IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 114-119
www.iosrjournals.org

Survey on Different Techniques of Threshold Cryptography

Ravleen Kaur[1], Pragya Kashmira[2], Kanak Meena [3], Dr. A.K.Mohapatra[4]
[1](Department of Information Technology, Indira Gandhi Delhi Technical University for Women, India)
[2](Department of Computer Science, NIT Delhi, India)
[3](Department of Information Technology, Indira Gandhi Delhi Technical University for Women, India)
[4](Department of Information Technology, Indira Gandhi Delhi Technical University for Women, India)

ABSTRACT : *Threshold cryptography protects information by distributing the key among several servers instead of giving it to just a single server. Hence, in order to decrypt a message, a single server's key wouldn't work. Generally, a threshold number of servers' keys are required to co-operate for decryption to be performed. Threshold cryptography has, thus, been proved to be an effective technique for key distribution and decryption. In our paper, we discuss various techniques to implement threshold cryptography effectively in real life scenarios.*

Keywords *- Dynamic Threshold Schemes, Efficient RSA Key Generation and Threshold Paillier, File Transfer Service, Mobile Ad hoc Network, Multi-Key Leakage-resilient, Password based cryptography*

I. INTRODUCTION

Paper media has been drastically replaced by electronic media in the last 30 years. As the use of electronic media is increasing for exchange of information, so is the risk of the act of eavesdropping. Today, an eavesdropper has an increased amount and variety of information available, making the act of eavesdropping much easier. This has led to an increase in interest in private and commercial cryptography, taking the realm of cryptography to a whole new level.

In cryptography, the given data is processed into unintelligible form such that the original data can be retrieved using the obtained form without any loss of data in the process.

Traditional cryptography includes only one party in order to encrypt a message and a single party in order to decrypt it which renders it insecure as a single key can easily be stolen or misused. In real case scenarios, a given server cannot always be trusted, but we can assume that a majority of servers are trustworthy. Threshold cryptography has been developed based on this assumption. In threshold cryptography, the secret key is fault tolerantly broken into several bits. Only by possessing more than a threshold number of bits of the secret key can the secret be determined. Thus, threshold cryptography requires that many systems must be compromised prior to decryption of a secret. This paper is intended to study some popular techniques used to implement threshold cryptography in the real world. If the threshold cryptography is used via efficient protocols, it comes out to be the most secure cryptosystem and signature scheme. The concept of threshold cryptography is used in different applications, with some changes according to the requirement of the application.

The next section explores the work done in this field incorporating the changes done so far starting with the basic concept of cryptography. This section describes the changes done in the original concept of cryptography after the improvements done by various researchers, leading to the concept of threshold cryptography as we know it today. The third section discusses various versions of encryption schemes. In other words, the existing encryption schemes are altered in order to be able to incorporate the features of threshold cryptography. This is followed in Section IV by discussing various techniques used to implement threshold cryptography effectively in real world. In order to make threshold cryptography effective for different cases, it is implemented after making some required changes according to the application.

The last section covers the results concluded from this paper.

II. RELATED WORK

Shamir [1] was the first to discuss that a company's secret key, used to digitally sign documents, should not be given to a single entity. Shamir's (k, n) threshold scheme problem statement is given as:

"Divide data D into n pieces D1,..., in such a way that:

(1) Knowledge of any k or more Di pieces makes D easily computable;

(2) Knowledge of any k - 1 or fewer Di pieces leaves D completely undetermined (in the sense that all its possible values are equally likely)."

Shamir's early idea of distributing shares of a secret as evaluations of a polynomial has become a standard building block in threshold cryptography. The solution suffers from many problems, the signature generating device can: Leak the master key, modify the message being signed (indeed the co-signers have no control over the message that is allegedly being signed), and sign extra messages.

So, full trust is necessary on the manufacturer of the device and the one who operates it. Thus, this solution is not very secure. The fact that sometimes a cipher text needs to be decrypted jointly by a group of users, instead of by a single user, was addressed by R. A. Croft and S. P. Harris in 1986 [2] and later by Y. Desmedt in 1987 [3].

The first solution presented was not very secure and the second one was far from practical since it relies on mental games (general secure distributed computation) mechanisms.

Feldman [4] introduced verifiable secret sharing (VSS) by publishing the coefficients of the polynomial hidden in the exponent of the generator of a group in which the discrete-log assumption holds.

" VSS is a protocol in which a distinguished processor or dealer selects and encrypts a "secret message", s, and gives a "share" of s to each of n processors. There exist parameters t, u such that no t processors can recover s, but any set of u processor are guaranteed that they can easily compute s. When, u=t+1, we say that t is threshold. The efficiency of a VSS protocol is measured by other protocols as well:

1. The number of rounds of communication required
2. The number of bits which must be communicated between processors
3. The number of computations the processors must do."

Another important characteristic is the way in which the processors are guaranteed that they can recover the secret from their shares. All the previous schemes have been interactive; the validity of a share is proven by an interactive protocol. But P. Feldman introduced the concept of a non-interactive VSS, in which a share "proves its own validity". This widens the applicability of VSS to scenarios in which interaction is infeasible, such as sharing a key in entire country.

VSS was first introduced by Chor, Goldwasser, Micali and Awerbuch [5], but the scheme was based on interactive VSS. Feldman contributed the first non-interactive VSS protocol

Predersen [6] then used this idea to construct the first distributed key generation (DKG) protocol, sometimes also referred to as Joint Feldman, by having each player in a group run an instance of Feldman's protocol in parallel. But it can't achieve the unconditional security for the secret. Further, Pedersen's scheme also has the requirement of the random selection of generators g and h such that no player should know the relation between them; adding an additional round of communication. Therefore, with its simplicity, and efficiency, This VSS scheme by Feldman forms the basis for most of the VSS-based DKG systems in the literature and for the one in this paper, as well.

Soon thereafter, Pedersen [7] produced another remarkable result. He made Feldman's VSS scheme information-theoretically secure by choosing two polynomials and broadcasting the corresponding coefficients as paired commitments, which are known as Pedersen commitments. Pedersen next developed a completely distributed VSS-based DKG [7]. In this scheme, each node runs a variation on Feldman's VSS (with digital signatures and a commitment function) and distributed shares are at last added generating a combined shared secret.

Gennaro et al. [8] made an observation that use of digital signatures and a commitment function does not provide any additional security to Pedersen's DKG and thus, presented a simplification using just original Feldman's VSS called the Joint Feldman DKG (JF-DKG) with the claim that these DKGs do not guarantee a uniformly random distribution of secret keys generated.

In Secure Applications of Pedersen's Distributed Key Generation Protocol [9], the same set of authors proved the security of JF-DKG against a static adversary, when it is used with a provably secure Schnorr signature scheme. They showed that an adversary who compromises even two out of n servers can skew the distribution of the generated secret key. While it is not clear if the adversary can control the distribution of the private key in a way that help shim break the cryptosystem that uses this key, the adversary's ability to skew this distribution from uniform means that the above security reduction argument does not hold.

Interestingly, Gennaro et al. showed later [10] that, despite the biased distribution of the key, certain discrete-log schemes that use Pedersen DKG can still be proved secure at the cost of an increased security parameter. When the DKG protocol of Gennaro et al. is substituted for Pedersen's DKG in a threshold cryptosystem whose security proof assumes uniform distribution of the generated secret – which is the case of

all the discrete-log based cryptosystems mentioned above – this substitution renders the threshold cryptosystem provably secure.

Canetti et al. [5] used interactive knowledge proofs and erasures, i.e., players erase private data before commitments or public values are broadcast, in the key construction phase of the DKG of [8] to make the protocol secure against adaptive adversaries. The main contribution of Canetti et al. was in providing concrete, fully specified, fully-analysed solutions to some of the central problems in threshold cryptography, and proving their security in the adaptive adversary model. These solutions add little overhead relative to existing solutions for the same problems in the static adversary model. They are also constant-round; namely, the number of rounds of communication is fixed and independent of the number of parties in the system, the input length, or the security parameters. Thus this protocol was the first to be of real use in emerging threshold cryptography applications. Also, this protocol introduced new techniques for the design and analysis of protocols in the adaptive-adversary model.

Comparable adaptively secure threshold schemes were presented by Frankel et al. [6]. When attacking a distributed protocol, an adaptive adversary is able to determine its actions (e.g., which parties to corrupt) at any time based on its entire view of the protocol including the entire communication history. Proving security of cryptographic protocols against adaptive adversaries is a fundamental problem in cryptography. In this paper, Frankel et al. consider distributed public-key systems which are secure against an adaptive adversary. Specifically, they construct distributed discrete-log-based and RSA-based public-key systems secure against an adaptive adversary. They also extend the discrete-log-based systems to have proactive security, that is, security against an (adaptive) mobile adversary that has an upper bound on the number of servers it may corrupt at any one time, but no upper bound on the number of servers it may corrupt over the lifetime of the system.

In the protocols discussed so far, it is assumed that there are private channels between each pair of players. Both [11] and [12] suggest that these channels can still be established even with an adaptive adversary using the non-committing encryption technique of Beaver and Haber [14], which assumes erasures.

Jarecki and Lysyanskaya [15] pointed out that the protocols presented in [11] and [12] are not secure in the concurrent setting, i.e., two instances of the same scheme cannot be run at the same time. They solved this by introducing a "committed proof", i.e., a zero-knowledge proof where the statement that is being proved is not revealed until the end of the proof. To implement the secure channels without erasures they use an encryption scheme which is non-committing to the receiver. They put forward two new measures of security for threshold schemes secure in the adaptive adversary model: security under concurrent composition; and security without the assumption of reliable erasure. They exhibit efficient secure threshold protocols for a variety of cryptographic applications using novel constructions and analytical tools, in both these settings. They constructed adaptively secure threshold cryptosystems secure against adaptive chosen cipher text attack under the DDH intractability assumption in particular. These techniques are also applicable to other cryptosystems and signature schemes, like RSA, DSS, and ElGamal. These techniques include the first efficient implementation of secure channels in erasure-free adaptive model for a wide but special class of protocols.

Abe and Fehr [16] later proposed an adaptively-secure (Feldman-based) DKG and applications with complete security proofs in the Universal Composability framework of Canetti [17]. They propose the first distributed discrete-log key generation (DLKG) protocol which is adaptively-secure in the non-erasure model as well as completely avoids the use of interactive zero-knowledge proofs. The protocol can be proven secure in a universally-composable (UC) like framework which prohibits rewinding. They proved the security in the single-inconsistent-player (SIP) UC model, as a result guaranteeing arbitrary composition as long as all protocols are executed by the same players. Their results are based on adaptively-secure Feldman VSS scheme. Although adaptive security was already addressed by Feldman in the original paper, but the scheme by Feldman requires secure communication, secure erasure, and either a linear number of rounds or digital signatures to resolve disputes. This scheme overcomes all of these shortcomings. But this scheme also requires some restriction on the corruption behaviour of the adversary, which however disappears in some applications including DLKG protocol. However, they still need a single inconsistent player and a secure message transmission functionality (private channels), but that can be realised using a receiver non-committing transmission protocol.

As a consequence of private channels, each of the aforementioned DKG protocols has some kind of complaint procedure or dispute resolution mechanism. To get rid of these, several authors have proposed protocols that provide public verifiability.

Stadler [10] was of the first to propose a publicly verifiable secret sharing (PVSS) protocol. In addition to the Feldman commitments, shares were broadcast in encrypted form and verified using a proof of equality of (double) discrete logarithms. A secret sharing scheme shares a secret among several participants in a manner

only certain groups of them can recover it. To achieve security against cheating participants, verifiable secret sharing has been proposed. It had the special property that everybody can verify that the shares are correctly distributed and not only the participants. Such schemes are called publicly verifiable secret sharing schemes.

The PVSS scheme initialization process includes:
1. Generating all system parameters.
2. Ensuring each participant has a registered public key.

Excluding the initialization process, the PVSS consists of two phases:
1. Distribution of secret s shares is performed by the dealer D
2. Decryption and pooling of the shares

A more efficient protocol was presented by Fujisaki and Okamoto [14], which is secure under a modified RSA assumption.

The first PVSS shown secure under the Decisional Diffie-Hellman (DDH) assumption was given by Schoenmakers [20]. The shares are broadcast in encrypted form by hiding them in the exponent of each player's individual public key, which has a different base (another generator) than the Feldman commitments. The dealer then uses non-interactive proofs of discrete-log equality. Furthermore, correct behaviour of the players is verified by extending the secret reconstruction phase with additional proofs of correctness. It is improved from both Stadler and Fujisaki and Okamoto both in terms of efficiency and in the type of intractability assumptions.

Based on Schoenmakers' result Heidarvand and Villar [12] presented the first PVSS protocol where verifiability is obtained from bilinear pairing.

The first full DKG that does not require private channels was given by Fouque and Stern [13]. The idea behind their construction is the Paillier cryptosystem and a new non-interactive zero-knowledge proof. To deal with a rushing adversary it is simply assumed that communication is completely synchronous. For participants not present during the DKG the amount of information that needs to be stored, i.e., the subshares that need to be decrypted, is linear in the number of participants that are active in the DKG.

III. DIFFERENT APPROACHES OF THRESHOLD CRYPTOGRAPHY

3.1. Multi-Key Leakage-Resilient Threshold Cryptography

In this scheme, attacks due to the exposure of key can be prevented and hence, security is promised. [14]

Advantages:
1. It offers an overall unbounded leakage throughout the life time of the key.
2. The multi-key leakage-resilient threshold when extended with the continual leakage model allows periodic updates on the secret key while bounding the leakage between updates.

Applications: It is suitable for systems where long-term secure storage on leaky hardware is required.

3.2. Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting

This construction [15] generates a distributed RSA composite by protecting its factorization's leakage and a distributed decryption for Paillier.

Advantages: Security against malicious software is achievable in the two party setting by this scheme.

Applications:

It can be readily used for evaluating functions of specific interests securely such as the common reference string model (CRS) in generic form or set interactions, pseudorandom functions, etc.

3.3. On Demand Self-Organized Public Key Management for Mobile Ad hoc Network

This scheme [16] exploits an on demand distance vector routing protocol infrastructure to discover a certificate chain through a web of trust. Authentication of the key management is enhanced since trust values are used with the public key certificates.

Advantages:

This scheme has low communication cost and negligible impact on network performance.
It is robust in both dynamic and static networks.
It prevents network against malicious node attacks.

Applications:

This scheme finds its application for stationery networks.

3.4. Doubly Encrypted Identity-Based Encryption

In this approach [17], an encryption scheme is used which encrypts a message doubly. By using this scheme, the decryption right is distributed to three servers, and only the receiver can decrypt ciphertext.

Advantages:

There is no need to maintain public key certificates and to communicate preliminarily to get public keys.
The Private Key Generator (PKG) provides complete trust at the decryption end.

Applications: This scheme finds its greatest use is in the file transfer service.

3.5. Multi-instance Security and Its Application to Password-Based Cryptography

Mi-security [18] is used in systems where a single instance can be compromised and a second line of defence is provided, aiming to ensure that the effort to compromise all of some large number m of instances grows linearly with m.

Advantages: Mi security is potentially much higher than the traditional single-instance (si) security.

Applications: It finds its application in password-based cryptography by using the process of salting.

3.6. On Dealer-free Dynamic Threshold Schemes

This scheme [19] aims at dynamically generating new secrets in the absence of the dealer. At the same time, it does the increasing or decreasing of the threshold and performs changes in the secret from time to time.

Advantages:

It overcomes the problem of almost all secret sharing schemes of being 'one-time', i.e. knowing of the secret and shares to all after the public secret recovery process.

Applications:

It finds its use in systems where frequent changes in the threshold and secret are required at multiple times.

3.7. Composite Trust Based Threshold cryptography Key Management for Mobile Ad hoc Network

This scheme [20] uses an optimal trust threshold that can best balance and meet the conflicting goals between performance and security, exploiting the inherent trade off between trust and risk.

Advantages:

It is efficient in minimizing communication overhead incurred by the key management operations.
It can be operated with and without the existence of the certificate authority.
It is resilient against misbehaving nodes.

Applications:

This scheme is suitable in MANET.

IV. CONCLUSION

Threshold cryptography enhances security by dividing the secret key into several bits. It is a very effective technique for encrypting data as it requires many systems to be compromised prior to taking control of a secret, when the shares of each shareholder are refreshed periodically. It maintains the security by interchanging the shares among its shareholders to prevent unauthorized access. In this paper, we presented the different schemes used for key distribution and key management using threshold cryptography. Each scheme applies its own methods and approaches to provide security measures in different applications. 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

REFERENCES

Journal Papers:

[1] A. Shamir. How to share a secret. Commun. ACM, 22, pp. 612-613, November 1979.
[2] Y. Desmedt. Society and group oriented cryptography : a new concept. In C. Pomerance, editor, Advances in Cryptology, Proc. of Crypto '87), pp. 120-127. Springer-Verlag, 1988. Santa Barbara, California, U.S.A., August 16-20.
[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] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults, FOCS85, pp. 383-395.
[5] T. P. Pedersen. A threshold cryptosystem without a trusted party (extended abstract) in D. W. Davies, editor, Advances in Cryptology EUROCRYPT '91, volume 547, pages 522-526. Springer-Verlag, 1991.
[6] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, Advances in Cryptology CRYPTO '91, volume 576 of Lecture Notes in Computer Science, pages 129-140. Springer-Verlag, 1992.
[7] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. In J. Stern, editor, Advances in Cryptology EUROCRYPT '99, volume 1592 of Lecture Notes in Computer Science, pages 295-310.Springer-Verlag, 1999.
[8] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure Applications of Pedersen's Distributed Key Generation Protocol. In CT-RSA, pages 373–390, 2003.
[9] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure applications of pedersen's distributed key generation protocol. In M. Joye, editor, Topics in Cryptology - CT-RSA 2003,volume 2612 of Lecture Notes in Computer Science, pages 373-390. Springer, 2003.
[10] M. Stadler. Publicly verifiable secret sharing. In U.M. Maurer, editor, Advances in Cryptology-EUROCRYPT '96, pp. 190-199. Springer-Verlag, 1996.
[11] E. Fujisaki and T. Okamoto. A practical and provably secure scheme for publicly veri_ablesecret sharing and its applications. In K. Nyberg, editor, Advances in Cryptology EUROCRYPT '98, pp. 32-46. Springer-Verlag,1998.
[12] B. Schoenmakers. A simple publicly veri_able secret sharing scheme and its application toelectronic voting. In M. J. Wiener, editor, Advances in Cryptology CRYPTO '99, volume1666, pp. 148-164, Springer-Verlag, 1999.
[13] S. Heidarvand and J. L. Villar. Public verifiability from pairings in secret sharing schemes. in R. Avanzi, L. Keliher, and F. Sica, editors, Selected Areas in Cryptography , SAC 2008, pp. 294-308. Springer, 2009.
[14] Cong Zhang, Tsz Hon Yuen,HaoXiong, Sherman S. M. Chow, Siu Ming Yiu, Yi-Jun He, "Multi-Key Leakage-Resilient Threshold Cryptography" in ASIA CCS'13 Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, pp. 61-70,2009
[15] 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
[16] 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.
[17] Makoto Sato, Masami Mohri, Hiroshi Doi, Yoshiaki Shiraishi, "Doubly Encrypted Identity-Based Encryption," in Future Information Technology, Springer, pp 139-144.
[18] MihirBellare, Thomas Ristenpart, Stefano Tessaro, "Multi-Instance Security and its Application to Password-Based Cryptography", Advances in Cryptology – CRYPTO 2012, pp 312-329
[19] Nojoumian, Mehrdad, and Douglas R. Stinson. "On Dealer-free Dynamic Threshold Schemes."
[20] 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.