Attribute-Based Online/Offline Encryption in Smart Grid

Zhiwei Wang, Feng Chen, Aidong Xia
School of Computer Science
Nanjing University of Posts and Telecommunications
Nanjing, P.R.China 210023
Email: zhwwang@njupt.edu.cn

***Abstract*—A smart grid is a modernized electrical grid that uses distribution networks to deliver electricity. It aims to gather and act on information, such as information about the behaviors of grid entities, in an automated fashion to improve the efficiency, security and reliability. It is important that the sensitive information should be shared securely among the grid entities. In smart grid, smart devices (e.g., smart meters) usually have limited computational capability. In this paper, we propose an online/offline attribute based encryption (ABE) scheme based J.Hur's ABE scheme with hidden policy. In our scheme, the advantages of J.Hur's scheme are kept. Thus, the data privacy and policy privacy are all preserved well. The computational overhead of encryptors are reduced by splitting the computation for encryption algorithm into two phases: online/offline. Most of the laborious decryption operations are delegated to the offline phase. The online phase can then rapidly assemble an ABE ciphertext when the message and the attribute control policy become known.**

I. Introduction

Smart grid generally refers to a class of technology people are using to bring utility electricity delivery systems into the 21st century, using intelligent transmission and distribution networks. The reliability, security and efficiency of smart grid are made possible by two-way communication technology and computer processing. Smart grid should bring together manufacturers, consumers, energy providers, and regulators to develop "interoperable standards." The number of applications that can be used on the smart grid once the data communications technology is deployed is growing as fast as inventive companies can create and produce them. In smart grid, many grid operators (e.g., enterprise and control center), suppliers(e.g.,electric utilities) and consumers with smart devices (e.g.,smart meters) participate in managing and controlling the grid, they need to share information with each other to control the grid safely. If we use the traditional PKI(X.509 certificates) to transmit the sensitive information among smart devices in smart grid, it requires too much time and processing to periodically update cryptographic keys or at least to revoke them. Thus, NIST didn't recommend to use X.509 certificate-based cryptography in smart grid [2].

Alternatively, attribute-based encryption (ABE) does not need the PKI certificate, but just depends on the recipients' ability to satisfy a policy. Thus, ABE could be a useful solution in smart grid. Especially, the Ciphertext-Policy ABE could be a promising scalable access control method in smart grid. In Ciphertext-Policy ABE, each ciphertext is associated with an access policy, and receiver's key with a set of attributes. One can decrypt iff the attribute set satisfies the access policy. As the smart grid system is becoming decentralized, and many system operators in different security domain participate in the system, the Ciphertext-Policy ABE could be a promising alternative in smart grid, compared with other traditional cryptographic primitives.

In smart grid, we found that not only the sensitive data should be encrypted, but also the policies should be hidden. Some grid operators such as electric utilities competing with each other might not be comfortable to disclose their policies to other competitors, since these policies may directly contain private information. If some access policies of electric utilities are disclosed, then it will be result in negative publicity, or loss of market revenue. Thus, ABE scheme should hide access policies in smart grid. Some hidden policy ABE schemes have been proposed, such as [7],[9]. However, these schemes have disadvantages in efficiency and expressiveness. Recently, J.Hur [4] proposed an expressive hidden policy CP-ABE, which has four advantages:1) The access policy can be expressed with any arbitrary access formula. 2) Sensitive information and access policies are preserved well without any disclosure. 3) Computational cost of decryptor is greatly reduced by delegating most of the heavy pairing operations to the storage center. 4) The key escrow problem is also resolved.

Our motivation The security issues in smart grid are four folds: 1) Attack detection and resilience operations; 2)Security for network protocols; 3)Identification, authentication and access control 4) Information privacy of some grid operators. Our goal is the information privacy of smart meter, which is a big concern of smart grid security. As we discussed above, ABE with hidden policy is a good solution for the information privacy of smart meter. However, the resource of smart meter is very limited, and the computational cost of common ABE scheme is too heavy to deployed in a smart meter.

In this work, we want to solve the above problem by introducing methods for online/offline encryption based on J.Hur's ABE scheme with hidden policy[4]. By delegating most computational cost of encryption into an offline phase, the smart meter only need do lightweight computation in the online phase. The offline work will be done by the storage center[11], and the smart meter's battery consumption is also

978-1-4799-9964-4/15/$31.00 ©2015 IEEE

greatly reduced for only doing the online work. The storage center performs the offline work, and sends the intermediate ciphertexts to a smart meter such that the smart meter can form ABE ciphertexts rapidly.

Related works Even, Goldreich and Micali first used online/offline method to the cryptographic primitives[8], and they proposed a notion of online/offline signature. After then, Shamir and Tauman presented a general method for constructing the online/offline signature by using chameleon hash functions. For the online/offline signature, the signing algorithm is divided into two phase. Most of laborious computation will be done in the offline phase without knowing the message to be signed. later, when the signer learns the message, he can sign it quickly. However, no online/offline schemes have been proposed after two decades, since the encryption schemes are not separable, for example, RSA encryption, or separating the encryption schemes into online/offline parts is very trivial, such as ElGamal encryption.

Until 2008, Fuchun et al. [6] proposed the first online/offline encryption scheme in identity system. They supposed that there are some sensitive data stored in a smart device, which has limited computation power. In order to send the sensitive date to a receiver in a secure way, it should be encrypted by using the receiver's identity. A distinctive advantage of ID-based systems is that any string which denotes the user uniquely can be used as the public key and potentially a large number of identities are supported. To ensure timely delivery, part of the encryption process could be performed prior to knowing the real data to be delivered and the public key (ID) of the receiver. The great challenge is that the receivers ID must be known for pre-computation, and the previous IBE schemes do not accommodate this feature. However, Fuchun et al. did not directly tackle this challenge, and their scheme can be carried out without knowing the identity of the receiver. After then, Liu et al. [5] presented an efficient ID-based online/offline encryption scheme, which solved the problem that it does not require the knowledge of the real data or the receivers identity in the offline phase. In 2013, Wang et al. [10] proposed an ID-based online/offline encryption scheme which can be proved sure in the standard model.

In many application scenario, it requires to distribute these encrypted data to a specific set of users. However, the traditional cryptosystems, e.g., PKI, ID-based cryptosystem, cannot do it, since the ciphertext size and computational cost of encryption/decryption algorithms are linear with the number of receivers. For this reason, Sahai and Waters[1] firstly proposed the concept of attribute-based encryption. In attribute-based encryption, ciphertexts and keys are associated with sets of attributes and access structure over attributes. Only when the attributes of the ciphertext match those of the users' key, the corresponding ciphertext can be decrypted. However, it is very difficult to construct attribute-based online/offline encryption scheme due to the access structure. To the best of our knowledge, there is only one online/offline ABE scheme proposed by Hohenburger et al.[3], by using a method of "pooling" work done offline. In their system, ciphertext pieces for every attribute will be done continuously offline, and stored in a pool. When the encryption algorithm encrypts a message with a set S of attributes, it select $|S|$ pieces from the pool, and connects each other to a complete ciphertext. They call this as "connect and correct" approach.

Our contributions We design online/offline encryption method for J.Hur's hidden policy ABE scheme [4] to make it more compatible with smart grid. Our construction is mainly based on Hohenburger et al.'s "connect and correct" approach, however, the access structure in J.Hur's scheme is more complex than Hohenburger et al.'s CP-ABE scheme. We use modular division to add the correction factors. In this work, our contributions can be concluded as follows:

1) To the best of our knowledge, our scheme is the first online/offline ABE scheme with hidden policy. Although Hohenburger et al.'s scheme[3] is a online/offline ABE scheme, the access policy in their scheme is not hidden, and not suitable for the smart grid. The second difference between Hohenburger et al.'s scheme and our scheme is the access structure. Hohenburger et al.'s scheme is based on the Linear Secret-sharing Scheme (LSSS) which only support the monotonic access structure, while our scheme is based on the tree access structure.
2) We provide the chosen plaintext attack(CPA) secure model of online/offline ABE scheme with hidden policy. We proved our scheme is CPA secure under J.Hur's scheme[4]. That is to say, if our scheme can be broken, then J.Hur's scheme is not secure.
3) Compared with J.Hur's scheme[4], the online encryption cost of our scheme is greatly reduced, since the heavy encryption cost is outsourced to the storage center in the offline phase.

Organization The rest of the paper is organized as follows: Section 2 introduces some preliminaries related to our scheme. Section 3 provides the definition and security model of online/offline CP-ABE with hidden policy. The concrete scheme is proposed in Section 4. The security proof is presented in Section 5, and we conclude the paper in Section 6.

II. Preliminaries

In this section, we review the formal definition of access tree in [4]. Then, we briefly review the definition of bilinear map.

Attribute Tree: An access tree Υ has a root r and some branch nodes and leaf nodes. Each branch node x is associated with a threshold value k_x, which means that if x has num_x child nodes, then it is requires that $k_x \leq num_x$. x's every child node z is indexed from 1 to num_x. Each leaf node x is associated a single attribute, denoted as λ_x. $p(x)$ denotes x's parent.

Satisfying an Access Tree: Υ_x is a sub-tree of an access tree Υ, and x is Υ'_xs root. Let $\Upsilon_x(\gamma) = 1$ denote that an attribute set γ satisfies the access tree Υ_x. If x is a branch node, then $\Upsilon_x(\gamma) = 1$ when at least k_x child nodes z , $\Upsilon_z(\gamma) = 1$. If x is a leaf node, then $\Upsilon_x(\gamma) = 1$ when $\lambda_x \in \gamma$.

Bilinear Mapping: Let $\mathbf{G}_0$ and $\mathbf{G}_1$ be two groups of prime order p and g be generator of $\mathbf{G}_0$. The map $e : \mathbf{G}_0 \times \mathbf{G}_0 \rightarrow \mathbf{G}_1$ is said to be an admissible bilinear mapping if the following three conditions hold true:

- e is bilinear, i.e., $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbf{Z}_p$.
- e is non-degenerate, i.e., $e(g, g) \neq 1_{\mathbf{G}_1}$.
- e is efficiently computable.

III. Definition and security model

In this section, we define online/offline CP-ABE scheme with hidden policy, which consists of seven polynomial time algorithms. Then, we define the security model. Let $\mathbf{A}$ denote an access structure, and KGC denote key generation center. Let IT denote intermediate ciphertext, CT' denote partial ciphertext, and CT denote ciphertext.

Definition of online/offline CP-ABE scheme with hidden policy:

- **Setup**$(1^\lambda) \rightarrow (PK_K, MK_K), (PK_S, MK_S)$ This algorithm takes as input a security parameter λ, and outputs the public key and secret key pairs $(PK_K, MK_K), (PK_S, MK_S)$ for KGC and storage center respectively.
- **Extract**$(MK_K, S) \rightarrow SK$ The extract algorithm takes as input the secret key MK_K of KGC, and a set of attributes S. It outputs a private key SK associated with the attribute set S.
- **Offline.Encrypt**$(PK_K, PK_S) \rightarrow IT$ The offline encryption algorithm takes as input the public keys PK_K, PK_S, and outputs an intermediate ciphertext IT.
- **Online.Encrypt**$(PK_K, PK_S, IT, A) \rightarrow CT$ The online algorithm takes as input public keys PK_K, PK_S, an intermediate ciphertext IT and an access structure A. It produces a ciphertext CT such that only the decryptor possesses a set of attributes that satisfies the access structure can decrypt it.
- **GenToken**$(SK, \Lambda) \rightarrow TK_\Lambda$ This algorithm can generate a token TK_Λ for a set of attributes $\Lambda \subseteq S$.
- **PDecrypt**$(TK_\Lambda, CT) \rightarrow CT'$ This algorithm takes as input the token TK_Λ and the ciphertext CT. It outputs a partial ciphertext CT', if Λ satisfies the access policy of CT. However, the plain attributes in Λ are not compromised.
- **Decrypt**$(SK, CT') \rightarrow M$ This algorithm decrypts CT' by using the private key SK, and returns the message M.

Security model of online/offline CP-ABE scheme with hidden policy Let Π=(Setup, Extract, Offline.Encrypt, Online.Ecrypt, GenToken, PDcrypt, Decrypt) be an online/offline CP-ABE scheme with hidden policy (OO-CP-ABE-HP). We define CPA security model of Π by the game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ as follows.

Setup: The challenger $\mathcal{C}$ runs the Setup algorithm, and returns the public keys PK_K and PK_S to the adversary $\mathcal{A}$.

Phase 1: In this phase, $\mathcal{A}$ can only make extract queries adaptively, since it is in the CPA-secure model. $\mathcal{C}$ firstly initializes an empty table T, and an empty set D and an integer counter $j = 0$. When $\mathcal{A}$ makes an extract query on an attribute set S, if the entry (j, S, SK) exists in T, then $\mathcal{C}$ sets $D = D \cup S$ and sends SK to $\mathcal{A}$. Otherwise, $\mathcal{C}$ sets $j = j + 1$ and runs the Extract algorithm. Then, $\mathcal{C}$ sends SK to $\mathcal{A}$, and keeps the entry (j, S, SK) in T.

Cha: $\mathcal{A}$ provides a challenge access structure A^* such that for all $S \in D$, $S \notin A^*$. Then, $\mathcal{C}$ runs the $Offline.Ecrypt$ and $Online.Ecrypt$ algorithms to get CT^*. It randomly selects a bit b. If $b = 0$, then $\mathcal{C}$ sends CT^* to $\mathcal{A}$, else if $b = 1$, then $\mathcal{C}$ sends a random number R to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ repeats the extract query as phase 1. However, it cannot make any query on S such that $S \in A^*$.

Guess: $\mathcal{A}$ outputs a guess b' of b. $\mathcal{A}$ wins the game iff $b = b'$.

Definition 3.1 (OO-CP-ABE-HP Security). *An OO-CP-ABE-HP scheme is CPA secure if all probabilistic polynomial time adversaries $\mathcal{A}$ can win the above game (OO-CP-ABE-HP-Game) with a negligible probability:*

$$Pr(OO{-}CP{-}ABE{-}HP{-}Game_{\mathcal{A},\Pi} = 1) \leq \frac{1}{2} + negl(\lambda).$$

IV. Proposed scheme

A. Construction

Let U denote an universe set of attributes, and $|U| = P$. Our scheme consists of seven algorithms which are designed as follows:

Setup. This algorithm is the same as J.Hur's scheme[4]. KGC chooses two hash functions: $H : \{0,1\}^* \rightarrow \mathbf{G}_0$, $H_1 : \mathbf{G}_1 \rightarrow \{0,1\}^{\log p}$. Then, it chooses two random exponents $\alpha, \beta \in \mathbf{Z}_p$, and computes the public/secret key pair as $(PK_K = (h = g^\beta, e(g,g)^\alpha), MK_K = (\beta, g^\alpha))$. The storage center selects a random number $\gamma \in \mathbf{Z}_p$, and computes the public/secret key pair as $(PK_S = g^\gamma, MK_S = H(ID_S)^\gamma)$, where ID_S is the identity of storage center.

Extract. This algorithm is also the same as J.Hur's scheme[4]. When KGC generates a private key for a user u_t on an attributes set S, it firstly chooses a random number $r_t \in \mathbf{Z}_p$ for u_t. Then, it selects random $r_j \in \mathbf{Z}_p$ for each attributes $j \in S$. Finally, it outputs u_t's private key as $SK_u = (D = g^{\frac{\alpha + r_t}{\beta}}, \forall j \in S : D_j = g^{r_t} \cdot H(j)^{r_j}, D'_j = g^{r_j}, D''_j = H(j)^\beta)$.

Offline.Encrypt. The offline.Encrypt algorithm only takes as input the public keys PK_K, PK_S. It firstly chooses two random exponent $a, x \in \mathbf{Z}_p$, and computes $K_S = e((g^\gamma)^a, H(ID_S))$, $\tilde{C}' = K_S \cdot e(g,g)^{\alpha x}$, $C' = h^x$. Secondly, for $j = 1$ to P, it chooses random $x_j \in \mathbf{Z}_p$ and computes $s_j = e((g^\beta)^a, H(\lambda_j))$, $H_1(s_j)$. Then, it computes $C_{j1} = g^{x_j}, C_{j2} = H(\lambda_j)^{x_j}$, where $\lambda_j \in U$. The intermediate ciphertext IT is

$$(x, g^a, \tilde{C}', C', \{x_j, C_{j1}, C_{j2}\}_{j \in [1,P]}).$$

Online.Encrypt. When the encryptor wants to encrypt a message M over a tree access structure Υ, it firstly chooses

a polynomial q_x for each node x in tree Υ in a top-down manner. The degree of q_x is $d_x = k_x - 1$, where k_x is the threshold value. For the root node r, it chooses a random exponent $s \in \mathbf{Z}_p$, and sets $q_R(0) = s$. For other branch node x, it sets $q_x(0) = q_{p(x)}(index(x))$. Let Y be the set of leaf nodes in Υ, and $|Y| = l$. It computes $t = \frac{s}{x} modp$, $\tilde{C} = \tilde{C}' \cdot M$. For $j = 1$ to l, it computes $C_{j3} = \frac{q_y(0)}{x_j} modp, \quad \forall y \in Y$. The ciphertext is $(t, g^a, \tilde{C}, C', \{C_{j1}, C_{j2}, C_{j3}\}_{j\in[1,l]})$.

GenToken. This algorithm is the same as J.Hur's scheme[4], which takes as input an attribute set $\Lambda \subseteq S$. For all $j \in \Lambda$, it computes $s_j = e(g^a, D_j'') = e(g^a, H(j)^\beta)$. Then, it selects a random $\tau \in \mathbf{Z}_p$, outputs the token as $TK_{\Lambda,u_t} = (\forall j \in \Lambda : I_j = H_1(s_j), (D_j)^\tau, (D_j')^\tau)$. Here, I_j can be seen as an index for the obfuscated attribute j.

PDecrypt. This algorithm takes as input the token TK_{Λ,u_t} and ciphertext CT. It firstly checks if the token satisfies the access policy by using I_j and $H_1(s_y)$ without compromising the plain attributes. Then, if j is a leaf node, and $H_1(s_j) \in \Theta$ where Θ is a set of all indices I_j associated with the token, it computes

$$\begin{aligned} & DecryptNode(CT, TK_{\Lambda,u_t}, j) \\ = & \frac{e((D_x)^\tau, (C_{j1})^{C_{j3}})}{e((D_x')^\tau, (C_{j2})^{C_{j3}})} \\ = & \frac{e((g^{r_t} \cdot H(\lambda_j)^{r_j})^\tau, (g^{x_j})^{q_j(0)/x_j})}{e((g^{r_j})^\tau, (H(\lambda_j)^{x_j})^{q_j(0)/x_j})} \\ = & e(g,g)^{r_t \tau q_j(0)} \end{aligned}$$

If $H_1(s_j) \notin \Theta$, the algorithm outputs failure. When j is a non-leaf node, the algorithm performs in a recursive way by using the Lagrange interpolation formula to obtain $e(g,g)^{r_t \tau q_j(0)}$. Finally, if tree Υ is satisfied by the token, it can get $A = DecryptNode(CT, TK_{\Lambda,u_t}, R) = e(g,g)^{r_t \tau s}$. Then, it computes $K_S = e(g^a, MK_S) = e(g^a, H(ID_S)^\gamma)$ and $\hat{C} = \tilde{C}/K_S = M \cdot e(g,g)^{\alpha x}$. The partial ciphertext is $CT' = (\hat{C}, C = C'^t = (h^x)^{s/x} = h^s, t, A)$.

Decrypt. This algorithm takes as input CT' and the private key of user, and computes

$$\begin{aligned} & (\hat{C}^t / e(C, D) / A^{1/\tau})^{1/t} \\ = & (M^t e(g,g)^{\alpha s} / e(g^{\beta s}, g^{(\alpha + r_t)/\beta}) / e(g,g)^{r_t s})^{1/t} \\ = & M. \end{aligned}$$

B. Comparison

We use $\mathcal{HW}$ and $\mathcal{J}.\mathcal{H}$ to denote the ABE schemes proposed by Hohenburger et al.[3] and J.Hur [4] respectively. We assume that $|\mathbf{G}_0| = 160$ bits,$|p| = 160$ bits, $|\mathbf{G}_1| = 1024$ bits , the size of universe set of attributes $P = 1024$, the size of attributes set $l = 160$, and the length of the plaintext $n = 1024$ bits for the following comparison. Let MUL and DIV denote the multiplication and division in $\mathbf{Z}_p$ respectively, $E_{\mathbf{G}_0}$, $E_{\mathbf{G}_1}$ denote the exponentiations in groups $\mathbf{G}_0$ and $\mathbf{G}_1$ respectively, $ME_{\mathbf{G}_0}$ dennote the multi-exponentiation in $\mathbf{G}_0$ (which cost about 1.3 times more than a single exponentiation respectively), and $\mathbf{P}$ denote the pairing over $\mathbf{G}_0$. The table 1 presents the comparison of computation cost and size.

	$\mathcal{HW}$	$\mathcal{J}.\mathcal{H}$	Our scheme
Offline computation	$1\mathbf{P}$ + $1025E_{\mathbf{G}_0}$ + $1E_{\mathbf{G}_1}$+$1024ME_{\mathbf{G}_0}$	no offline	$1026\mathbf{P}$+$1028E_{\mathbf{G}_0}$ +$1E_{\mathbf{G}_1}$
Online computation	$160MUL$	$162\mathbf{P}$+$482E_{\mathbf{G}_0}$ +$1E_{\mathbf{G}_1}$	$161DIV$
Offline storage (intermediate ciphertext)	655.5kbits	no offline	493kbits
Ciphertext length	76.8kbits	52.4kbits	78.1kbits
Decryption computation	$480\mathbf{P}$+$160E_{\mathbf{G}_0}$ +$160E_{\mathbf{G}_1}$	$1\mathbf{P}$+$1E_{\mathbf{G}_1}$	$1\mathbf{P}$+$2E_{\mathbf{G}_1}$
Security level	CPA	CPA	CPA
Hidden policy	no	Yes	Yes

TABLE I
COMPARISON OF COMPUTATION COST AND SIZE

From Table 1., it can be seen that the online computational cost of our scheme is almost the same as Hohenbuger et al.'s scheme, while the offline cost of ours is much more heavy than theirs. However, the offline phase is carried by a powerful storage center, we only need to concern with the online phase. Compared with J.Hur's scheme, the online computational cost of our scheme is greatly reduced, since the heavy computational operations are outsourced to the storage center in the offline phase. Thus, for this distinctive feature, our scheme can be implemented on the smart devices. The decryption cost of our scheme is also very light, since most of the decryption cost is also outsourced to the storage center like J.Hur's scheme.

Although the ciphertext length of our scheme is a bit larger than Hohenbuger et al.'s scheme, the storage cost of ours is better than theirs due to the smaller size of intermediate ciphertext. The security level of the three schemes in Table 1 is the same (CPA secure), so how to construct an efficient chosen ciphertext attacke (CCA) secure online/offline ABE scheme is still a challenge.

V. SECURITY PROOF

Theorem 5.1 *The above online/offline CP-ABE scheme with hidden policy is selectively CPA-secure on the condition that J.Hur's scheme[4] is a selective CPA-secure scheme.*

Proof. To prove this theorem, we will prove that if some PPT adversary $\mathcal{A}$ can win the above OO-CP-ABE-HP-Game with non-negligible probability, then a PPT simulator $\mathcal{B}$ can break the selective CPA-secure of the J.Hur's scheme[4]. $\mathcal{B}$ will act as the challenger interacts with $\mathcal{A}$ in OO-CP-ABE-HP-Game.

Initialization. $\mathcal{A}$ sends a tree access structure Υ^* to $\mathcal{B}$. Then, $\mathcal{B}$ gives it to the challenger of J.Hur's scheme.

Setup. $\mathcal{B}$ receives the public keys (PK_K, PK_S) from the challenger, and sends it to $\mathcal{A}$.

Phase1. $\mathcal{A}$'s extract queries are passed to the challenger to get the private key.

Challenge. $\mathcal{B}$ selects two distinct and random message $m_b, b \in \{0,1\}$, and sends to the challenger, and receives the response

as $CT^* = (\Upsilon^*, \tilde{C} = m_b \cdot K_S \cdot e(g,g)^{\alpha s}, C = h^s, \forall j \in Y : C_{j1} = g^{q_j(0)}, C_{j2} = H(\lambda_j)^{q_j(0)})$. Then, $\mathcal{B}$ selects random blind values $z_1, \cdots, z_l \in \mathbf{Z}_p$ and computes the ciphertext of OO-CP-ABE-HP scheme as follows:

$$\begin{aligned} C^*_{j1} &= (C_{j1})^{1/z_j} \\ C^*_{j2} &= (C_{j2})^{1/z_j} \\ C^*_{j3} &= z_j \\ t^* &= 1 \end{aligned}$$

Then, $\mathcal{B}$ sends $(\Upsilon^*, t^*, \tilde{C}, C, \forall j \in Y : C^*_{j1}, C^*_{j2}, C^*_{j3})$ to $\mathcal{A}$, which is a correctly formed ciphertext.

Phase 2. This phase is the same as Phase 1.

Guess. Finally, $\mathcal{A}$ outputs a bit b' to $\mathcal{B}$, and $\mathcal{B}$ also outputs b'. The distribution for $\mathcal{A}$ is perfect. If $\mathcal{A}$ has a non-negligible probability to win the OO-CP-ABE-HP-Game, then $\mathcal{B}$ also can breaks the J.Hur's scheme with the same probability.

VI. CONCLUSION

In this paper, we present an online/offline scheme based on J.Hur's ABE scheme with hidden policy. Our scheme keeps the advantages of J.Hur's ABE scheme, and divides the encryption algorithm into two phases, online and offline. In smart grid, the laborious offline work will be done by the storage center which has high computational capability. Then, it sends the intermediate ciphertext to the smart devices (e.g., smart meters) which usually have limited computational resource. Later in the online phase, the smart meters will get the measured data, and set the access policy. Given the offline work, the smart meters should be able to encrypt data quickly.

ACKNOWLEDGMENTS.

This research is partially supported by the National Natural Science Foundation of China under Grant No.61373006, and the Jiangsu Overseas Research and Training Program for University of Prominent Young and Middle-aged Teachers and Presidents.

REFERENCES

[1] S. A and W. B. Fuzzy identity based encryption. EUROCRYPT05, LNCS 3494,, pages 457C473, 2005.

[2] T. C. S. C. T. Group. Smart grid cyber security strategy and requirements. NIST Technical Report Draft, NISTIR 7628, 2009.

[3] S. Hohenberger and B. Waters. Online/offline attribute-based encryption. Public-Key Cryptography PKC 2014, pages LNCS Volume 8383, 2014,pp 293C310, 2014.

[4] J.Hur. Attribute-based secure data sharing with hidden policies in smart grid. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 24(11):2171C2180, 2013.

[5] J. K. Liu and J. Zhou. An efficient identity-based online/offline encryption scheme. In ACNS, pages 156C167, 2009.

[6] F. G. Y. Mu. and Z. Chen. Identity-based online/offline encryption. In Financial Cryptography, pages 247C261, 2008.

[7] K. R. S. Yu and W. Lou. Attribute-based content distribution with hidden policy. Proc. Workshop Secure Network Protocols, pages 39C44, 2008.

[8] O. G. Shimon Even and S. Micali. Online/offline digital signatures. J. Cryptology, 9(1):35C67, 1996.

[9] K. Y. T. Nishide and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structure. Proc. Sixth Intl Conf. Applied Cryptography and Network Security (ACNS 08), pages 111C129, 2008.

[10] Z. Wang and W. Chen. An id-based online/offline signature scheme without random oracles for wireless sensor networks. Personal and Ubiquitous Computing, pages 17(5): 837-841, 2013.

[11] Zhiwei Wang, Guozi Sun and Danwei Chen. A new definition of homomorphic signature for identity management in mobile cloud computing. J. Comput. Syst. Sci., 80(3):546-553, 2014