IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 41-44
www.iosrjournals.org

DKG protocol in hierarchical threshold access structure

Ms. Pratima Popat Gutal
(Computer Department, RSCOE,Pune University, India)

Abstract: *A distributed key generation (DKG) protocol is a central segment in distributed cryptosystems. It permits a gathering of members to mutually produce a pair of keys (private key and public key) without assuming any trusted member. The public key is output in clear but only authorised subgroups of members are able to reconstruct or utilize the private key. Existing study on DKG protocols assumes equal authority for members or participants. In this study, the authors consider the issue of DKG in groups with various levelled structure where the authorised subsets can be characterized by a hierarchical threshold access structure. They first propose an verifiable hierarchical threshold secret sharing protocol. On the premise of this development, they then propose another DKG protocol with with hierarchical threshold access structure for discrete-logarithm-based cryptosystems. It is demonstrated that the proposed protocols fulfill all the security necessities.*
Keywords: *access control, authentication, capability list, threshold, outsourced data, malicious outsiders*

I. Introduction

In this paper, we utilize the combination of threshold cryptography and pairing cryptography in order to design a fully distributed certificate and encryption scheme with simple certificate revocation, participant addition or removal mechanisms not requiring trusted entities for secret sharing. The proposed is an extended adaptation of the work done in (Fournaris, 2012) and uses Certificate-based Encryption (CBE) at its center in an approach to disentangle key administration and denial. To achieve secret sharing without a trusted dealer, we propose a threshold cryptography Distributed Key Generation (DKG) mechanism that we combine with the CBE approach to supply each dCA participant a share of the master secret key without providing any information about the master secret key itself. The proposed dCA is based on bilinear pairing and Elliptic Curve (EC) cryptography as drafted by the most promising related research works. The proposed scheme is capable of certificate issuing in a totally distributed way since the CA master secret key is constructed and distributed with the contribution of all involved participants. Also, the provided certificates and certificate attributes act as private and public key, respectively, for encryption/decryption, thus reducing revocation overhead and avoiding key escrow. The master secret key is not known or stored by any participant. Also, t out of n participants must collaborate in order to use it and issue a CBE certificate following the approach in (Noack & Spitz, 2008; Shao, 2011). The proposed scheme supports easy, efficient participant addition-removal while retaining the issued certificates unchanged and usable. Its performance is very good with minimal requirements of computational intensive operations like bi-linear pairing and EC point multiplication.

II. Literature Survey:

2.1 Certificate-Based Encryption Scheme with No Trusted Entities

Authors: Apostolos P. Fournaris Year: 2013.

Description**:** The distributed paradigm as manifested in distributed networks, calls for a different way from the traditional client-server model for providing Trusted third party (TTP) services to strengthen security. Certificate Authorities (CAs) are among the most common such TTP. Generating certified keys and manage certification information (the basic functionality of a CA) in a fully distributed manner is a key challenge in the distributed IT environment. Current approaches are based on the use of trusted entities within the distributed system that constitute single points of failure and follow complex certificate management and revocation mechanisms capable of hindering their adoption in a large scale. The hardware resources cost of each distributed system member committed to realizing and maintaining such certificate authority system can be high. Furthermore, distributed CA approaches lack flexibility when it come to dynamic member behavior such as dynamic member joining or leaving the system, since they employ complex, computational intensive mechanisms for retaining the CA consistency during such activity. In this paper, we propose the combination of a distributed key generation threshold cryptography scheme along with an efficient secure certificate-based encryption scheme to provide a solution that matches the above problems. The outcome of this proposal is a distributed Threshold Certificate-Based Encryption Scheme that has no need for any centralized trusted entity to create, and split secrets or distribute keys-certificates at any point during its operating cycle. The proposed

scheme has few requirements concerning certificate management due to its inherited Certificate-based Encryption features which enables the scheme's participants to use their certificates as keys and has an easy participant addition-removal mechanism to support dynamic network environments. Extending the work done in (Fournaris, 2012), in this paper the proposed distributed Certificate Authority and encryption/decryption scheme is described and analyzed, participant addition and removal mechanisms as detailed and the scheme's security and performance is discussed. Performance characterization reveals that our scheme is very efficient in terms of computational intensive and resource constraining operations like Elliptic Curve point multiplication and bi-linear pairing.

2.2. Hierarchical Threshold Secret Sharing
Author: Tamir Tassa. Year: 2007.
Description:

Author considered the problem of threshold secret sharing in groups with hierarchical structure. In such settings, the secret is shared among a group of participants that is partitioned into levels. The access structure is then determined by a sequence of threshold requirements: a subset of participants is authorized if it has at least $k0$ members from the highest level, as well as at least $k1 > k0$ members from the two highest levels and so forth. Such problems may occur in settings where the participants differ in their authority or level of confidence and the presence of higher level participants is imperative to allow the recovery of the common secret. Even though secret sharing in hierarchical groups has been studied extensively in the past, none of the existing solutions addresses the simple setting where, say, a bank transfer should be signed by three employees, at least one of whom *must* be a department manager. Presented a perfect secret sharing scheme for this problem that, unlike most secret sharing schemes that are suitable for hierarchical structures, is ideal. As in Shamir's scheme, the secret is represented as the free coefficient of some polynomial. The novelty of our scheme is the usage of polynomial derivatives in order to generate lesser shares for participants of lower levels. Consequently, scheme uses Birkho interpolation, i.e., the construction of a polynomial according to an unstructured set of point and derivative values.

2.3. Efficient Dealer-Less Threshold Sharing of Standard RSA
Author: Maged Hamada Ibrahim Year:2009
Description:

The efficient two-party, two-prime RSA function sharing protocol was proposed. The protocol proves efficiency over previously proposed protocols. When the sharing of standard RSA is considered, the protocol is faster than ever. In this paper, under the assumption that the adversary has eavesdropping and halting capabilities, we propose an efficient extension to the protocol of. The protocol enjoys the following properties. The protocol is fully distributed (i.e. does not require an honest dealer). It is a t-private and t-resilient ($t; n$)-threshold structure against a stationary adversary and also t-proactive ($t; n$)- threshold structure against a mobile adversary, where the number of players $n > 3t$. The players jointly generate two-prime RSA modulus in a number of trials of $O(\text{`}=\lg\text{`})$ since, the protocol avoids the inefficient distributed biprimality test. An extension of the protocol allows the generation of a RSA modulus which is a composite of two safe primes. Distributed primality tests are performed over a public modulus not a shared secret one, which reduces complexity on a per trial basis. We must emphasize that robustness against malicious adversaries (adversaries that masquerade the corrupted player by altering, deleting, sending wrong values, etc.) are beyond the scope of this paper.

2.4. Ideal Perfect Multilevel Threshold Secret Sharing Scheme.
Authors: C. Lin, L. Harn, Dingfeng Year Year:2009
Description:

Shamir proposed the first (t, n) threshold secret sharing scheme. Shamir's scheme is ideal and perfect. In this paper, presented two modifications of Shamir's secret sharing scheme. In first modification, each shareholder keeps both x-coordinate and y-coordinate of a polynomial as private share. In second modification, dealer uses polynomial with degree *larger* than the threshold value t to generate shares for a (t, n) threshold scheme. We show that these two modified schemes are ideal and perfect. Using these two modifications, designed a *multilevel threshold secret sharing schemes* (MTSS). Proved that the proposed scheme is secure.
2.5. Signcryption schemes with threshold unsigncryption, and applications
Authors: J. Herranz, A. Ruiz, G. Sáez. Year:2014

Description: The goal of a signcryption scheme is to achieve the same functionalities as encryption and signature together, but in a more efficient way than encrypting and signing separately. To increase security and reliability in some applications, the unsigncryption phase can be distributed among a group of users, through a *(t, n)*-threshold process. In this work we consider this task of threshold unsigncryption, which has received very fewattention from the cryptographic literature up to now(maybe surprisingly, due to its potential applications). First describe in detail the security requirements that a scheme for such a task should satisfy: existential unforgeability and indistinguishability, under insider chosen message/ciphertext attacks, in a multi-user setting. Then we show that generic constructions of signcryption schemes (by combining encryption and signature schemes) do not offer this level of security in the scenario of threshold unsigncryption. For this reason, we propose two new protocols for threshold unsigncryption, which we prove to be secure, one in the random oracle model and one in the standard model. The two proposed schemes enjoy an additional property that can be very useful. Namely, the unsigncryption protocol can be divided in two phases: a first one where the authenticity of the ciphertext is verified, maybe by a single party; and a second one where the ciphertext is decrypted by a subset of *t* receivers, without using the identity of the sender. As a consequence, the schemes can be used in applications requiring some level of anonymity, such as electronic auctions.

III. Proposed Protocol

The VHTSS protocol is proposed which will be used implicitly to propose a HTDKG protocol.
LetU = {P1, . . . , Pn}.
be the set of participants and D be the dealer.
Then, a VSS protocol is a pair of three phased as follows.

3.1. Sharing verify: In this phase, on input the secret s, D generates the share corresponding to each participant Pi ∈ U and sends it through a secure channel to Pi. The dealer also generates some public information to verify the validity of shares. At the end of this phase, each participant Pi ∈ U is instructed to output a value verificationi ∈ {accept, reject}.

3.2. Reconstruction: The input of this phase is the shares corresponding to a subset of participants. At first, the validity of each share is verified by other participants. Then, if the set of participants with valid shares is an authorised set, the secret can be computed by applying a reconstruction function on the provided shares.

A VSS protocol is called secure if it satisfies the following properties:

(1) Acceptance: If an honest participant outputs 'reject', then all honest participants also output 'reject' at the end of sharing–verify phase. Moreover, if the dealer is not corrupted by the adversary, then all honest participants output 'accept'.

(2) Verifiability/ reconstructability: All subsets of participants containing one authorised subset of participants with valid shares recover the same unique secret σ. With the assumption of honesty of the dealer, we should have σ = s, where s is the original shared secret.

(3) Privacy: If the dealer is not corrupt, then no unauthorised subset of participants is able to obtain any information about the secret.

IV. Conclusion:

The combination of efficient DKG schemes along with pairing-based cryptography schemes such as CBE can lead to a realistic fully distributed DCA and encryption/decryption approach capable of certificate issuing for participant identification attributes that can be used as keys for encryption and decryption. This approach does not need trusted entities and has easy participant addition removal and CBE certificate revocation mechanism. It can also be remarked from the scheme's performance characteristics that as long as the participant number is contained under a reasonable bound (that can be matched by most current distributed network applications, i.e., Ad Hoc networks or MANETs), a strong and efficient security backbone can be achieved offering flexibility, scalability, and robustness. Our future goal is to include dishonourable participant protection in the proposed solution and provide a testing platform security infrastructure for distributed network applications.

References

[1]. Herranz, J., Ruiz, A., Sáez, G.: 'Signcryption schemes with threshold unsigncryption, and applications', Des. Codes Cryptogr., 2014, 70, (3), pp. 1–23
[2]. Budurushi, J., Neumann, S., Olembo, M., et al.: 'Pretty understandable democracy – a secure and understandable internet voting scheme'. Proc. Eighth Int. Conf. on Availability, Reliability and Security (ARES), University of Regensburg, Germany, September 2013, pp. 198–207
[3]. Wang, F., Chang, C.-C., Harn, L.: 'Simulatable and secure certificate-based threshold signature without pairings'. Security and Communication Networks, 2013, 7, (11), pp. 2094–2103.
[4]. Fournaris, A.P.: 'A distributed approach of a threshold certificate-based encryption scheme with no trusted entities', Inf. Secur. J. Glob. Perspect., 2013, 22, (3), pp. 126–139
[5]. Kate, A., Goldberg, I.: 'Distributed key generation for the internet'. Proc. 29th
[6]. IEEE Int. Conf. on Distributed Computing Systems (ICDCS '09), Montreal, Quebec, Canada, June 2009, pp. 119–128
[7]. Boneh, D., Franklin, M.: 'Efficient generation of shared RSA keys'. Proc. Advances in Cryptology (Crypto '97), CA, USA, August 1997, pp. 425–439
[8]. Ibrahim, M.H.: 'Efficient dealer-less threshold sharing of standard RSA', Int. J. Netw. Secur., 2009, 8, (2), pp. 139–150
[9]. Damgrd, I., Mikkelsen, G.: 'Efficient, robust and constant-round distributed RSA key generation'. Proc. Theory of Cryptography, Zurich, Switzerland, February 2010, pp. 183–200
[10]. Brzezniak, B., Hanzlik, L., Kutylowski, M.: 'Attack against Ibrahim's distributed key generation for RSA', Int. J. Netw. Secur., 2013, 15, (4), pp. 313–316
[11]. Simmons, G.J.: 'How to (really) share a secret'. Proc. Advances in Cryptology
[12]. (Crypto '88), CA, USA, August 1988, pp. 390–448
[13]. Brickell, E.F.: 'Some ideal secret sharing schemes'. Proc. Advances in Cryptology (Eurocrypt '89), Houthalen, Belgium, April 1989, pp. 468–475
[14]. Lin, C., Harn, L., Ye, D.: 'Ideal perfect multilevel threshold secret sharing scheme'. Proc. Fifth Int. Conf. on Information Assurance and Security, (IAS '09), Xi'An, China, August 2009, pp. 118–121
[15]. Tassa, T.: 'Hierarchical threshold secret sharing', J. Cryptol., 2007, 20, (2), pp. 237–264
[16]. Tassa, T., Dyn, N.: 'Multipartite secret sharing by bivariate interpolation', J. Cryptol., 2009, 22, (2), pp. 227–258
[17]. Chen, Q., Pei, D., Tang, C., et al.: 'Efficient integer span program for hierarchical threshold access structure', Inf. Process. Lett., 2013, 113, (17), pp. 621–627
[18]. Pakniat, N., Noroozi, M., Eslami, Z.: 'Secret image sharing scheme with hierarchical threshold access structure', J. Vis. Commun. Image Represent., 2014, 25, (5), pp. 1093–1101