Anonymous Key Issuing Protocol for Distributed Sakai-Kasahara Identity-based Scheme

Amar SIAD
Laboratoire Analyse Géométrie et applications LAGA-Paris 13
Université Paris 8, 2 rue de la Liberté 93526
SAINT-DENIS, France
siad@math.univ-paris13.fr

Moncef AMARA
Université Paris 8, 2 rue de la Liberté 93526
SAINT-DENIS, France
amara02@etud.univ-paris8.fr

***Abstract*—Practical implementations of identity based cryptosystems are faced to key escrow problem, which is not always a good property in many realistic scenarios. Thus, efficient key issuing protocols are needed to generate and deliver user's private keys in secure manner without leakage. Three major approaches exist in the literature, we are interested in two of them. The first one suggested the distribution of the master secret key over multiple authorities. The second approach, concerned about user privacy, and proposed to generate and deliver user's private keys in an anonymous manner. Each one of the above approaches has its own drawbacks and key escrow problem is steal an issue in identity-based systems. In this paper, we design a new framework that combines the two approaches above to solve key escrow problem and single point of failure in Identity-based Encryption systems by allowing privacy-preserving propriety. As instantiation, we construct an anonymous key issuing protocol for the distributed sakai-kasahara IBE scheme presented recently by *Kate and Goldberg* based on the anonymous key issuing protocol proposed by *Chow*, along with a security analysis.**

Keywords-Key issuing protocols; Distributed key generation; Anonymous IBE.

I. INTRODUCTION

Traditional Public Key Infrastructure PKI, supporting Public Key Cryptography PKC, provided mechanisms required for certificate issuing, maintain, and revocation. Thus, it has succeeded in many applications by managing the trust between different entities. However, PKI is not a perfect solution, and many problems steal subsists due to the administrative burden of certificates, revocation lists or trees, and cross-domain certification.

In 1984, Shamir [1] proposed a novel concept called Identity Based Public Key Cryptography (ID-PKC), where the original motivation is to simplify certificate management in PKI-based systems. The main idea of so called ID-PKC is to derive users public key from his identity information whereas the private key is generated by a third party called Private Key Generator (PKG) and issued to the user via a secure channel. Shamir presented an identity based signature system (IBS) using RSA and conjectured that encryption systems could be constructed. Compared to traditional Public Key Cryptography, ID-PKC present the advantage of simplified key distribution and management (no need for certificates). However, it suffers from an inherent drawback of key escrow, where the PKG could decrypt any message addressed to a user by generating that user's private key. Moreover, it requires a secure channel for users' private keys issuance.

Since the shamir's challenge, the cryptographic community had to wait until the turn of the century to see practical constructions of ID-PKC systems, considered thus far an open problem. The first scheme by Cocks [2] using the quadratic residues, whereas the second one by Boneh and Franklin [3] using Weil pairings on elliptic curves.

Boneh and Franklin construction have widely opened doors to an important development in recent years. Thus, a flurry of schemes have been proposed, improved, proven secure, and security formal models have been more and more strengthen. However, the deployment of practical ID-based systems have not followed the same rhythm of these theoretical improvements and the few systems' implementations proposed deal with a set of particular limited scenarios. [4] pointed-out that the deployment of an ID-based system requires an infrastructure as complex as a PKI. *Chen et al.* [5] presented a hybrid scheme combining traditional PKI with ID-PKC in a multi-authority environment.

Interoperability issues of ID-PKC and PKI are also discussed in [6]. Whereas many works studied key issuing protocols [3], [7], [8], [9], [10], [11] presenting wide rage solutions of key escrow problem, but none of the proposed solution is perfect and key escrow is steal an issue facing the deployment of ID-based systems. In the same scope [12] developed an architecture model for distributed PKG, using PKI, for internet applications. Recently, Chow [10] exploited the anonymity propriety to fight against key escrow problem by defining an anonymous key issuing protocol for Gentry scheme.

We organize the rest of the paper as follows. In Section II, we give related work and our contribution. In Section III, we give some preliminaries. In Section IV, we define the general framework and architecture along with security requirement. In Section V, we present a construction of a

Copyright (c) IARIA, 2011 ISBN:978-1-61208-113-7

distributed AKI for SK-IBE scheme. Finally, we conclude in Section VI.

II. Related work

Key escrow problem made the deployment of practical ID-PKC cryptosystems limited to small and relatively closed organisations where the trust in PKG is very heigh. To tackle this restriction and extend the use of ID-PKC in scenarios equivalent to the ones of PKI-based PKC, key issuing protocols are studied. These protocols allow the user to have his key without leakage. We classify key issuing protocols into three main categories described hereafter.

Multi-authorities and distributed protocols. in addition of key escrow problem, this approach deal with the problem of single point of failure. [3], [13], [14], [15], [16] proposed different but related approaches to split the master secret key to multiple $\mathcal{KGC}$s. The user obtains a partial private key from each $\mathcal{KGC}$ and reconstructs his private key in threshold manner. [7], [17] used the concept of key privacy authorities $\mathcal{KPA}$ to deliver user's private key in blinded manner using a single $\mathcal{KGC}$ and multiple $\mathcal{KPA}$. Recently, *Geisler and Smart* [11] proposed distribution version of sakai-kasahara based systems, *Kate and Goldberg* [18] developed a distributed private-key generators for three IBE schemes along with their security proofs.

Anonymous protocols. Anonymous key issuing protocols where first considered by *Sui et al.* [19] where they separate authentication phase from key issuing by using a database to store identities and corresponding passwords, whereas the fact of using the database gives the $\mathcal{KGC}$ the capability to link key requests with user's identity and break the anonymity of the proposed protocol. Recently, chow [10] extended the anonymity notion to fight against adversaries who hold the master key and proposed an anonymous key issuing protocol for a modified gentry IBE scheme. However, as chow pointed out, the proposed protocol has a major drawback where the $\mathcal{KGC}$ can generate all possible user private keys by guessing user identities according to some dictionary.

User-chosen secret information. Another approach have been introduced by [8], [9] who proposed respectively the concept of Certificate-Based Encryption (CB-PKC) and Certificateless Cryptography (CL-PKC). These two solutions avoid successfully the escrow problem by combining advantages of traditional PKC and ID-PKC to create a hybrid model. However, as already evoked in [7] these approach loose the main propriety of an IBE system in which the user public key is derived from his identity, and thus are not considered purely IBE systems.

A. Our contribution.

The main idea behind our protocol is to combine multi-authorities approaches with anonymous protocols in order to develop a new class of protocols. In [10], the use of an anonymous protocol prevent the $\mathcal{KGC}$, or an adversary having access to the master key, from linking user's identity to the private key generated for that identity. However, the $\mathcal{KGC}$ can still generate private keys for identities of his choice (ie. by guessing users' identities) and then proceed by an off-line analysis of messages flow by trying to decrypt messages using the key generated. To overcome this drawback, we propose to extend the anonymous key issuing protocol in [10] to prevent the $\mathcal{KGC}$ from this capability by distributing the $\mathcal{KGC}$ master secret key over multiple authorities in conjunction with a certification authority CA to authenticate users and deliver new kind of certificates by signing on a committed value of the user identity, the same way as in [10]. The certificate will be presented by user to each one of the n $\mathcal{KGC}$ to get his private key. This new architecture, will solve key escrow problem and single point of failure. Our contribution can also seen as an extension of the distributed protocols in [11], [18] to support user anonymity.

III. Preliminaries

A. Bilinear pairings

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be cyclic groups of prime order q, P_1 a generator of $\mathbb{G}_1$, and P_2 a generator of $\mathbb{G}_2$. A bilinear pairing e is a map defined by e: $\mathbb{G}_1$x $\mathbb{G}_2 \rightarrow \mathbb{G}_T$ with the following properties:

1) Bilinear : $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_q^*$.
2) Non degeneracy : $e(P_1, P_2) \neq 1$.
3) Efficiently computable: there exists an efficient algorithm to compute $e(P, Q)$ for all $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$.

B. Distributed key generation

Hereafter we give a quick review of the distributed computation primitives used in this work, for more details we refer the reader to [18]. Distributed key generation DKG is introduced by Pederson [20], who developed a DKG that requires no dealer. An (n, t) DKG is composed of n nodes that generate a secret $z \in \mathbb{Z}_p$ in a distributed fashion. Each node gets a share $z_i \in \mathbb{Z}_p$ such that any subset of size greater than t could reconstruct the secret.

Shares Generation. depending on weather we use discrete logarithm (Dlog) or Pedersen (Ped) commitments, nodes use one of the two protocol $(Random_{Dlog}(), Random_{Ped}())$ to generate shares of a secret $z \in \mathbb{Z}_p$ chosen jointly at random.

1) $\left(\mathcal{C}_{\langle g \rangle}^{(z)}, z_i\right) = Random_{DLog}(n, t, g)$
2) $\left(\mathcal{C}_{\langle g,h \rangle}^{(z,z')}, \left[\mathcal{C}_{\langle g \rangle}^{(z)}, NIZKPK_{\equiv com}\right], z_i, z_i'\right) = Random_{Ped}(n, t, g, h)$.

Recall that $\left(\mathcal{C}_{\langle g \rangle}^{(z)}\right) = [g^z, g^{\phi(1)}, ..., g^{\phi(n)}]$ and $\left(\mathcal{C}_{\langle g,h \rangle}^{(z,z')}\right) = [g^z h^{z'}, g^{\phi(1)} h^{\phi'(1)}, ..., g^{\phi(n)} h^{\phi'(n)}]$ are respectively Discret log and Pedersen commitment victors for z, and $\phi, \phi' \in \mathbb{Z}_p[x]$ are polynomials of degree t where $\phi(0) = z, \phi'(0) = z'$, $\phi(i) = z_i$, and $\phi'(i) = z_i'$.

Distributed Multiplication. for distributed multiplication we use the second protocol from [18] that uses a multiplication protocol against computational adversaries with a non-interactive proof of knowledge defined as follows.
$\left(\mathcal{C}_{\langle \hat{g},\hat{h} \rangle}^{(\alpha\beta,\alpha\beta')}, (\alpha\beta)_i, (\alpha\beta')_i\right) = Mul_{Ped}(n, t, \hat{g}, \hat{h}, \left(\mathcal{C}_{\langle g \rangle}^{(\alpha)}, \alpha_i\right), \left(\mathcal{C}_{\langle \hat{g},\hat{h} \rangle}^{(\beta,\beta')}, \beta_i, \beta_i'\right))$.
By this each node computes locally the share of the product of two shared secrets α, β.

C. Sakai-Kasahara-IBE

SK-IBE Setup(λ): Given the security parameter λ, the parameter generator follows the steps.

1) Generate three cyclic groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of prime order q, a bilinear pairing map $e : \mathbb{G}_1$ x $\mathbb{G}_2 \rightarrow \mathbb{G}_T$ and random generators $(g, \hat{g})$ for respectively $\mathbb{G}_1$, $\mathbb{G}_2$.
2) Pick four cryptographic hash functions $H_1 : \{0,1\}^* \longrightarrow \mathbb{Z}_p$, $H_2 : \mathbb{G}_2 \longrightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n$x$\{0,1\}^n \rightarrow \mathbb{Z}_q^*$ and $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ for $n > 0$.
3) Pick a random $s \in \mathbb{Z}_q^*$ and compute $pk = g^s$

The public parameters are $params = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, n, g, \hat{g}, g^s, H_1, H_2, H_3, H_4)$

SK-IBE Extract(msk, ID): the private key d_{ID} of user having ID as identity is computed bay:$d_{ID} = \hat{g}^{\frac{1}{s+H_1(ID)}}$

SK-IBE Encryption(mpk, ID, m) : to encrypt a k' bit length message M, the sender picks at random $\sigma \in \{0,1\}^{k'}$, computes $r = H_3(\sigma, M)$, $h_{ID} = H_1(ID)$ and sends the cyphertext $C = (u, v, w) = ((g^s g^{h_{ID}})^r, \sigma \oplus H_2(e(g, \hat{g})^r), M \oplus H_4(\sigma))$ to the recipient.

SK-IBE Decryption(d_{ID}, c): to decrypt the cyphertext $C = (u, v, w)$ with the private key d_{id}, the receiver successively computes $\sigma = v \oplus H_2(e(u, d_{id}))$, $M = \sigma \oplus H_4(\sigma)$, $r = H_3(\sigma, M)$. If $(g^s g^{h_{ID}})^r \neq u$ then C is rejected else M is a valid message.

D. Anonymity in IBE

Anonymity against user attacks for IBE was introduced first by *Abdella et al.* [21] similarly to semantic security. The attacker's goal is to distinguish the intended recipient of a ciphertext between two chosen identities.The previous definition of anonymity cannot provide security against $\mathcal{KGC}$ attacks. Recently, this notion was strengthen and extended to handle $\mathcal{KGC}$ attacks by two independent works [22], [10]. Izabachne and pointcheval [22] called it KwrtA-Anonymity (Key Anonymity with respect to the Authority) and applied it in password-authenticated key exchange. Whereas, Chow [10] called it $\mathcal{ACI} - \mathcal{KGC}$ (Anonymous Cyphertext Indistinguishability) and used it to fight against key escrow.

IV. General framework

We extend the framework given in [10] to support the distributed architecture. We assume the existence of a certification authority $\mathcal{CA}$ and multiple key generation centres.

A. Entities and Their Roles

The entities involved the new architecture are as follows.

- $\mathcal{CA}$**:** certification authority is a trusted authority in the standard PKI based model. The CA is responsible for checking users identities and certificate issuing, it is clear that $\mathcal{CA}$ holds the identity list of all users in the system. $\mathcal{CA}$ has a master secret key sk_{cert} and the corresponding public key pk_{cert}.
- n $\mathcal{KGC}$**:** multiple authorities for user key generation using (n, t) threshold secret sharing scheme and without knowing the identity of the user. Each $\mathcal{KGC}$ has a secret key s_i and the corresponding public key pk_i. We make the assumption that $\mathcal{CA}$ doesn't collude with $\mathcal{KGC}s$, otherwise the user anonymity can be broken.
- **User:** he should first present authenticate himself to the $\mathcal{CA}$ which issue a certificate on a commitment on the user identity. Then he presents his certificate to each one of the t $\mathcal{KGC}$s to get partial private keys. Finally, the user compute his private key by interpolation.

B. AKI for distributed IBE

Définition 4.1: **(AKI for (n, t) IBE)** an anonymous key issuing protocol for (n, t) IBE scheme consists of components ($\mathcal{SIGN}, \mathcal{P} - \mathcal{SIGN}, \mathcal{DKG}, \mathcal{C}$) specified as follows:

1) $\mathcal{SIGN}$: signature scheme run by $\mathcal{CA}$ to generate user certificate. The certificate is delivered to the user securely and is presented by user to $\mathcal{KGC}$. Note that the certificate doesn't contain user's name and not used anywhere else in the system.
2) $\mathcal{P} - \mathcal{SIGN}$: p-signature scheme [23] that allows the user, with a private input, to get a signature on a commuted value of the identity without revealing it to the signer. Note that p-signature is a primitive that uses secure two-party computation protocol on committed values.
3) $\mathcal{DKG}$: Distributed key generation protocol, that takes as input the security parameter λ , the threshold parameters (t,n) and outputs for each player P_i (for $i = 1, ..., n$) a share s_i of the master secret key s and

a public-key vector K_{pub} of a master public key and n public-key shares.;

4) $\mathcal{C}$: non interactif commitment scheme.

More formally, An AKI-protocol for (n, t) IBE scheme is defined by the following algorithms as follows:

$(pk_{CA}, sk_{CA}, cert_{CA}) \leftarrow$ **SetupCA(λ):** probabilistic algorithm executed by $\mathcal{CA}$, it takes as input security parameter λ and returns $\mathcal{CA}$ public key pk_{CA}, master secret key sk_{CA}, and $\mathcal{CA}$ certificate $cert_{CA}$.

$(cert_U, open) \leftarrow$ **CertIssue(sk_{CA}, ID):** probabilistic algorithm executed by $\mathcal{CA}$ to deliver certificates to users. It takes as input $\mathcal{CA}$ secret key sk_{CA}, user identity ID and returns user certificate $cert_U = (sig, comm, open)$, where $open$ is chosen at random from the decommitment-string space and sig is a signature on $comm = Commit(H(ID), open)$, where H is a hash function.

$(s_1, pk_1, ..., s_n, pk_n, pk) \leftarrow$ **DKeyGen(λ, t, n):** distributed key generation protocol runs between the n $\mathcal{KGC}$ and results in each $\mathcal{KGC}$ obtaining a share $s_i \in \mathbb{Z}_q$ of the master secret s. The tuple $(pk, pk_1, ..., pk_n)$ is the system public-key.

ObtainKey$(\mathcal{U}(params, id, cert_U, open)) \leftrightarrow$ **IssueKey** $(\mathcal{KGC}_i(params, s_i, cert_U))$ **:** an interactive protocol, using a secure two-party computation protocol, executed between user $\mathcal{U}$ and $\mathcal{KGC}_i$ for $i = 1, ...t+1$ ($t+1$ out of n $\mathcal{KGC}$). $\mathcal{U}$ takes as input master public key mpk, the identity id, certificate $cert$, opening information $open$ and gets a partial secret key $d_{id}^{(i)}$ as output. $\mathcal{KGC}_i$ takes as input master secret key s_i, user certificate $cert_U$ and gets nothing as output.

ReconstructKey($d_{id}^{(1)}, ..., d_{id}^{(t+1)}$): upon receiving $t+1$ partial private key, user reconstructs his private keys in threshold manner.

C. Security requirements

Définition 4.2: **(Secure AKI :)** an anonymous key issuing protocol for (n, t) IBE is secure if: *(1)* p-signature scheme is unforgeable and satisfies signer privacy and user privacy; *(2)* DKG protocol satisfies correctness and secrecy; *(3)* commitment scheme is perfectly binding and strongly computationally hiding.

V. Construction

chow [10] argued that SK-IBE can be made $\mathcal{ACI} - \mathcal{KGC}$ the same way as gentry scheme by separating parameters generation from key generation. Admitting this fact, hereafter we modify SK-IBE to support anonymity against $\mathcal{KGC}$ and give an anonymous key issuing protocol. p-signature scheme from [23] is used in [10] to construct an anonymous key issuing protocol for modified gentry scheme, assuming the same framework architecture, we adapt this protocol to a modified version of SK-IBE scheme that supports $\mathcal{ACI} - \mathcal{KGC}$.

A. AKI for SK-IBE scheme

Setup public parameters are generated by trusted initializer as follows. $params = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, n, g, \hat{g}, H_1, H_2, H_3, H_4)$

SK-IBE KeyGen: the $\mathcal{KGC}$ randomly chooses an exponent s and computes g^s. (s, g^s) is the private/public key pair of the $\mathcal{KGC}$.

Encrypt(), Decrypt(): these algorithms remain as in the original version, whereas the private key extraction algorithm **Extract()** is modified as follows.

ObtainKey$(\mathcal{U}(params, id, cert_U, open)) \leftrightarrow$ **IssueKey** $(\mathcal{KGC}(\ params, msk, cert_U))$ **:**

- User presents his certificate $cert_U$ to $\mathcal{KGC}$, the latter verifies certificate signature using the CA public key pk_{cert} if certificate verification fail it aborts the protocol.
- The user chooses at random ρ in $\mathbb{Z}_q$;
- The user and $\mathcal{KGC}$ engage in a secure two-party computational protocol[24], where the user's private input is $(\rho, H_1(ID), open)$, and the $\mathcal{KGC}$'s private input is msk. As result, the $\mathcal{KGC}$ gets a private output which is either $x = (x + H_1(ID))\rho$ if $comm = commit(H_1(ID), open)$ or $\perp$ in this case the $\mathcal{KGC}$ aborts.
- if $x \neq \perp$ the $\mathcal{KGC}$ send $\sigma' = \hat{g}^{\frac{1}{x}}$ to the user;
- the user computes, upon receiving σ', $\sigma = (\sigma')^{\rho} = \hat{g}^{\frac{1}{msk + H_1(ID)}}$.

B. Security analysis

Recall the definition of p-signature, which is a signature on a committed message without revealing the message using a secure two-party computation protocol on committed inputs, the user private key in SK-IBE scheme can be seen as the first p-signature [23]. Thus, the above protocol is a direct application of the weak p-signature scheme proposed in [23], proven secure, and having properties: Signer Privacy, User privacy, Correctness, Unforgeability, and Zero-Knowledge.

Intuitively, security in the above protocol concerns two entities $\mathcal{KGC}$ and user. Following the same analysis in [10] the above protocol is secure if the underlying p-signature scheme is secure and the Signer Privacy, User privacy properties hold. In one hand, Signer Privacy ensures that a malicious user interacting with the $\mathcal{KGC}$ can't get any information on $\mathcal{KGC}$ master secret key other than user private key. On the other hand, the certificate presented by

the user to a malicious KGC reveals no information about the real identity of the user.

VI. Distributed anonymous SK-IBE

A. AKI for distributed SK-IBE

Smart el al. [11] presented a distributed version of Sakai-Kasahara scheme, in this section we give a modification of this scheme combined with the IND-ID-CCA scheme from [18], which we call DSK-IBE, assuring user anonymity when generating his private key by $\mathcal{KGC}$. As in Chow [10], master key generation is separated from the Setup stage, reducing further trust required in the $\mathcal{KGC}$.

DSK-IBE Setup : We first define explicitly the system's public parameters. Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ denote groups of large prime order q, which are equipped with a bilinear pairing, $e : \mathbb{G}_1$ x $\mathbb{G}_2 \rightarrow \mathbb{G}_T$. We assume that $\mathbb{G}_1$, $\mathbb{G}_2$ are respectively generated by g and $\hat{g}$. We define four hash functions, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \mathbb{G}_T \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n$x$\{0,1\}^n \rightarrow \mathbb{Z}_q^*$ and $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ for $n > 0$.

DSK-IBE KeyGen : distributed protocol runs between the n $\mathcal{KGC}$ and results in each $\mathcal{KGC}$ obtaining a share $s_i \in \mathbb{Z}_q$ of the master secret s. The tuple $\mathcal{C}_{\langle g \rangle}^{(s)} = [g^s, g^{s_1}, ..., g^{s_n}]$ is the system public-key. Note that a coalition of upto t entities should gain nothing about s, whereas $t+1$ entities could reconstruct the secret s.

ObtainKey$(\mathcal{U}(params, id, cert_U, open))$ $\leftrightarrow$ **IssueKey** $(\mathcal{KGC}_i(params, s_i, cert_U))$ **:** DAKI protocol run between m $\mathcal{KGC}$s ($t < m \leq n$) to produce m outputs $d_{id}^{(i)}$ which are shares of private key d_{id}. We modify the distributed SK-IBE Private key extraction [18] by adding steps 1 to 3 which made the protocol anonymous as follows:

1) User presents his certificate $cert_U$ to each one of the $t+1$ $\mathcal{KGC}$, the latter verifies certificate signature using the CA public key pk_{cert} if certificate verification fail it aborts the protocol.
2) The user chooses at random ρ in $\mathbb{Z}_q$;
3) The user and KGC_i (for $i = 1, ..., t$) engage in a secure two-party computational protocol [24], where the user's private input is $(\rho, H_1(ID), open)$, and the KGC_i's private input is s_i. As result, the KGC_i gets a private output which is either $S_i^{ID} = (s_i + H_1(ID))\rho$ if $com = commit(H_1(ID), open)$ or $\perp$ in this case the $\mathcal{KGC}_i$ aborts.
4) $\mathcal{KGC}_i$ runs $\left(\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(z,z')}, z_i, z_i'\right) = Random_{Ped}(n, t, \hat{g}, \hat{h})$, where $\hat{h} \in \mathbb{G}_2$ is a generator for Pedersen commitments precomputed by $\mathcal{KGC}$s using $\left(\mathcal{C}_{\langle \hat{g} \rangle}^{(r)}\right) = Random_{DLog}(n, t, \hat{g})$, and set $\hat{h} = \left(\mathcal{C}_{\langle \hat{g} \rangle}^{(r)}\right)_0 = \hat{g}^r$. $\mathcal{KGC}_i$ also computes $\left(\mathcal{C}_{\langle g \rangle}^{(S_i^{ID})}\right)_j = g^{(s_j + H_1(ID))\rho}$ for $0 \leqslant j \leqslant n$.
5) $\mathcal{KGC}_i$ runs $\left(\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(w,w')}, w_i, w_i'\right) = Mul_{Ped}(n, t, \hat{g}, \hat{h}, \left(\mathcal{C}_{\langle g \rangle}^{(S_i^{ID})}, S_i^{ID}\right), \left(\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(z,z')}, z_i, z_i'\right))$, where $w = s^{ID}z = (s + H_{1(ID)})\rho z$, $w' = s^{ID}z' = (s + H_{1(ID)})\rho z'$ and sends $\left(\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(w,w')}, w_i\right)$ along with $PK_1^{(i)} = NIZKPK_{\equiv} com(w_i, w_i', \left(\mathcal{C}_{\langle \hat{g}, \rangle}^{(w)}\right)_i, \left(\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(w,w')}\right)_i)$ to the user.
6) $\mathcal{KGC}_i$ sends to the user $\left(\mathcal{C}_{\langle \hat{g} \rangle}^{(z)}\right)_i = \hat{g}^{z_i}$ and $\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(z,z')}$ along with $PK_2^{(i)} = NIZKPK_{\equiv} com(z_i, z_i', \left(\mathcal{C}_{\langle \hat{g}, \rangle}^{(z)}\right)_i, \left(\mathcal{C}_{\langle \hat{g}, \hat{h} \rangle}^{(z,z')}\right)_i)$.

ReconstructKey$(w_i, \hat{g}^{z_i}, PK_1^{(i)}, PK_2^{(i)})$**:** Upon receiving $(w_i, \hat{g}^{z_i}, PK_1^{(i)}, PK_2^{(i)})$ for $(i = 1, ..., t+1)$ the user do the following computations:

1) verifies $\left(\mathcal{C}_{\langle \hat{g} \rangle}^{(z)}\right)_i$ using $PK_2^{(i)}$;
2) reconstructs (w, g^z) using Lagrange interpolation;
3) if $w = 0$ it aborts else it computes $w^{-1} = \frac{1}{(s+H_1(ID))\rho z}$;
4) computes his private key by: $d_{id} = (\hat{g}^z)^{w^{-1}\rho} = \left(\hat{g}^{\frac{1}{(x+H_1(ID))\rho}}\right)^{\rho} = \hat{g}^{\frac{1}{x+H_1(ID)}}$

B. Analysis

The above (n, t) SK-IBE scheme, without the anonymity propriety, was proven IND-ID-CCA secure in [18], assuming a standard t-limited Byzantine adversary in a system with n nodes, where any t nodes are compromised by the adversary. In contrast of this, and by adding steps (1) to (3), the obtained protocol is a distributed form of the p-signature scheme given in [23]. We argue that the new anonymous (n, t) SK-IBE scheme is IND-ID-CCA secure assuming the three following statements: (1) (n, t) SK-IBE scheme in [18] is IND-ID-CCA, (2) the underlying distributed p-signature scheme is unforgeable, satisfies issuer and user privacy, (3) the signature scheme used by $\mathcal{CA}$ is unforgeable.

Two primitives in the above construction are concerned by this analysis. Firstly, p-signature security follows the same rules as in Section (V.B) and results on user privacy, where a malicious $\mathcal{KGC}$ can't get any information about the real identity id of the user contained in the certificate $cert_U$ (this is ensured by the $\mathcal{CA}$ signature scheme proprieties that signs on a strongly computationally hiding commitment of id). For $\mathcal{KGC}$s privacy, due to the proprieties of the underlying secret sharing scheme, a malicious user can't get any information about $\mathcal{KGC}$ partial private key because shares he obtain $(w_i, \hat{g}^{z_i})$ reveal no information. Secondly, the signing algorithm of the certification authority is not specified, so the use of an unforgeable signature scheme, that signs on a perfectly binding and strongly computationally hiding commitment of the identity included in the certificate, should be fine for our purpose of security.

VII. Conclusion

In this paper, we proposed an architecture for developing new class of distributed key issuing protocols that have the privacy-preserving propriety. Assuming this architecture, we proposed a new anonymous key issuing protocol for the distributed SK-IBE, which belongs to the exponent-inversion family, along with a informal security analysis.

Our construction is based on the recently proposed distributed private key generator [18], [11] combined with the anonymous key issuing protocol [10] thus coupling advantages of the two approaches. The proposed protocol aims to solve key escrow problem and single point of failure in IBE systems, which will reduce trust needed in $\mathcal{KGC}$.

Further work is required to extend the proposed protocol to other IBE frameworks (i.e. commutative-blinding IBEs and full-domain-hash IBEs), and to define a formal security model.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *CRYPTO 84*, 1985, pp. 47–53.

[2] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *8th IMA International Conference*, ser. volume 2260 of LNCS. Springer Berlin, 2001, pp. 360–363.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, ser. volume 2139 of LNCS. Springer Berlin, 2001, pp. 213–229.

[4] Y. Desmedt and M. Burmester, "Identity-based key infrastructures iki," in *SEC 2004*, 2004, pp. 167–176.

[5] L. Chen, K. Harrison, A. Moss, D. Soldera, and N. Smart, "Certification of public keys within an identity based system," in *ISC 2002*, ser. volume 2433 of LNCS, Springer-Verlag. Canterbury, UK, June 30 July 1, 2005, pp. 322–333.

[6] G. Price and C. J. Mitchell, "Interoperation between a conventional pki and an id-based infrastructure," in *EuroPKI 2005*, ser. volume 3545 of LNCS. Canterbury, UK, June 30 July 1, 2005, pp. 73–85.

[7] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Secure key issuing in id-based cryptography," in *proceedings of the Second Australian Information Security Workshop-AISW 2004, ACS Conferences in Research and Practice in Information Technology vol.32*, 2004, pp. 69–74.

[8] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology - EUROCRYPT 2003*, ser. volume 2653 of LNCS. Springer Berlin, 2003, pp. 272–293.

[9] S. Al-Riyami and S. Paterson, "Certificateless public key cryptography," vol. 2894. Springer-Verlag, 2003, pp. 375–391.

[10] S. Chow, "Removing escrow from identity-based encryption," in *12th International Conference on Practice and Theory in Public Key Cryptography*, 2009, pp. 256–272.

[11] M. Geisler and N. P. Smart, "Distributing the key distribution centre in sakai-kasahara based systems," in *Conf. on Cryptography and Coding 09*, 2009, pp. 252–262.

[12] A. Kate and I. Goldberg, "A distributed private-key generator for identity-based cryptography, cryptology eprint archive, report 2009/355," Tech. Rep., 2009.

[13] L. Chen, K. Harrison, N. P. Smart, and D. Soldera, "Infrasec 2002," in *Applications of multiple trust authorities in pairing based cryptosystems*, ser. volume 2437 of LNCS, Springer-Verlag, 2002, pp. 260–275.

[14] K. Paterson, "Cryptography from pairings: a snap shot of current research," Information Security Technical Report 7 (3), Tech. Rep., 2002.

[15] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in CryptographySAC 02*, ser. volume 2595 of LNCS, Springer-Verlag, 2002, pp. 310–324.

[16] S. Kwon, "Cryptanalysis for secure key issuing in id-based cryptography and improvement, manuscript," Tech. Rep., 2004.

[17] B. Lee, E. Dawson, and S. Moon, "Efficient and robust secure key issuing in id-based cryptography," in *proceedings of the 6-th International Workshop on Information Security Applications (WISA 2005)*, 2005, pp. 267–280,.

[18] A. Kate and I. Goldberg, "Distributed private-key generators for identity based cryptography," in *To appear at SCN 10*, 2010.

[19] A. Sui, S. S. M. Chow, L. C. K. Hui, S. M. Yiu, K. P. Chow, W. W. Tsang, C. F. Chong, K. H. Pun, and H. W. Chan, "Seperable and anonymous identity-based key issuing without secure channel," in *11th International Comference on Parallel and Distributed Systems ICPADS*, ser. volume 2, 2005, pp. 275–279.

[20] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Cryptology CRYPTO 91*, 1991, pp. 129–140.

[21] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in *In CRYPTO*. Springer-Verlag, 2005, pp. 205–222.

[22] M. Izabachene and D. Pointcheval, "New anonymity notions for identity-based encryption," in *the 6th international conference on Security and Cryptography for Networks*, 2008, pp. 375–391.

[23] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in *In Theory of Cryptography Conference*, 2008, pp. 356–374.

[24] S. Jarecki and V. Shmatikov, "Efficient two-party secure computation on committed inputs," in *EUROCRYPT 07*, 2007, pp. 97–114.

Copyright (c) IARIA, 2011 ISBN:978-1-61208-113-7