifiably at random. The random number of the cloud user data are generated based on the SHA-1 hashing function ,This proposed system gives more assurance to each cloud user and their cloud user data or information in elliptic it might consequently make use to recover the clouds user's private keys.

ALGORITHM 1: GENERATING A RANDOM ELLIPTIC CURVE OVER .

INPUT: A field size , where is an odd prime.

OUTPUT: A bit string of length at least 160 bits and attribute elements which define an elliptic curve over

1. Select an random bit string of duration .
2. Calculate random hash key for each cloud user and let represent the bit string of length bits attain through taking the rightmost bits
3. Let be the randomly generated number for cloud user integer whose twofold development is specified through the -bit string
4. For from 1to s do:

4.1 let through string which is the twofold development of the digit.

4.2. Compute

5. Let be the integer whose twofold development is specified through .
6. If then go to step 1.
7. Select random integers , for cloud user attribute field information not both , such that
8. The elliptic curve of the cloud user data are selected over
9. Output

C. *Domain parameter generation*

1. Choose coefficients and from verifiably at arbitrary manner
2. Calculate
3. Authenticate that is separable through a huge prime number ,if not accept than go to step 1.
4. Confirm with the intention of it might not for each k . If not, then go to step 1.
5. Authenticate that .If it doesn't satisfy then go to step 1.
6. Select an arbitrary point and set

Repeat until .

D. *Domain Parameter Validation*

Domain parameter confirmations make sure that the cloud user information parameters include the necessary mathematical property these are defined through the use of digital signature algorithm by Blake-Wilson and Menezes [23].

The assurance that a set of ECC domain parameters is valid for cloud user information if the selected cloud user is valid only ,it is verified using following one of the methods:

1. cloud user information process explicit cloud organization information and parameter validation
2. generates itself with a trusted scheme.
3. receives guarantee from a trusted party through performing Domain parameter generation and validation
4. receives guarantee from a trusted party with the intention of was created through the use of trusted system.

EXPLICIT VALIDATION OF A SET OF EC DOMAIN PARAMETERS:

INPUT: A set of EC domain parameters D = (PCC

OUTPUT: Acceptance or rejection of the validity of .

1. Authenticate that is an odd prime.
2. Authenticate that FR is a "valid" representation for .'.
3. Authenticate that
4. Authenticate that , and are appropriately characterized cloud user attribute elements of for elliptic curve
5. Authenticate that lies on the elliptic curve defined through two different cloud user attributes
6. Authenticate that n is prime , and authenticate that
7. Compute and verify that .
8. Authenticate that does not separate for each cloud user .
9. Authenticate that .
10. If any confirmation be unsuccessful, then is unacceptable; otherwise is suitable.

An ECCDSA key pair for cloud user information is connected through a specific set of the general ECC parameters discussed above steps. The public key of the cloud user is a random numerous and private key of the cloud user information is generated based on the integer number to perform multiple auditing task.

E. Key Pair Generation

An entity of cloud user 's pair of the key value is generated through a particular set of ECC parameter values are mentioned above. .

ECCDSA KEY PAIR GENERATION: Each cloud user does the following:

1. Select a random primed number cloud user in the interval .
2. Calculate private key for cloud user
3. Cloud user s public key is 's private key is .

METHODS FOR VALIDATING CLOUD DATA OWNER PUBLIC KEYS: The guarantee with the intention of a public key generation for cloud data owner is valid or not be present to specific cloud user using one of the following methods:

1. Cloud user complete explicit public key confirmation algorithm as specified in 6 for each cloud user in the cloud sharing environment.
2. Cloud user generates hitself with a expectation scheme.
3. Cloud user accept guarantee from a trust party in Algorithm 6.
4. Cloud user accept guarantee from a that public key was created via a trusted system.

EXPLICIT VALIDATION OF AN ECDSA PUBLIC KEY:

INPUT: A public key h PCC associated through suitable domain parameters (P(

OUTPUT: approval or elimination of the cloud user along with verification of public key .

1. Confirm that .
2. Also verify that 7Ê and =Ê are appropriately stand for fundamentals of .'
3. Confirm that presents within elliptic curve definite through and
4. Confirm that .
5. If it becomes failure then select cloud user is not a valid user ; otherwise selected user cloud user is valid user.

F. Batch Auditing

Sometimes, a public verifier might require verifying the suitability of manifold auditing tasks in an extremely small instance. Straightforwardly authenticate these manifold auditing tasks independently would be ineffective. By leveraging the characteristic of the bilinear maps, extend this presents ECCDSA to support group auditing mechanism, which be able to confirm the suitability of manifold auditing tasks concurrently and develop the efficiency of public auditing.

IV. EXPERIMENTATION WORK

In this section, to measure the public auditing results for proposed ECCDSA and Oruta privacy preserving auditing mechanism by using the communication cost and computation time parameters . In our experiments, proposed ECCDSA based privacy preservation public auditing mechanism is implemented in .net language with different number of cloud user are created and information is shared from one user to another cloud user with a base field size of 159 bits based file size , which has a perform better than existing oruta privacy preservation auditing mechanism on cloud computing environment.

4.1. Computation Cost

During a batch auditing task, the public verifier create a number of keys for each cloud data owner with randomly generation of prime numbers to build an assessment challenge, which is minimally create a key values with less key generation time for each cloud user in cloud computing environment . As shown in Figure 2 when d number of the user in the group is fixed in cloud computing environment which is implemented in JAVA environment. Key generation time for ECCDSA in the cloud computing environment is less when compare to existing Oruta public key based data auditing mechanism. Particularly, when d =15 a user in the group requires concerning 24 milliseconds less to calculate a digital signature to each cloud user information sharing between one to another cloud user.

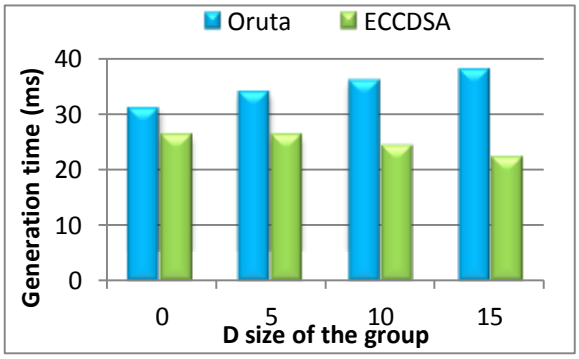

Figure 2. Generation time for cloud user vs methods

4.2. Communication cost

During a batch auditing task, the public verifier create a number of keys for each cloud data owner with randomly generation of prime numbers to build an assessment challenge, which is minimally create a key values with less key generation time for each cloud user in cloud computing environment in JAVA platform, it shows that the proposed ECCDSA methods have consumes less cost when compare to existing methods for batch auditing public task results which is experimented and shown in Figure 3.

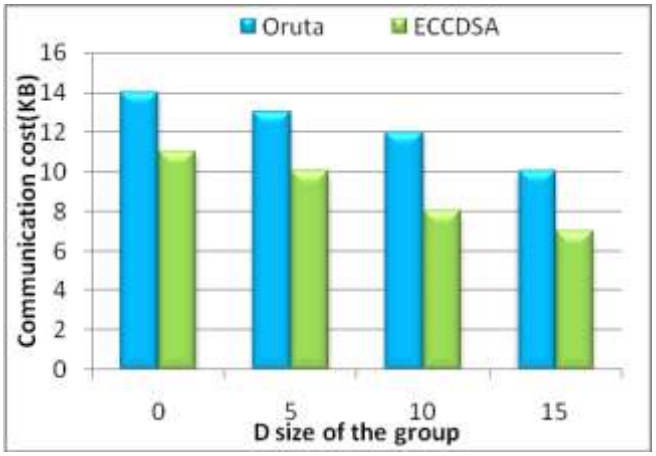

Figure 3. Communication cost for cloud user vs methods

The communication cost of proposed ECCDSA public data auditing task under when d =10 a user in the group is presented in cloud computing environment which is implemented in JAVA environment and shown in Figure 4. Compared to the size of d =10 a user in the group the shared information, communication cost in an manifold data auditing task is extremely small for proposed ECCDSA when compared with existing Oruta methods.

V. CONCLUSION AND FUTURE WORK

In this paper, propose a novel elliptic curve cryptography based digital signature based privacy preservation public data auditing schema for cloud information during the sharing process one cloud user to another cloud user in any organization without leaking of confidential information from cloud storage information .Proposed ECCDSA create a digital signature to each cloud data owner for data truthfulness ,consequently with the aim of a public verification process was proficient to assessment of shared information from one cloud data owner to another data owner to differentiate each signer in the cloud computing environment . In order to enhance the efficiency of the proposed ECCDSA manifold auditing information tasks is further expanded to support batch auditing task. The experimentation results of the proposed ECCDSA also perform to manifold data auditing task and performance analysis shows that the proposed ECCDSA system is together protected and well-organized for cloud storage space information system for auditing task than the Oruta and existing methods . The following interesting directions are expanded to our current study and solve existing issues. The present propose may not sustain traceability. Another difficulty intended for our potential work is how to confirm information originality.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, 2012, pp. 69-73.

[2] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, 2012, pp. 39-45.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, 2010. pp. 525-533.

[4] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), 2013, pp. 90-99.

[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, 2010, pp. 50-58.

[6] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Applied Cryptography and Network Security, Springer, 2008, pp. 111–129.

[7] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 195– 203.

[8] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT 2011, pp. 568–588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM, 2010, pp. 1–9.

[10] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 735–737.

[11] J. Liu, Z. Wan, and M. Gu, "Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing," Information Security Practice and Experience, 2011,pp. 98–107.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 261– 270.

[13] The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS 2007), pp. 598-610.

[15] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transaction Services Computing, 2013, pp. 2904-2912.

[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 557–557, 2005.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, 2006, pp. 89–98.

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

[19] J. Kubiatowicz, D. Bindel, Y. Chen, S. Czerwinski, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, C. Wells, and B. Zhao, "Oceanstore: an architecture for global-scale persistent storage," SIGOPS Oper. Syst. Rev., vol. 34, 200,pp. 190– 201.

[20] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in Trust and Trustworthy Computing, A. Acquisti, S. Smith, and A.-R. Sadeghi, Eds. Springer Heidelberg, 2010, vol. 6101, pp. 417–429.

[21] S. Pearson, Y. Shen, and M. Mowbray, A privacy manager for cloud computing, in Cloud Computing. Springer Berlin / Heidelberg, 2009, pp. 90–106.

[22] M. Mowbray, S. Pearson, and Y. Shen, Enhancing privacy in cloud computing via policy-based obfuscation, Springer eidelberg, 2010, pp. 1–25.

[23] S. Blake-Wilson and A. Menezes, Unknown key-share attacks on the station-to-station (STS) protocol, Public Key Cryptography – Proceedings of PKC '99, Lecture Notes in Computer Science, 1560 (1999), 154-170.