DOI: http://dx.doi.org/10.26483/ijarcs.v11i5.6659

ISSN No. 0976-5697

Volume 11, No. 5, September-October 2020

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A STUDY ON THE EXISTING THRESHOLD CRYPTOGRAPHY TECHNIQUES

Prabha Elizabeth Varghese
Department Of Computer Science
School of Engineering, CUSAT
Kerala, India

Latha R Nair
Department Of Computer Science
School of Engineering, CUSAT
Kerala, India

Abstract: Threshold cryptography in simple words is the art of splitting a secret into many bits. The secret can be recreated only by possessing more than a threshold number of bits of the secret. The information is first encrypted and distributed among a cluster of fault tolerant computers. Encryption is done using a public key and the participating parties possess the corresponding private key. Thus for asymmetric key cryptography, threshold versions of encryptions can be built. In this paper we explore the various extensions and techniques of threshold cryptography.

Keywords: threshold cryptography; secret sharing scheme; distributed key generation; distributed encryption; dynamic threshold scheme

I. Introduction

The first approach that comes to our mind when it comes to protecting information or data is protecting it using a password. When we have a lot of password protected data, it becomes very difficult to remember the passwords. Some of the secrets are too confidential or important to be kept only by one person. For storing very important and highly sensitive information, secret sharing schemes are ideal. Care must be taken that each of these information is kept safe without getting lost and is kept confidential. In a traditional secret sharing scheme, the secret is distributed amongst a group of participants, Each participant is allocated a share of the secret. To reconstruct the secret, the shares are to be combined together. An individual share on its own does not make any sense. Traditional methods fail to achieve reliability and confidentiality at the same time. Storing multiple copies puts confidentiality factor at stake. This problem can be addressed by using secret sharing schemes where reliability and confidentiality can be achieved. In this paper the authors have explored various threshold cryptographic schemes.

In a threshold cryptographic scheme, the private key is shared among a set of receivers so that the message can be decrypted by only authorized sets of users. Key is generated jointly by all participants. Ideally the encryption protocol is hidden from the sender. The cipher text can be decrypted by an authorized set without explicitly reconstructing the private key. Thus without reconstructing the private key, a group of participating processes or parties can perform security operations such as encryption, decryption, signature generation and verification. It enhances the security of highly sensitive keys and the availability of the systems. The main applications of threshold cryptography are in public key encryption and signature schemes. Crypto currencies make use of the concept of threshold cryptography

A simple distributed signature generation is depicted here,

Let *sk* be the secret key, *m* be the message then signature can be computed as m^{sk}

$Sk = sk_1+sk_2+sk_3$ where the key is divided among 3 parties.

The server publishes m^{ski}

$$m^{sk1}\, m^{sk2}\, m^{sk3} = m^{sk1+sk2\ +sk3} = m^{sk}$$

This scheme can be modified to enable a subset to generate a signature. This thought is the backbone of threshold cryptography.

II. Literature Review

Probably the first mention of the problems of having the power to sign a digital document being vested on one entity was brought up by Shamir[1]. His suggestion was to distribute shares of a secret as evaluations of a polynomial. The data is divided into n pieces and only k < n pieces are needed to reconstruct the data. k becomes the threshold value if knowledge about k-1 pieces do not let the message to be reconstructed. Here this approach is robust against partial errors. However loopholes like leaking the master key, signing unintended messages or modifying the messages being signed by the signature generating device were possible.[20]

Verifiable secret sharing (VSS) protocol is introduced by Chor et al. [2] which allows the players to verify that their shares are consistent. This protocol consists of two phases: a sharing phase and a reconstruction phase. In the sharing phase, the dealer holds the secret as input and each player holds an independent random input. It may consist of several rounds. At each round, the messages can be sent privately or it can be broadcast to other players. Messages from other players received in previous rounds along with its random input forms the input for the next message. In the reconstruction phase, each player provides its entire view from the sharing phase and a reconstruction function is applied and is taken as the output. A secret message is selected and encrypted by a distinguished dealer or processor and each processor *n* gets a share of *s*. There exist parameters *t*, *u* such that *s* cannot be recovered by that processors while it is guaranteed that *s* can be easily computed by any set of *u* processors.

t becomes the threshold when *u*=*t*+1

Unlike the previous schemes which were interactive, P. Feldman[3] introduced the concept of non-interactive VSS where a share proves its own validity. This idea was used to construct the distributed key generation protocol (DKG) protocol by Predersen[4]. To initialize the cryptosystem and generate its private and public keys, this protocol can be used. It is also used as a sub protocol. A pair of public and private keys are jointly generated by a set of n servers/players in such a way that using a threshold secret sharing scheme the private key is shared by the n servers while the public key is published to all. Unless more than a specified threshold number of players are compromised, the generated private key remains secret and its secret-sharing can be subsequently used by these servers to jointly compute signatures or decryptions. In discrete–log based threshold schemes, the distributed key generation protocol is used to generate the random value *x* and the public value y = g^x. Feldman's protocol is run in parallel by each participant in a group. An additional round of communication was required here as generators g and h were selected randomly so that the players were unaware of the relation between them. A completely distributed VSS-based DKG was developed by Pedersen [5] where a variation of Feldman's VSS with commitment function and digital signatures is run on each node. A combined shared secret is generated by adding distributed shares at the last.

Gennaro et al. [6] presented the Joint Feldman DKG (JF-DKG) using original Feldman's VSS. In this paper it was pointed out that additional security to Pedersen's DKG was not provided by the use of digital signatures and a commitment function.

Gennaro et al. [7] presented that at the cost of an increased security parameter despite the biased distribution of the key, certain discrete-log schemes that make use of Pedersen DKG can be proven to be secure. The threshold cryptosystem was found to be secure when Pedersen's DKG is substituted by the DKG protocol of Gennaro et al.

Canetti et al. [8] provided adaptively secure solutions for distributed key generation in discrete log based cryptosystems and for the problem of distributed generation of DSS signatures. Fully specific, concrete, fully analyzed solutions to some of the key problems in threshold cryptography were also provided. Interactive knowledge proofs and erasures were used. To make the protocol secure against adaptive adversaries, before public values are broadcast or commitments, private data of the participants were erased in the key construction phase of the DKG. The number of parties in the system, input length or the security parameters are not dependent on the number of rounds of communication which is fixed.

Frankel et al. [9] presented comparable adaptively secure threshold schemes. One of the fundamental issues in cryptography is providing security of cryptographic protocols against adaptive adversaries. RSA-based and distributed discrete-log-based public-key systems are made secure against an adaptive adversary. Proactive security is also assured for discrete-log-based systems in this approach.

Jarecki and Lysyanskaya [10] proposed an approach that is secure in a concurrent setting. The concept of committed proof was introduced here. An encryption scheme that is non-committing to the receiver was used to implement the secure channels without erasures. Two new threshold security schemes were suggested namely security without the assumption of reliable erasure and security under concurrent composition. In erasure-free adaptive model, for special class of protocols, the techniques proposed here include the first efficient implementation of secure channels.

Abe and Fehr [11] proposed the first distributed discrete-log key generation (DLKG) protocol which in the non-erasure model is adaptively-secure that does not use the interactive rewinding zero-knowledge proofs. In a universally-composable (UC) like framework that prohibits rewinding, this protocol can be proven secure. In the inconsistent-player (SIP) UC model, security was proven. Arbitrary composition was guaranteed if the same players execute all protocols. This scheme does not require secure erasure, secure communication, and a linear number of rounds or digital signatures to resolve disputes. However some restriction on the corruption behavior of the adversary is required. A secure message transmission functionality and a single inconsistent player is needed.

Stadler [12] proposed a publicly verifiable secret sharing (PVSS) protocol. In a PVSS scheme, to resist malicious players, verification that the participants received correct shares can be done by anybody irrespective of whether they are a participant or not. In encrypted form shares were broadcast and a proof of equality of (double) discrete logarithms was used to verify this. Initialization process in PVSS scheme includes generation of all system parameters and ensuring that each participant has a registered public key. Apart from the initialization process, the PVSS also consists of distribution of secret shares, verification, decryption and pooling of the shares.

Fujisaki and Okamoto [13] presented a protocol that is secure under a modified RSA assumption. Another protocol was proposed by Schoenmakers [13] which is secure under Decisional Diffie-Hellman (DDH) assumption. In the exponent of each player's individual public key, the encrypted form of the shares are hidden and they are broadcast. Non-interactive proofs of discrete-log equality is used by the dealer. Additional proofs of correctness is provided in the secret reconstruction phase to verify the correct behavior of the players. Heidarvand and Villar [14] used bilinear pairing to attain verifiability.

III. VARIOUS PERSPECTIVES OF THRESHOLD CRYPTOGRAPHY

In Multi-Key Leakage-Resilient Threshold Cryptography [15] security is guaranteed under various key-exposure attacks. In many leakage-resilient non-threshold cryptosystems, the leakage function is always applied to the only one available secret key. In some advanced encryption primitives, such as leakage-resilient identity-based encryption (IBE), leakage of more than one keys may be allowed. The leakage of both kinds of key at the same time are not modelled in most of them. In the multi-key leakage-resilient model, security of dynamic threshold public key encryption and threshold ring signature is demonstrated.

In Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting [16] a distributed RSA composite is generated by protecting its factorization's leakage and a distributed decryption for Paillier. It is fully simulatable. In a two-party malicious setting, it is the first RSA key generation and Paillier threshold scheme. The extension of the protocol to a multiparty setting with dishonest majority is also described.

In RSA key generation protocol, an RSA composite is generated using a distributed sub protocol. The generated composite is verified through a bi-primality test. For the public key, Paillier threshold encryption scheme uses the RSA composite. It comprises of a sub protocol for the distributed generation of the corresponding secret key shares and another subprotocol for the distributed decryption for decrypting according to Paillier.

Dealer-free Dynamic Threshold Schemes [17] is secure in the setting of a passive adversarial coalition. Two methods, termed public evaluation (for threshold reduction) and zero addition (for threshold increase) that can be used in both the passive and active adversarial setting are also discussed here. New secrets are dynamically generated in the absence of the dealer.

In Composite Trust Based Threshold cryptography Key Management for Mobile Ad hoc Network [18] a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust is proposed. Performance parameters like efficiency, service availability etc. is maximized while the risk of security vulnerability is mitigated.

CTPKM enables a node to make decisions in interacting with others based on their trust levels considering three different trust dimensions, namely, competence, integrity, and social contact.

A summary of the various approaches discussed and its advantages are shown in Table 1.

Table I. Various Threshold Cryptographic Approaches

THRESHOLD CRYPTOGRAPHY APPROACH	***ADVANTAGES***
Multi-Key Leakage-Resilient Threshold Cryptography	- Throughout the life time of the key an overall unbounded leakage is offered. - Allows periodic updates on the secret key while bounding the leakage between updates when extended with the continual leakage model.
Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting	- In the two party setting, security against malicious software is achievable
On Dealer-free Dynamic Threshold Schemes	- The problem of most of the secret sharing schemes being 'one-time' is overcome here.
Composite Trust Based Threshold cryptography Key Management for Mobile Ad hoc Network	- Minimizes communication overhead incurred by the key management operations. - A certificate authority is not mandatory for its operation. -Withstands misbehaving nodes to an extent. - Dynamically switches to a distributed scheme of trust. from a centralized one.

IV. Conclusion

In threshold cryptography, a secret is split into many shares that are distributed among the participating parties. This approach can effectively reduce the total number of secret keys used and thus has proven very effective for key management and signatures. Threshold cryptography was explored and various approaches for it was discussed. According to the application requirement, the technique suitable can be chosen. Each technique we discussed in this paper has its own advantages and disadvantages and are used depending upon the parameters we can compromise according to the application

V. References

[1] A. Shamir. How to share a secret. Commun. ACM, 22, pp. 612-613, November 1979.

[2] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults, FOCS85, pp. 383-395.

[3] P. Feldman., A practical scheme for non-interactive variable secret sharing, 28th Annual Symposium on Foundations of Computer Science, pp. 427437. IEEE Computer Society, 1987.

[4] T. P. Pedersen. A threshold cryptosystem without a trusted party. Advances in Cryptology EUROCRYPT '91, volume 547, pages 522-526. Springer-Verlag, 1991.

[5] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. Advances in Cryptology CRYPTO '91, volume 576 of Lecture Notes in Computer Science, pages 129-140. Springer-Verlag, 1992.

[6] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure Applications of Pede“rsenDistributed Key Generation Protocol. In CT-RSA, pages 373–390, 2003.

[7] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. Advances in Cryptology EUROCRYPT '99, volume 1592 of Lecture Notes in Computer Science, pages 295-310.Springer-Verlag, 1999.

[8] R Canetti, R Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Adaptive Security for Threshold Cryptosystems. Advances in Cryptology-CRYPTO’99,pp 9-116

[9] Y. Desmedt. Society and group oriented cryptography : a new concept. Advances in Cryptology, Proc. of Crypto '87), pp. 120-127. Springer-Verlag, 1988. Santa Barbara, California, U.S.A., August 16-20.

[10] S Jarecki, A Lysyanskaya. Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures, Advances in Cryptology-EUROCRYPT 2000 pp 221-242

[11] M Abe, S Fehr. Perfect NIZK with Adaptive Soundness. Cryptology ePrint Archive: Report 2006/423

[12] M. Stadler. Publicly verifiable secret sharing. Advances in Cryptology-EUROCRYPT '96, pp. 190-199. Springer-Verlag, 1996.

[13] E. Fujisaki and T. Okamoto. A practical and provably secure scheme for publicly variable secret sharing and its applications. Advances in Cryptology EUROCRYPT '98, pp. 32-46. Springer-Verlag,1998.

[14] S. Heidarvand and J. L. Villar. Public verifiability from pairings in secret sharing schemes. Selected Areas in Cryptography , SAC 2008, pp. 294-308. Springer, 2009.

[15] Cong Zhang, Tsz Hon Yuen,HaoXiong, Sherman S. M. Chow, Siu Ming Yiu, Yi-Jun He, “Multi-Key Leakage-Resilient Threshold Cryptography” in ASIA CC“S13 Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pp. 61-70,2009

[16] Carmit Hazay, Gert Læssøe Mikkelsen, Tal Rabin, Tomas Toft, “Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting” in The Cryptographers“ Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 – March 2, 2012. Proceedings, pp 313-331, 2012

[17] Nojoumian, Mehrdad, and Douglas R. Stinson. "On Dealer-free Dynamic Threshold Schemes."

[18] Cho, Jin-Hee, Kevin S. Chan, Ing-Ray Chen, "Composite trust-based public key management in mobile ad hoc networks." in Proceedings of the 28th Annual ACM

Symposium on Applied Computing, pp. 1949-1956.ACM, 2013.

[19] H Dahshan and James Irvine, "On demand self-organized public key management for mobile ad hoc network," in IEEE 69th Vehicular Technology Conference: VTC2009-Spring, 2009.

[20] Ravleen Kaur, Pragya Kashmira, Kanak Meena, Dr. A.K.Mohapatra, "Survey on Different Techniques of Threshold Cryptography," in IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) pp. 114-119