Distributed Threshold Certificate based Encryption Scheme with No Trusted Dealer*

Apostolos P. Fournaris
Electrical and Computer Engineering Department,University of Patras, Rion Campus, Patras, Greece

Keywords: Threshold Cryptography, Certificate based Encryption, Elliptic Curve Cryptography, Pairing based Cryptography, Distributed System, Certificate Authority.

Abstract: Generating certified keys and managing certification information in a fully distributed manner can find a wide range of applications in the increasingly distributed IT environment. However, the prohibition of trusted entities within the distributed system and the high complexity certificate management and revocation mechanism, hinder the adoption of this approach in a large scale. Threshold cryptography offers an elegant solution to these issues through Shamir's secret sharing scheme, where a secret (the Certificate Authority's (CA) master key) is split and shared among all participants. Combining this approach with the reasonable certificate service requirements of Certificate based encryption (CBE) schemes could result in a functional and efficient distributed security scheme. However, centralized entities, denoted as trusted dealers, are needed in most threshold cryptography schemes even those few that support CBE, while the static way in which the system's functionality is viewed, considerably limits possible applications (i.e. dynamic environments like p2p, Ad-Hoc networks, MANETS). In this paper, we explore the potentials of combining the latest developments in distributed key generation threshold cryptography schemes with efficient yet highly secure certificate based encryption schemes in order to provide a solution that matches the above concerns. We draft a fully distributed Threshold Certificate Based Encryption Scheme that has no need for any centralized entity at any point during its operating cycle, has few requirements concerning certificate management due to CBE and does not need any trusted dealer to create, and split secrets or distribute certificates. The proposed scheme has an easy participant addition-removal procedure to support dynamic environments.

1 INTRODUCTION

The idea of a Trusted Third party authority (i.e. a Certificate Authority, CA) that is distributed among several different entities, capable of vouching about user credentials, keys (certificates) in a distributed way, offers a high degree of flexibility - scalability and can have many advantages. Since the CA is not restricted to a single machine it cannot constitute a single point of failure. A malfunction of a CA engaged entity won't result in the CA system crash-down. The distributed CA is more secure than a centralized one since an attacker would have to target many entities concurrently to compromise it. This makes the system more resistant to Denial of Service related attacks. Furthermore, since the CA sensitive information, secret keys, are distributed among many entities, even if some of those entities become dishonest, malicious (up to a certain degree) the information as a whole can remain safe, the CA's honesty can be preserved and the corrupted entities can be detected and removed. Since modern trends in IT systems favor the distributed paradigm, the described CA approach can find many real applications. P2p systems, Ad-Hoc networks, MANETS or even Cloud computing and Future Internet applications could greatly favor from such an endeavor.

Distributing the certificate authority's trust to many entities may be achieved either through a "web of trust" (WOT) approach where a number of entities communicate with each other using a trust graph path in a chain-like fashion to sign a requester's public/private key information or through a fully distributed approach where the CA's information is split into shares and send to all involved entities forcing them to collaborate in order to reconstruct these information. The WOT approach, primarily used for privacy purposes, strongly relies on creating, maintain-

*This work is supported by the SECRICOM FP7 European project (contract FP7 SEC 218123)

P. Fournaris A..
Distributed Threshold Certificate based Encryption Scheme with No Trusted Dealer.
DOI: 10.5220/0004075803140320
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 314-320
ISBN: 978-989-8565-24-2

ing and discovering trust paths between a distributed system's participants and cannot easily be applied in a large scale fashion since the path discovery introduces a considerable performance overhead as the number of participants escalates. The path discovery has an unbound latency that is not easily contained. Also, WOT is susceptible to treachery and even one (or a few) dishonest participants can harm the system. The fully distributed approach, based on secret sharing, can solve the above issues since there is no requirement of trusted paths. In this approach, all participants have equal responsibilities to handle secret keys and certificates and the security balance of the system is maintained by following wholly applicable cryptographic rules, following (mostly) threshold cryptography principles. While the performance overhead on the fully distributed approach is not negligible, it is bounded for a given participant number and fits very well to fully distributed systems like p2p and adhoc networks. For this reason, this concept is adopted in our distributed system model and constitute the focus point from this point on in this paper.

A distributed CA (dCA) must be able to issue legitimate certificates of an entity's characteristics, like his identity and his keys (following a specific certificate format) by collaboration of the various entities comprising it. Each dCA's engaged entity (denoted as participant) must hold a share of the dCA secret information which by itself cannot be used to deduce the whole secret. Questions that arise on this aspect is how to generate and distribute such shares and more importantly who is responsible to do this without knowing the whole secret. Furthermore, CAs have a heavy load to handle especially when they service a high number of involved participants since apart form issuing a certificate, a CA is responsible for its management, providing services like certificate reissuing and revocation. Certificate revocation is becoming a very complex problem for CAs since the needed information about revoked certificates are so many that they have a considerably negative impact on the CA efficiency. In the dCA case, this problem can become very potent since revocation information would have to be maintained in more than one places, spare copies of this information should be kept and complex distributed revocation management mechanisms would have to be devised. The last decade, progress in theoretic public key cryptography have provided the means to solve several of the above issues independently.

Identity Based cryptography/encryption (IBE) (Boneh and Franklin, 2001) and its extension to Certificate Based Encryption (CBE) (Gentry, 2003), by offering to the user the tools to utilize his identity (IBE) or his certificate (CBE) as a key, has managed to reduce the role and work load of the centralized CAs, minimizing the need for certificate revocation. The CBE scheme, introduced by Gentry in (Gentry, 2003) combines the advantages of both IBE and tradition Public key Encryption (PKE). As in traditional PKE, each user in CBE generates his own public/private key pair and requests a Certificate from the CA responsible for its generation and information freshness. The issued certificate in CBE has all functionalities of PKE but acts as a partial decryption key. Combining the certificate with his private key, the user can have a fully functional decryption key that is verifiable and legitimate. When the certificate expires or is revoked, the user is compelled to seek a new one because he can no longer decrypt any ciphertext with it. From its introduction in 2003, CBE has been widely studied by many researchers (Boyen, 2008) (Galindo et al., 2008)(Shao, 2011)(Lu and Li, 2009)(Lu, 2011) its security have been enhanced by solving key escrow issues and have reached a strong security status. However, CBE mainly still relies on centralized CAs that have a master secret key capable of signing the issued certificates and constitute a single point of failure.

Threshold cryptography, another branch of modern cryptography, can be very useful in distributing secrets. This approach is based on the work of Shamir (Shamir, 1979), who proposed the concept of (t,n) threshold scheme. Later, Desmedt and Frankel (Desmedt and Frankel, 1989)(Frankel et al., 1997) were among the first to use the idea of Shamir's secret share to design threshold cryptosystems based on ElGamal. Using Shamir's idea, a methodology is developed for splitting a secret into n shares, so that, for a certain threshold $t < n$, any t components-parts of the secret can be combined to reconstruct the secret, whereas any combination of $t-1$ or less shares is incapable of reconstructing the secret. This idea, providing a way to save a secret in a distributed manner, is very attractive to systems where no centralized control is administered and has been used by several researchers to provide strong security potentials to such an environment. However, Shamir's scheme, requires a trusted entity that must generate the secret value, split it into shares and distribute them to all the system's participants. This entity, usually denoted as a trusted dealer, has additional functionality compared to the rest of the system participants and most importantly it needs to be always trusted as well as protected because it has knowledge of the secret. Compromise of the trusted dealer constituted a single point of failure for the distributed system, very much like what a centralized CA would be.

Distributed key generation (DKG) is an obvious application of Threshold cryptography. It allows a set of n entities to generate jointly a pair of public-private key pair according to a distribution defined by the underlying cryptographic concept without ever having to compute, reconstruct or store the secret key in any single location and (ideally) without assuming a trusted dealer. During 1991, Pedersen (Pedersen, 1991) was among the first to present a DKG threshold scheme based on Shamir's idea and the ElGamal cryptosystem and made the first attempt to avoid the need for a trusted dealer. The above work have been complemented by many other publications expanding the DKG scheme functionality (Park and Kurosawa, 1996) (Shoup, 2000) (Gennaro et al., 2001) (Wang, 2003). Of interest is the work of Shoup (Shoup, 2000), where the trusted dealer problem was further addressed. This work was expanded by Damgard et al in (Damgard and Koprowski, 2000) where the trusted dealer was replaced by a honest dealer, with minimal intervention to the system. The above schemes have managed to avoid trusted dealer entities, but have also introduced security (Wang, 2003), (Gennaro et al., 2007) and functionality problems especially when new participants are added or removed to the system. Such operations are either not supported or are very difficult to deal with. Noack et al in (Noack and Spitz, 2008) offer a solution on threshold cryptography key distribution schemes for discrete logarithm systems where no trusted dealer is necessary and participants addition-removal is performed fairly easy. This work was extended in (Fournaris, 2011) to distributed Threshold cryptography certification scheme in order to demonstrate the possibility of such endeavor. However, the certificate revocation problem was not addressed and traditional, already existing, revocation methods where suggested. There has been some attempts to combine Threshold cryptography with CBE, like the work of Libert and Quisquater (Libert and Quisquater, 2003) who discuss the use of Threshold IBE schemes requiring a trusted dealer and the work in (Boneh et al., 2006) that proposed a threshold encryption scheme without random oracles yet still with a trusted dealer or the work of Lu et al (Lu et al., 2009) that adapts the CBE scheme of Galindo et al in (Galindo et al., 2008) to propose a highly secure threshold based CBE scheme with trusted dealer.

In this paper, an attempt is made to design a fully distributed certification and encryption solution that does not suffer from complex certificate revocation, participant addition/removal mechanisms nor requires trusted entities. The notion of a fully distributed Certification - encryption scheme that has no need for special purpose entities in order to issue certificates and use them for encryption/decryption, is introduced. The proposed approach explores the combination of a Threshold cryptography - DKG scheme that has no trusted dealer and a highly secure and efficient CBE scheme based on bilinear pairing and Elliptic Curve cryptography as drafted by the most promising related research works. The proposed scheme is capable of certificate issuing for encryption/decryption in a totally distributed way since the CA master secret key is constructed and distributed with the contribution of all involved participants. This master secret key is not known nor 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 and Spitz, 2008) and (Shao, 2011). The proposed scheme supports easy participant addition-removal while retaining the issued certificates unchanged and usable. System compromise is very difficult as long as less than t participants are susceptible to secret information leakage and behave in a honest way.

The rest of the paper is organized as follows. In section 2 the proposed scheme is presented and analyzed and the scheme's various stages are described. In section 3, participant addition and removal is presented in detail while the mechanism for issuing a new certificate after addition is commented. Finally, section 4 concludes the paper.

2 PROPOSED THRESHOLD CBE SCHEME WITH NO TRUSTED DEALER

The proposed scheme methodology is based on pairing based cryptography principles and more specifically on pairings based on Elliptic Curve additive Groups and Finite field multiplicative groups, like Weil pairing, Tate pairing, Ate pairing e.t.c. Let $\mathbb{G}_1$, $\mathbb{G}_2$ be additive cyclic groups of prime order q and $\mathbb{G}_T$, a multiplicative cyclic group where each element has order dividing q. Then, we can define the mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ as a pairing if it satisfy the following properties:

1. Bilinear: $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$ and $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$ and $e(a_h P, b_h Q) = e(P, Q)^{a_h b_h}$ for all $P_1, P_2, P \in \mathbb{G}_1, Q, Q_1, Q_2 \in \mathbb{G}_2$, and $a_h, b_h \in \mathbb{Z}$

2. Non-degenerate:$e(P, Q) = 1_{\mathbb{G}_T}$ for all $Q \in \mathbb{G}_2$ if and only if $P = 1_{\mathbb{G}_1}$ and similarly $e(P, Q) = 1_{\mathbb{G}_T}$ for all $P \in \mathbb{G}_1$ if and only if $Q = 1_{\mathbb{G}_2}$

3. Computable: There is an efficient algorithm to compute the pairing mapping $e(P,Q)$ for any $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$

We assume that the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are identical ($\mathbb{G}_1 \equiv \mathbb{G}_2$) (admissible pairing) and defined by Elliptic curve E of prime order q determined by its parameters $\{p,a,b,G,q,h\}$. In that case, the e mapping will be based on the EC based pairing approach (like Weil, Tate or Ate pairing e.t.c.). We require the Decisional Bilinear Diffie Hellman (DBDH) assumption to remain strong in $\mathbb{G}_1$ and therefore assume that the elliptic curve is non-supersingular or special case supersingular with high embedding factor. To fully describe the needed parameters for the proposed scheme we define the EC parameters $\{e,\mathbb{G}_1,\mathbb{G}_T,H_0(),H_1(),H_2(),H_3(),H_4()\}$. The full set of parameters, denoted as public parameters, of the proposed scheme $T = \{p,\mathbb{G}_T,a,b,G,q,h,e,H_0(),H_1(),H_2(),H_3(),H_4()\}$ are described below:

1. p: specifies $\mathbb{F}_p$ defining the Elliptic Curve E
2. q: the order of the $\mathbb{F}_p$
3. $a,b \in \mathbb{F}_p$ specify the Elliptic Curve.
4. $G:(x_G,y_G) \in E(\mathbb{F}_p) \equiv \mathbb{G}_1$ is a generator point in $\mathbb{G}_1$ of order q
5. Integer $h = \#E(\mathbb{F}_p)/q$ called cofactor
6. e is the bilinear mapping $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$
7. $H_0: \{0,1\}^* \to \mathbb{F}_p^*$, $H_1(): \{0,1\}^* \to \mathbb{G}_1$, $H_2(): \mathbb{G}_T \to \{0,1\}^n$, $H_3(): \{0,1\}^n \times \{0,1\}^n \to \mathbb{F}_p^*$, $H_4(): \{0,1\}^n \to \{0,1\}^n$

We assume that a set $\mathbf{U} = \left\{U^{(1)}, U^{(2)}, ..U^{(n)}\right\}$ of n participants $U^{(i)}$ wish to cooperate in order to establish a common Public Key $Pub = \{T, Q_{pub}\}$ and a corresponding private key $priv$ (master secret) for providing Identity Based Encryption functionality in a distributed manner. To recover $priv$, at least *t+1* participants need to cooperate (threshold cryptography principle) where $t < n$ using the Lagrange Interpolation equation $LI(x,y) \stackrel{def}{=} \prod_{g\in U, g\neq y} \frac{x-g}{y-g}$ where $x,y \in 1,2...n$ representing a participant $U^{(x)}$ or $U^{(y)}$.

2.1 Setup Stage

Initially, all participants that care to establish the proposed distributed system, must generate local public-private key pairs (one for each participant) and agree on a global public private key pair (Q_{Pub} - $priv$). This stage, denoted as *Setup*, performs key generation, establishment and distribution, is based on distributed secret sharing schemes (Shoup, 2000)

In the first step of this process each participant $U^{(j)}$ generates a local public - private key pair similar to the ElGamal Elliptic Curve scheme as follows:

1. Choose randomly $pr_j \in \mathbb{F}_p$
2. Compute point $Pu_j = pr_j \cdot G \in E(\mathbb{F}_p) \equiv \mathbb{G}_1$

This local key pair constitutes, at this stage, $U^{(j)}$'s contribution to the master secret generation. When completed, each participant issues a broadcast request to the remaining participants requesting a master key secret share and provides his local public key Pu_j. When requests from every participant k and associated local public keys are received, each participant $U^{(i)}$ performs the following steps:

1. Choose t random elements $\{s_1, s_2, \dots s_t\} \in \mathbb{F}_p$
2. Construct a t degree secret polynomial

$$f_i(x) = s_t x^t + s_{t-1} x^{t-1} + \cdots + s_1 x + s_0$$

where $s_0 = priv_{i,0} = pr_i$ and denote as $privi,0$ the participant's partial key share (at this point it is identical to local private key).

1. Generate for all $U^{(k)} \in U$, $priv_{i,k} = f_i(k)$ where $k \in \{0,1,\dots t \mid k \neq i\}$
2. $Q_i = priv_{i,0} \cdot G = pr_i \cdot G = Pu_i$
3. Send to each participant $U^{(j)}$ the following:

$\langle nonce_i, Q_i, Encr_{Q_j}(priv_{i,j}, H_0(Q_i, priv_{i,j}, nonce_i)) \rangle$ where j is one specific participant number out of the k requesting participants.

The above actions are performed by each participant of the system. When the requesting participant $U^{(j)}$ receives $n-1$ messages (one for each remaining participant $U^{(i)}$) he archives all $priv_{k,j}$ values, where $k \in \{1,2,...n\}$, $k \neq j$ and performs the following operations to construct the global public key Q_{pub} and his master key share $priv_j$:

$$\begin{aligned} Q_{pub} &= \sum_{k=1}^{n} Q_k = \\ &= \sum_{k=1}^{n} priv_{k,0} \cdot G = \sum_{k=1}^{n} pr_k \cdot G = priv \cdot G \end{aligned} \tag{1}$$

$$priv_j = \sum_{k=1}^{n} priv_{k,j} = \sum_{k=1}^{n} f_k(j) \in \mathbb{F}_p \tag{2}$$

The outcome of the *Setup* stage is the full setup of Threshold Certificate based encryption scheme, that consists of the public parameters T and the global public key Q_{pub} along with the set of master key secret shares $\mathbf{S_{priv}} = \{priv_1, priv_2, ...priv_i...priv_n\}$ distributed securely to each participant $U^{(i)}$. Note that each master secret key share $priv_i$ is known only to participant U^i. The *Setup* stage parameters are:

$$\{p, \mathbb{G}_T, a, b, G, q, h, e, H_0(), H_1(), H_2(), H_3(), H_4(), \mathbf{S_{priv}}, Q_{pub}\} \quad (3)$$

2.2 Certificate Extraction Stage

At this stage each participant requests from t+1 participants to vouch for his identity and certify it along with its public key. To achieve that, each participant $U^{(j)}$ chooses an identifying value ID_j and concatenates it with a identification validity period v_j, his local public key Pu_j and any other info he wish to include is his certification. The resulting concatenation is $(IDD_j) = \langle Pu_j \left| v_j \right| ID_j \left| other \right\rangle$. Using the (IDD_j) value, participant $U^{(j)}$ can issue a certificate request, performing the following procedure:

1. Participant $U^{(j)}$ chooses randomly t+1 participants and constructs U_{cert} subset of U of these participants.
2. Participant $U^{(j)}$ sends to each participant $U^{(k)} \in U_{cert}$ the following:

$$\langle IDD_j | U_{cert} | sign_{pr_j}(IDD_j | U_{cert}) \rangle \quad (4)$$

3. Upon receipt, each participant $U^{(k)} \in U_{cert}$ verifies the signature (apart from message integrity, the signature verification acts as a proof of knowledge of $U^{(j)}$'s private key) and calculates $Q_{ID_j} = H_1(IDD_j | U_{cert} | Q_{pub})$ as well as $P_{C_j} = priv_k \cdot LI(0,k) \cdot Q_{ID_j}$ and sends to $U^{(j)}$ the following:

$$\langle Q_{ID_j} | P_{C_k} | g_1 \rangle \quad (5)$$

where $g_1 = e(pr_k \cdot Q_{ID_j}, priv_{k,j} \cdot G)$

4. The requesting participant $U^{(j)}$ collects all answers from the U_{cert} set and for each reply, validates the $U^{(k)}$'s knowledge of the pr_k and $priv_{j,k}$ (it was transmitted to $U^{(j)}$ from $U^{(k)}$ during setup stage) by calculating $\acute{Q_{ID_j}} = H_1(IDD_j | U_{cert} | Q_{pub})$ and evaluating if the equation $g_1 =^? e(\acute{Q_{ID_j}}, Q_k)^{priv_{k,j}}$ is true.
5. When the above validation is successful then $U^{(j)}$ performs

$$d_{ID_j} = \sum_{k \in U_{cert}} P_{C_k} = priv \cdot Q_{ID_j} \quad (6)$$

6. Participant $U^{(j)}$ calculates $f_{ID_j} = H_0(CI_j)$, where $CI_j = (IDD_j | U_{cert} | Q_{pub})$ and computes its full certificate $Cert_j$ of his identification characteristics CI_j by performing:

$$Cert_j = f_{ID_j} \cdot pr_j \cdot Q_{ID} + d_{ID_j} \quad (7)$$

2.3 Encryption Stage

When the certificate is established by the cooperation of $t+1$ participants, $U^{(j)}$ can use it as a private key in order to perform encryption/ decryption operations. If a participant wants to send securely a message $M \in \{0,1\}^n$, where n is an integer indicating M's bit length, to $U^{(j)}$, he uses $U^{(j)}$'s identity characteristics CI_j including the local public key (Pr_j), the identification validity period and the global public key Q_{pub} and needs to perform the following steps:

1. Compute $g_{ID_j} =$

$$\begin{aligned} & e(Cert_j, G) = e(f_{ID_j} \cdot pr_j \cdot Q_{ID} + d_{ID_j}, G)) \\ & = e((f_{ID_j} \cdot pr_j + s) \cdot Q_{ID_j}, G) \\ & = e(H_1(CI_j), H_0(CI_j) \cdot Q_j + Q_{pub}) \end{aligned} \quad (8)$$

2. choose a random number $\sigma \in \{0,1\}^n$
3. Set $sk_j = H_4(\sigma)$, $c = E^E_{sk_j}(M)$, $h_1 = H_3(\sigma, c)$, $e_1 = h_1 \cdot G$, $e_2 = \sigma \oplus H_2(g^{h_1}_{ID_j})$
4. The encrypted message is $C = (e_1 | e_2 | c)$

2.4 Decryption Stage

When an encrypted message C reaches participant $U^{(j)}$, he uses his certificate $Cert_j$, acting as a private key, and performs the following:

1. Assign values to the variables e_1, e_2, c from C
2. Compute $e_3 = e(Cert_j, e_1)$ and $\acute{\sigma} = e_2 \oplus H_2(e_3)$
3. Check if $\acute{\sigma} \in \{0,1\}^n$ and if true compute $\acute{sk_j} = H_4(\acute{\sigma})$
4. Compute $\acute{h_1} = H_3(\acute{\sigma}, c)$
5. Perform validity check using equations $(e_1 = \acute{h_1} \cdot G)$ and $(e_2 = \acute{\sigma} \oplus H_2(g^{\acute{h_1}}_{ID_j})$
6. If validity check is passed successfully, compute $m = E^D_{\acute{sk_j}}(c)$. Then, $M = m$.

2.5 Algorithm Analysis

The verification of the encryption/decryption validity is straightforward. Taking into account that $g_{ID_j} = e(Cert_j, G) = e(H_1(CI_j), H_0(CI_j) \cdot Q_j + Q_{pub})$ the validity of decryption is as follows:

$$
\begin{aligned}
e_3 &= e(Cert_j, e_1) = e(Cert_j, h_1 \cdot G) \\
&= e(Cert_j, G)^{h_1} = g_{ID_j}^{h_1} \\
\acute{\sigma} &= e_2 \oplus H_2(e_3) = \sigma \oplus H_2(g_{ID_j}^{h_1}) \oplus H_2(g_{ID_j}^{h_1}) \\
&= \sigma \qquad (9) \\
s\acute{k}_j &= H_4(\acute{\sigma}) = H_4(\sigma) \\
&\textit{and} \\
m &= E^D_{s\acute{k}_j} = E^D_{sk_j} = M
\end{aligned}
$$

The notations $Esk_j{}^E()$ and $Esk_j{}^D()$ refer to the encryption and decryption functions of a one-time secure symmetric encryption scheme, as is referred in (Shao, 2011), (Fujisaki and Okamoto, 1999). Instead of this, we can also use an one-time signature scheme as is suggested in (Galindo et al., 2008). The performance cost of the symmetric scheme is trivial in comparison with the bilinear pairing or point multiplication operations required during the execution of the proposed approach.

3 PARTICIPANT ADDITION - REMOVAL

One of the important benefits of the proposed certification scheme is its ability to easily add and remove Participants in the group U. To achieve that, we employ a mechanism similar to the one proposed in (Noack and Spitz, 2008). For these actions to function correctly, we assume that the certification scheme has been already established, that every participant has his local public-private key pair, his partial public key pair as well as his legitimate certificate and that he has contributed successfully to the generation of the global public-private key pair of the distributed CA. In other words, we can assume without loss of generality that all operations described in section 2 have been concluded successfully.

We employ the share renewal technique described in (Noack and Spitz, 2008), based on the PSS scheme of (Herzberg et al., 1995). PSS updates already distributed shares of all n members to provide proactive security. While adding a participant, $t+1$ members of U forming a subset U_{splt}, split off a part of their secret and share this part with the new member. Removing a participant is done by computing and redistributing the participant's secret to some remaining U members.

4 SECURITY ANALYSIS

The security of the proposed system is always retained as far as less than t participants are susceptible to secret information leakage. In our approach it is assumed that the system's participants act in a honest way. The lack of trusted dealer guarantees that the master secret key will not be compromised. The system's security is based on the CBE and DKG threshold cryptography schemes, inherited by the work of (Noack and Spitz, 2008) and (Shao, 2011). The CBE scheme of the proposed approach is semantically secure against adaptive Chosen Cipher text Attacks (IND-CB-CCA2) based on Type I and Type II Adversary challenges as indicated in (Shao, 2011).

Type I adversary is defined as an uncertified entity impersonating a legitimate participant by using forged credentials (key pairs or certificate) while Type II adversary is defined as a malicious CA, who wants to impersonate a legitimate participant with a given local public key. In both cases, the DKG scheme integrated in the proposed approach makes impossible for the adversaries to gain an advantage over the system's security. In all possible attacks, a Type I adversary cannot provide some legitimate master key share and therefore is exposed after his first attempt to perform an encryption/decryption operation with his credentials. Type II adversary has no foothold on the system since no participant can act as an individual CA unless we assume that each participant of the system is a CA of itself. In that case, it will have to act dishonorably from the setup phase which by default is not considered as an attack option.

The above security reasoning is accurate as long as the DKG CBE based scheme is considered secure. The Threshold cryptography DKG scheme is inherited from (Noack and Spitz, 2008) where the security of this scheme is proven. Even if dishonest participant are included as an option, the system's security can be retained by modifying the Threshold cryptography DKG scheme into a Verifiable Secret Sharing DKG scheme like the ones described in (Pedersen, 1991) and (Gennaro et al., 2007).

5 CONCLUSIONS

In this paper, we introduced the notion of a fully decentralized Threshold CBE Scheme that is capable of certificate issuing for encryption and decryption with not trusted dealer entity, easy participant addition-removal and CBE inherited simple certificate revocation mechanism. It can be concluded that the use of CBE schemes in combination with non trusted dealer, threshold cryptography, DKG schemes can result in a fully decentralized - distributed system. Such a system can be used in applications where no centralization is required like p2p networks, ad hoc networks or MANETs thus offering a strong security backbone to those applications and simplifying their security functionality with small compromises (mostly in performance). Our future goal is to expand the proposed solution so as to include better malicious participant discovery and provide formalization of the system's security characterization.

REFERENCES

Boneh, D., Boyen, X., and Halevi, S. (2006). Chosen ciphertext secure public key threshold encryption without random oracles. In Pointcheval, D., editor, *CT-RSA*, volume 3860 of *Lecture Notes in Computer Science*, pages 226–243. Springer.

Boneh, D. and Franklin, M. K. (2001). Identity-based encryption from the weil pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 213–229, London, UK. Springer-Verlag.

Boyen, X. (2008). A tapestry of identity-based encryption : practical frameworks compared. *International Journal of Applied Cryptography*, 1(1):3–21.

Damgard, I. and Koprowski, M. (2000). Practical threshold rsa signatures without a trusted dealer. pages 152–165. Springer Verlag.

Desmedt, Y. and Frankel, Y. (1989). Threshold cryptosystems. In Brassard, G., editor, *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 307–315. Springer.

Fournaris, A. P. (2011). Distributed threshold cryptography certification with no trusted dealer. In Lopez, J. and Samarati, P., editors, *SECRYPT 2011*, pages 400–404. SciTePress.

Frankel, Y., Gemmell, P., MacKenzie, P. D., and Yung, M. (1997). Optimal resilience proactive public-key cryptosystems. In *FOCS*, pages 384–393. IEEE Computer Society.

Fujisaki, E. and Okamoto, T. (1999). Secure integration of asymmetric and symmetric encryption schemes. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 537–554, London, UK. Springer-Verlag.

Galindo, D., Morillo, P., and Rfols, C. (2008). Improved certificate-based encryption in the standard model. *Journal of Systems and Software*, 81(7):1218 – 1226.

Gennaro, R., Jarecki, S., Krawczyk, H., and Rabin, T. (2001). Robust threshold dss signatures. *Inf. Comput.*, 164(1):54–84.

Gennaro, R., Jarecki, S., Krawczyk, H., and Rabin, T. (2007). Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology*, 20:51–83. 10.1007/s00145-006-0347-3.

Gentry, C. (2003). Certificate-based encryption and the certificate revocation problem. In Biham, E., editor, *Advances in Cryptology EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 641–641. Springer Berlin / Heidelberg.

Herzberg, A., Jarecki, S., Krawczyk, H., and Yung, M. (1995). Proactive secret sharing or: How to cope with perpetual leakage. In *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '95, pages 339–352, London, UK. Springer-Verlag.

Libert, B. and Quisquater, J.-J. (2003). Efficient revocation and threshold pairing based cryptosystems. In *Proceedings of the twenty-second annual symposium on Principles of distributed computing*, PODC '03, pages 163–171, New York, NY, USA. ACM.

Lu, Y. (2011). An efficient and provably secure certificate-based encryption scheme. In Zhou, Q., editor, *Theoretical and Mathematical Foundations of Computer Science*, volume 164 of *Communications in Computer and Information Science*, pages 54–61. Springer Berlin Heidelberg.

Lu, Y. and Li, J. (2009). Forward-secure certificate-based encryption. In *Proceedings of the 2009 Fifth International Conference on Information Assurance and Security - Volume 02*, IAS '09, pages 57–60, Washington, DC, USA. IEEE Computer Society.

Lu, Y., Li, J., and Xiao, J. (2009). Threshold Certificate-Based Encryption: Definition and Concrete Construction. In *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, pages 278–282. IEEE.

Noack, A. and Spitz, S. (2008). Dynamic threshold cryptosystem without group manager. Cryptology ePrint Archive, Report 2008/380. http://eprint.iacr.org/.

Park, C. and Kurosawa, K. (1996). New ElGamal Type Threshold Digital Signature Scheme. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E79-A(1):86–93.

Pedersen, T. P. (1991). A threshold cryptosystem without a trusted party. In *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'91, pages 522–526, Berlin, Heidelberg. Springer-Verlag.

Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22:612–613.

Shao, Z. (2011). Enhanced certificate-based encryption from pairings. *Comput. Electr. Eng.*, 37:136–146.

Shoup, V. (2000). Practical threshold signatures. In *Proceedings of the 19th international conference on Theory and application of cryptographic techniques*, EUROCRYPT'00, pages 207–220, Berlin, Heidelberg. Springer-Verlag.

Wang, G. (2003). On the security of the li-hwang-lee-tsai threshold group signature scheme. In Lee, P. and Lim, C., editors, *Information Security and Cryptology ICISC 2002*, volume 2587 of *Lecture Notes in Computer Science*, pages 75–89. Springer Berlin / Heidelberg. 10.1007/3-540-36552-4-6.