ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

An Extremely Scalable Input Pre-Distribution Proposal on Behalf of Wireless Sensor Networks

E.Ramesh[1], K.Tulasi[2]

Student, Dept of Computer Science and Engineering, Chadalawada Ramanamma Engineering College, Tirupathi, India[1]

Associate Professor, Dept of Computer Science and Engineering, Chadalawada Ramanamma Engineering College, Tirupathi, India[2]

ABSTRACT: An effective Position-based Opportunistic Course-plotting (POR) technique which uses the stateless property of regional redirecting and the passed on features of wi-fi technique. When a information package is sent out, some of the next door next door neighbor nodes that have overheard the transferring will provide as delivering candidates, and take turn to ahead the package if it is not relayed by the particular best forwarder within a certain time frame. By using such in-the-air back-up, connections is handled without being disrupted. The additional latency experienced by local direction recovery is reduced and the duplicate delivering due to package redouble is also reduced. In the case of connections gap, a Unique Destination-based Gap Managing (VDVH) strategy is further recommended to work together with POR. Both theoretical research and simulation outcomes show that POR achieves excellent efficiency even under excellent node versatility with appropriate cost and the new gap handling strategy also works well.A new scalable key control strategy for WSNs which provides a excellent secured relationship protection. For this purpose, we make use of the unital design. We show that the primary implementing from unitals to key pre-distribution allows us to achieve excellent program scalability. However, this simple implementing does not guarantee a higher key talking about probability. Therefore, we suggest an enhanced unital-based key pre-distribution strategy providing excellent network scalability and excellent key talking about probability roughly lower enclosed. We perform approximated research and designs and evaluate our solution to those of present methods for different requirements such as storage area space cost, program scalability, program relationship, and average secured direction length and program resiliency. Our outcomes show that the recommended strategy improves the program scalability while providing high secured relationship coverage and overall enhanced efficiency. Moreover, for an equivalent program size, our solution decreases significantly the storage area space cost compared to those of present alternatives.

KEY WORDS: Geographical routing, VDVH, PRO, unital-based key, Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

1. INTRODUCTION

A novel Position-based Opportunistic Redirecting (POR) method is suggested, in which several sending applicants storage cache the bundle that has been obtained using MAC interception. If the best forwarder does not ahead the bundle in certain time spots, suboptimal applicants will take convert to a head the bundle according to a regionally established purchase. In this way, provided that one of the applicants is successful in getting and sending the bundle, the information transmitting will not be disturbed. Prospective multipath are utilized on the fly on a per packet foundation, major POR's outstanding sturdiness. The primary efforts of this document can be described as follows: We recommend a position-based opportunistic redirecting procedure which can be implemented without complicated adjustment to MAC method and accomplish several wedding celebration without dropping the benefit of accident prevention offered by 802.11.The idea of in-the-air back-up considerably increases the sturdiness of the redirecting method and decreases the latency and copy sending due to local path repair. In the case of interaction gap, we recommend a Exclusive Destination-based Gap Managing (VDVH) plan in which the advantages of selfish sending (e.g., huge enhancement per hop) and opportunistic redirecting can still be obtained while handling interaction voids. We assess the effect of node flexibility on bundle distribution and describe the enhancement introduced about by the contribution of sending applicants. The expense of POR with focus on shield utilization and data transfer useage intake due to sending candidates' copy sending is also mentioned. Through research, we determine that due to the selection of sending area and the properly designed replication restriction plan, POR's efficiency gain can be carried out at little expense cost. Lastly, we assess the efficiency of POR through comprehensive models and confirm that POR accomplishes excellent efficiency in the face of great node flexibility while the expense is appropriate. In this perform, our aim is to deal with the scalability issue without degrading the other system efficiency analytics. For this objective, we focus on the style of a plan which guarantees a excellent protected protection of comprehensive systems with a low key storage expense and a excellent system resiliency. To this end, we make use, of the unital style idea for efficient WSN key pre-distribution. Indeed, we recommend a innocent applying from unital style to key pre-distribution and we show through systematic research that it allows to accomplish great scalability. Nonetheless, this innocent applying does not assurance a higher key discussing possibility. Therefore, we recommend an improved unital based key pre-distribution plan that preserves a excellent key discussing possibility while improving the system scalability. An initial perform and few conversations were offered in the efforts of our perform are given next: evaluation the primary state of the art of symmetrical key management techniques for WSNs that we categorize into two categories: probabilistic techniques and deterministic ones. We further define the classification into sub-categories in accordance with the real concepts and methods used in key come back and agreement. We present the use of unital style concept in key pre distribution for WSNs. We display that the primary applying from unitals to key pre-distribution gives beginning to extremely scalable plan while offering low possibility of discussing typical important factors. We recommend an improved unital-based key pre-distribution plan to be able to improve the system scalability while keeping a good key discussing possibility. We confirm that sufficient option of our remedy parameter should assurance high key discussing possibility roughly reduced surrounded by $1-e^{-1}$ while ensuring high system scalability. We analyze and compare our new approach against main existing schemes, with respect to different criteria: storage space expense, power intake, system scalability, protected connectivity coverage, average protected path length and system resiliency. The obtained results display that our remedy enhances the system scalability while providing good overall system activities. Moreover, we display that at equal system size, our remedy reduces significantly the storage space expense and thereby the power intake.

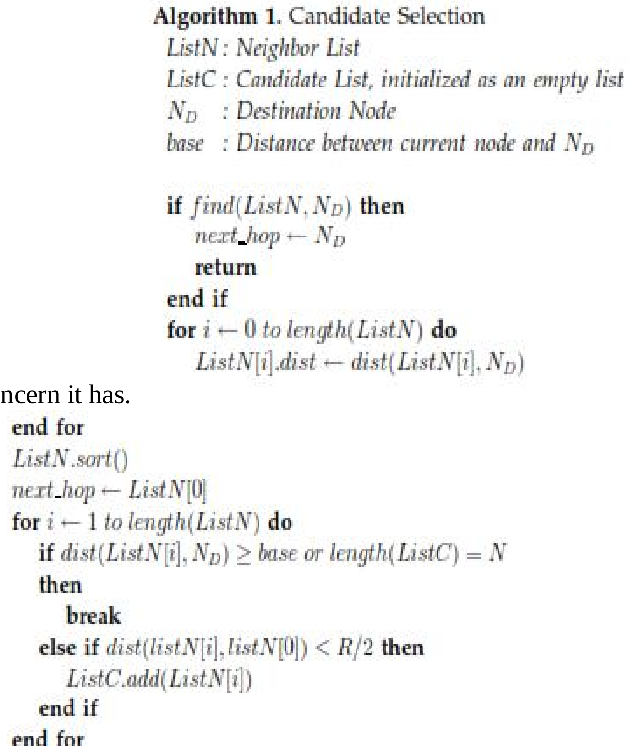
II. POSITION-BASED OPPORTUNISTIC ROUTING

2.1 Overview

The design of POR is depending on geographical redirecting and opportunistic sending. The nodes are believed to be aware of their own place and the roles of their immediate others who live nearby. Community place details can be interchanged using one-hop shining example or piggyback in the details packet's headlines. While for the place of the place, we believe that a place signing up and search assistance which charts node details to places is available just as in . It could be noticed using many types of place assistance. In our situation, some effective and effective way is also available. For example, the place of the place could be passed on by low bit rate but long variety receivers, which can be applied as regular shining example, as well as by responses when asked for by the resource. When a resource node wants to deliver a bundle, it gets the place of the place first and then connects it to the bundle headlines. Due to the place node's activity, the multiple hop direction may diverge from the true place of the ultimate place and a bundle would be decreased even if it has already been provided into the area of the place. To deal with such issue, additional examine for the place node is presented. At each hop, the node that sends the bundle will examine its next door neighbor list to see whether the place is within its transmitting variety. If yes, the bundle will be straight sent to the place, just like the place location forecast plan described in. By executing such recognition examine before selfish sending depending on place details, the impact of the direction divergence can be very much reduced. In traditional opportunistic sending, to have a bundle obtained by several applicants, either IP passed on or an incorporation of redirecting and MAC method is implemented. The former is vulnerable to MAC accident because of the deficiency of accident prevention assistance for passed on bundle in current 802.11, while the latter needs complicated synchronization and is not easy to be applied. In POR, we use identical plan as the MAC multicast method described in. The bundle is passed on as unicast (the best forwarder which makes the biggest positive improvement toward the place is set as the next hop) in IP part and several wedding celebration is obtained using MAC interception. The use of RTS/CTS/DATA/ACK considerably decreases the accident and all the nodes within the transmitting variety of the emailer can eavesdrop on the bundle efficiently with higher possibility due to method booking.

2.2 Selection and Prioritization of Forwarding Candidates

One of the key issues in POR is the choice and prioritization of sending applicants. Only the nodes in the sending place would get the opportunity to be back-up nodes. The sending place is identified by the emailer and the next hop node. A node in the sending place meets the following two conditions: 1) it creates beneficial improvement toward the destination; and 2) its variety to the next hop node should not surpass 50 percent of the transmitting variety of a wi-fi node (i.e., R=2) so that preferably all the sending applicants can listen to from one another. In Fig. 1, the place surrounded by the strong bend is identified as the sending place. The nodes in this place, besides node A (i.e., nodes B, C), are prospective applicants. According to the needed variety of back-up nodes, some (maybe all) of them will be chosen as sending applicants. The concern of a sending applicant is made the decision by its variety to the location. The closer it is to the location, the greater concern it will get. When a node delivers or delivers a bundle, it chooses the next hop forwarder as well as the sending applicants among its others who live nearby. The next hop and the applicant record consist of the forwarder record. Criteria 1 reveal the process to choose and focus on the forwarder record. The applicant record will be connected to the bundle headlines and modified hop by hop. Only the nodes specified in the applicant record will act as sending applicants. The reduced the catalog of the node in the applicant record, the greater concern it has.



```
Algorithm 1. Candidate Selection
  $ListN$ : Neighbor List
  $ListC$ : Candidate List, initialized as an empty list
  $N_D$   : Destination Node
  $base$  : Distance between current node and $N_D$

  if $find(ListN, N_D)$ then
      $next\_hop \leftarrow N_D$
      return
  end if
  for $i \leftarrow 0$ to $length(ListN)$ do
      $ListN[i].dist \leftarrow dist(ListN[i], N_D)$
  end for
  $ListN.sort()$
  $next\_hop \leftarrow ListN[0]$
  for $i \leftarrow 1$ to $length(ListN)$ do
      if $dist(ListN[i], N_D) \geq base$ or $length(ListC) = N$
      then
          break
      else if $dist(listN[i], listN[0]) < R/2$ then
          $ListC.add(ListN[i])$
      end if
  end for
```

Every node preserves a sending desk for the packages of each circulation (identified as source-destination pair) that it has sent or submitted. Before determining a new forwarder record, it looks up the sending table; an example is shown in Table 1, to examine if a real product for that location is still available. The sending desk is designed during details bundle signals and its servicing is much simpler than a redirecting desk. It can be seen as a trade-off between performance and scalability. As the organization of the sending desk only relies on regional details, it requires much less a chance to be designed.

2.3 Restriction on Possible Copy Relaying

Due to accident and nodes' activity, some sending applicants may don't succeed to get the bundle submitted by the next hop node or greater concern applicant, so that a certain quantity of duplicate sending would happen. If the sending applicant assumes the same sending situation as the next hop node, which indicates it also determines an applicant record, then in the most severe, the reproduction place of a bundle will protect the whole group including the location as the middle and the range can be as huge as the range between the resource and the location.

III. SCHEME DESCRIPTION

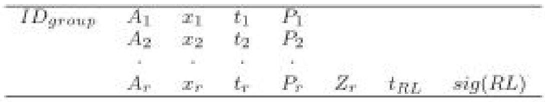
This section describes the details of Mona including system initialization, customer registration, customer revocation, computer file generation, computer file deletion

3.1 System Initialization

The group manager takes charge of system initialization as follows:

Generating a bilinear map group system $S = (q, G_1, G_2, e(\cdot,\cdot))$.

TABLE 1
Revocation List



ID_{group}	A_1	x_1	t_1	P_1		
	A_2	x_2	t_2	P_2		
	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
	A_r	x_r	t_r	P_r	Z_r	t_{RL}	$sig(RL)$

- Selecting two random elements $H, H_0 \in G_1$ along with two random numbers $\xi_1, \xi_2 \in Z_q^*$, and computing $U = \xi_1^{-1} H$ and $V = \xi_2^{-1} H \in G_1$ such that $\xi_1 \cdot U = \xi_2 \cdot V = H$. In addition, the group manager computes $H_1 = \xi_1 H_0$ and $H_2 = \xi_2 H_0 \in G_1$.
- Randomly choosing two elements P, $G \in G_1$ and a number $\gamma \in Z_q^*$, and computing $W = \gamma \cdot P, Y = \gamma \cdot G$ and $Z = e(G, P)$, respectively.
- Publishing the system parameters including (S, $H, H_0, H_1, H_2, U, V, W, Y, Z, f, f_1, Enc())$, where f is a one-way hash function: $\{0,1\}^* \rightarrow Z_q^*$; f1 is hash function $\{0,1\}^* \rightarrow G_1$; and $Enc_k()$ is a secure symmetric encryption algorithm with secret key k.

In the end, the parameter $(\gamma, \xi_1, \xi_2, G)$ will be kept secretes the master key of the group manager.

3.2 User Registration

For the registration of user i with identity ID, the group manager randomly selects a number $x_i \in Z_q^*$ and computes A_i, B_i as the following equation:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1. \end{cases} \qquad (1)$$

Then, the group manager adds (A_i, x_i, ID_i) into the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key (x_i, A_i, B_i), which will be used for group signature generation and file decryption.

3.3 User Revocation

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. As illustrated in Table 1, the revocation list is characterized by a series of the stamps $(t_1 < t_2 <, ..., t_r)$. Let ID_{group} ' denote the group identity. The tuple (A_i, x_i, t_i) represents that user i with the partial private key (A_i, x_i) is revoked at time t_i. $P_1, P_2, ..., P_r$ and Z_r are calculated by the group manager with the private secret γ as follows:

$$\begin{cases} P_1 = \frac{1}{\gamma + x_1} \cdot P \in G_1 \\ P_2 = \frac{1}{(\gamma + x_1)(\gamma + x_2)} \cdot P \in G_1 \\ P_r = \frac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)} \cdot P \in G_1 \\ Z_r = Z^{\frac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)}} \in G_2. \end{cases} \quad (2)$$

Inspired by the proven response procedure in [19], to assurance that customers acquire the newest edition of the cancellation record, we let the team manger upgrade the cancellation record each day even no customer has being suspended in the day. In other terms, the others can confirm the quality of the cancellation record from the included current date .In addition; the cancellation record is surrounded by a trademark sig(R, L) to announce its credibility. The trademark is produced by the team administrator with the BLS trademark criteria [20], i.e., $sig(RL) = \gamma f_1(RL)$. .Finally, the group manager migrates the revocation list into the cloud for public usage.

3.4 File Generation

To store and share a data file in the cloud, a group member performs the following operations:

1. Getting the revocation list from the cloud. In this step, the member sends the group identity ID_{group} as a request to the cloud. Then, the cloud responds the revocation list RL to the member.
2. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh. Second, verifying the contained signature sig(RL) by the equation $e(W, f_1(RL)) = e(P, sig(RL))$. If the revocation list is invalid, the data owner stops this scheme.
3. Encrypting the data file M. This encryption process can be divided into two cases according to the revocation list.

3.5 File Deletion

File stored in the cloud can be deleted by either the group boss or the data owner (i.e., the member who uploaded the file into the server). To delete a file ID_{data}, the group manager computes a signature $\gamma f_1(ID_{data})$ and sends the signature along with ID_{data} to the cloud. The cloud will delete the file if the equation $e(\gamma f_1(ID_{data}), P) = e(W, f_1(ID_{data}))$ holds.

Algorithm (1).

Signature Generation Input: Private key (A, x) system parameter (P, U, V, H, W) and data M. Output: Generate a valid group signature on M.

```
Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
Computes the following values
    $T_1 = \alpha \cdot U$
    $T_2 = \beta \cdot V$
    $T_3 = A_i + (\alpha + \beta) \cdot H$
    $R_1 = r_\alpha \cdot U$
    $R_2 = r_\beta \cdot V$
    $R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}}$
    $R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U$
    $R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V$
Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
Construct the following numbers
    $s_\alpha = r_\alpha + c\alpha$
    $s_\beta = r_\beta + c\beta$
    $s_x = r_x + cx$ .
    $s_{\delta_1} = r_{\delta_1} + c\delta_1$
    $s_{\delta_2} = r_{\delta_2} + c\delta_2$
Return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
```

End.

Algorithm(2). Signature Verification

Input:System parameter (P, U, V, H, W), M and a signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
Output: True or False.

```
begin
Compute the following values

$\begin{cases} \tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R}_2 = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R}_3 = (\frac{e(T_3, W)}{e(P, P)})^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta} \\ \qquad e(H, P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases}$
if $c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$

Return True
else
Return False
End
```

Algorithm (3). Revocation Verification

Input: System parameter (H_0, H_1, H_2), a group signature σ, and a set of revocation keys $A_1, ..., A_r$ Output: Valid or Invalid.

```
Begin
 set $temp = e(T_1, H_1) e(T_2, H_2)$
 for $i = 1$ to $n$
  if $e(T_3 - A_i, H_0) = temp$
  Return Valid
  end if
  end for
  Return Invalid
  End
```

IV. PROPOSED CP-ABE SCHEME WITH VERIFIABLE OUTSOURCED DECRYPTION

In this section, we first propose a new CP-ABE scheme utilizing Waters' CP-ABE scheme [4], which is proven to be selectively CPA-secure. Then, based on the scheme, we propose a CP-ABE scheme with outsourced decryption and prove that it is selectively CPA-secure and verifiable in the standard model.

A. New CP-ABE Scheme

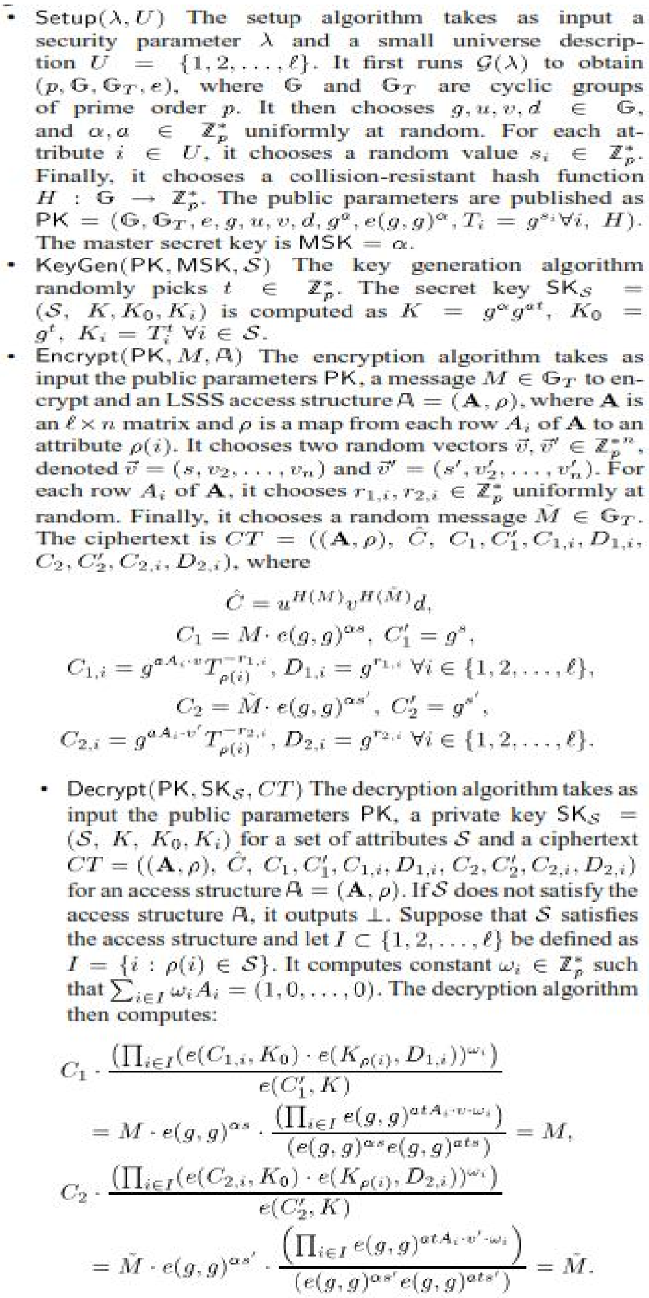
Before presenting our new CP-ABE scheme, we give some intuitions of our construction. Based on Waters' CP-ABE scheme [4], we add to the ciphertext the encryption of an extra random message and a checksum value, which is computed with this random message and the actual plaintext. We regard this checksum value as a commitment of the actual plaintext, which can be used to check if the transformation is done correctly in our CP-ABE Scheme with verifiable outsourced decryption. In fact, using our techniques, we can modify unbounded ABE schemes [7], [33] to unbounded ABE scheme with verifiable outsourced decryption.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014



- Setup(λ, U) The setup algorithm takes as input a security parameter λ and a small universe description $U = \{1, 2, \dots, \ell\}$. It first runs $\mathcal{G}(\lambda)$ to obtain $(p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of prime order p. It then chooses $g, u, v, d \in \mathbb{G}$, and $\alpha, a \in \mathbb{Z}_p^*$ uniformly at random. For each attribute $i \in U$, it chooses a random value $s_i \in \mathbb{Z}_p^*$. Finally, it chooses a collision-resistant hash function $H : \mathbb{G} \rightarrow \mathbb{Z}_p^*$. The public parameters are published as $\mathsf{PK} = (\mathbb{G}, \mathbb{G}_T, e, g, u, v, d, g^{a}, e(g,g)^{\alpha}, T_i = g^{s_i} \forall i,\ H)$. The master secret key is $\mathsf{MSK} = \alpha$.
- KeyGen$(\mathsf{PK}, \mathsf{MSK}, \mathcal{S})$ The key generation algorithm randomly picks $t \in \mathbb{Z}_p^*$. The secret key $\mathsf{SK}_{\mathcal{S}} = (\mathcal{S},\ K, K_0, K_i)$ is computed as $K = g^{\alpha} g^{at}$, $K_0 = g^t$, $K_i = T_i^t\ \forall i \in \mathcal{S}$.
- Encrypt$(\mathsf{PK}, M, \mathbb{A})$ The encryption algorithm takes as input the public parameters PK, a message $M \in \mathbb{G}_T$ to encrypt and an LSSS access structure $\mathbb{A} = (\mathbf{A}, \rho)$, where $\mathbf{A}$ is an $\ell \times n$ matrix and ρ is a map from each row A_i of $\mathbf{A}$ to an attribute $\rho(i)$. It chooses two random vectors $\vec{v}, \vec{v}' \in \mathbb{Z}_p^{*n}$, denoted $\vec{v} = (s, v_2, \dots, v_n)$ and $\vec{v}' = (s', v_2', \dots, v_n')$. For each row A_i of $\mathbf{A}$, it chooses $r_{1,i}, r_{2,i} \in \mathbb{Z}_p^*$ uniformly at random. Finally, it chooses a random message $\tilde{M} \in \mathbb{G}_T$. The ciphertext is $CT = ((\mathbf{A}, \rho),\ \hat{C},\ C_1, C_1', C_{1,i}, D_{1,i}, C_2, C_2', C_{2,i}, D_{2,i})$, where

$$\hat{C} = u^{H(M)} v^{H(\tilde{M})} d,$$
$$C_1 = M \cdot e(g,g)^{\alpha s},\ C_1' = g^s,$$
$$C_{1,i} = g^{aA_i \cdot v} T_{\rho(i)}^{-r_{1,i}},\ D_{1,i} = g^{r_{1,i}}\ \forall i \in \{1, 2, \dots, \ell\},$$
$$C_2 = \tilde{M} \cdot e(g,g)^{\alpha s'},\ C_2' = g^{s'},$$
$$C_{2,i} = g^{aA_i \cdot v'} T_{\rho(i)}^{-r_{2,i}},\ D_{2,i} = g^{r_{2,i}}\ \forall i \in \{1, 2, \dots, \ell\}.$$

- Decrypt$(\mathsf{PK}, \mathsf{SK}_{\mathcal{S}}, CT)$ The decryption algorithm takes as input the public parameters PK, a private key $\mathsf{SK}_{\mathcal{S}} = (\mathcal{S},\ K,\ K_0, K_i)$ for a set of attributes $\mathcal{S}$ and a ciphertext $CT = ((\mathbf{A}, \rho),\ \hat{C},\ C_1, C_1', C_{1,i}, D_{1,i}, C_2, C_2', C_{2,i}, D_{2,i})$ for an access structure $\mathbb{A} = (\mathbf{A}, \rho)$. If $\mathcal{S}$ does not satisfy the access structure $\mathbb{A}$, it outputs $\perp$. Suppose that $\mathcal{S}$ satisfies the access structure and let $I \subset \{1, 2, \dots, \ell\}$ be defined as $I = \{i : \rho(i) \in \mathcal{S}\}$. It computes constant $\omega_i \in \mathbb{Z}_p^*$ such that $\sum_{i \in I} \omega_i A_i = (1, 0, \dots, 0)$. The decryption algorithm then computes:

$$C_1 \cdot \frac{\left(\prod_{i \in I} (e(C_{1,i}, K_0) \cdot e(K_{\rho(i)}, D_{1,i}))^{\omega_i}\right)}{e(C_1', K)}$$
$$= M \cdot e(g,g)^{\alpha s} \cdot \frac{\left(\prod_{i \in I} e(g,g)^{atA_i \cdot v \cdot \omega_i}\right)}{(e(g,g)^{\alpha s} e(g,g)^{ats})} = M,$$
$$C_2 \cdot \frac{\left(\prod_{i \in I} (e(C_{2,i}, K_0) \cdot e(K_{\rho(i)}, D_{2,i}))^{\omega_i}\right)}{e(C_2', K)}$$
$$= \tilde{M} \cdot e(g,g)^{\alpha s'} \cdot \frac{\left(\prod_{i \in I} e(g,g)^{atA_i \cdot v' \cdot \omega_i}\right)}{(e(g,g)^{\alpha s'} e(g,g)^{ats'})} = \tilde{M}.$$

The first and second areas are encryptions of concept and a unique concept respectively, using the security criteria of Waters' CP-ABE plan [4]. Actually, the second and third areas are repetitive. However, the repetitive areas are the factor that we can build a CP-ABE with verifiable contracted decryption from the above CP-ABE plan.

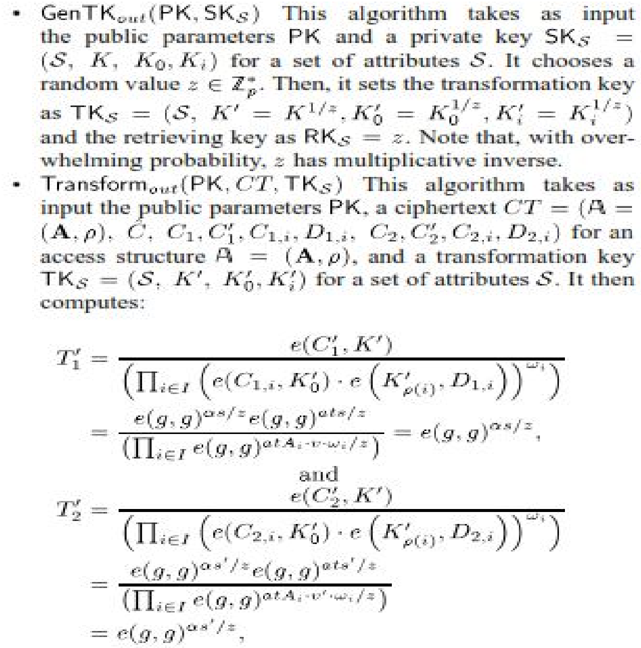
Theorem 1: Suppose that the construction of Waters [4] is a selectively CPA-secure CP-ABE scheme, then the above construction of CP-ABE scheme is also selectively CPA-secure.

Proof: To prove the selective CPA security of our CP-ABE scheme, we consider the following two games.

- Game_0 The original selectively CPA-secure game of CP-ABE.

- Game_1 Same as except for the way that the challenger generates the challenge ciphertext where the challenger picks $\hat{C} \in \mathbb{G}$ randomly and the rest parts of the challenge ciphertext are generated properly as in Game_0 .

B. Our CP-ABE Scheme with Verifiable Outsourced Decryption

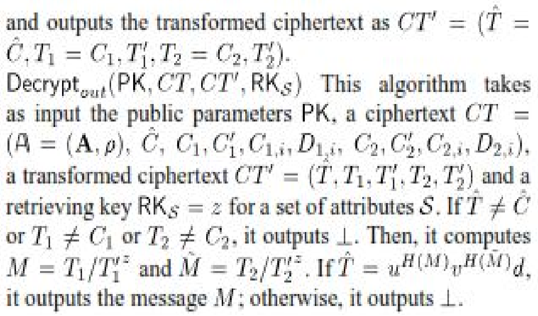


- $\mathsf{GenTK}_{out}(\mathsf{PK}, \mathsf{SK}_{\mathcal{S}})$ This algorithm takes as input the public parameters PK and a private key $\mathsf{SK}_{\mathcal{S}} = (\mathcal{S},\ K,\ K_0, K_i)$ for a set of attributes $\mathcal{S}$. It chooses a random value $z \in \mathbb{Z}_p^*$. Then, it sets the transformation key as $\mathsf{TK}_{\mathcal{S}} = (\mathcal{S},\ K' = K^{1/z}, K_0' = K_0^{1/z}, K_i' = K_i^{1/z})$ and the retrieving key as $\mathsf{RK}_{\mathcal{S}} = z$. Note that, with overwhelming probability, z has multiplicative inverse.
- $\mathsf{Transform}_{out}(\mathsf{PK}, CT, \mathsf{TK}_{\mathcal{S}})$ This algorithm takes as input the public parameters PK, a ciphertext $CT = (\mathbb{A} = (\mathbf{A}, \rho),\ \hat{C},\ C_1, C_1', C_{1,i}, D_{1,i},\ C_2, C_2', C_{2,i}, D_{2,i})$ for an access structure $\mathbb{A} = (\mathbf{A}, \rho)$, and a transformation key $\mathsf{TK}_{\mathcal{S}} = (\mathcal{S},\ K',\ K_0', K_i')$ for a set of attributes $\mathcal{S}$. It then computes:

$$T_1' = \frac{e(C_1', K')}{\left(\prod_{i\in I}\left(e(C_{1,i}, K_0') \cdot e\left(K'_{\rho(i)}, D_{1,i}\right)\right)^{\omega_i}\right)}$$
$$= \frac{e(g,g)^{\alpha s/z} e(g,g)^{ats/z}}{\left(\prod_{i\in I} e(g,g)^{atA_i \cdot v \cdot \omega_i/z}\right)} = e(g,g)^{\alpha s/z},$$

and

$$T_2' = \frac{e(C_2', K')}{\left(\prod_{i\in I}\left(e(C_{2,i}, K_0') \cdot e\left(K'_{\rho(i)}, D_{2,i}\right)\right)^{\omega_i}\right)}$$
$$= \frac{e(g,g)^{\alpha s'/z} e(g,g)^{ats'/z}}{\left(\prod_{i\in I} e(g,g)^{atA_i \cdot v' \cdot \omega_i/z}\right)}$$
$$= e(g,g)^{\alpha s'/z},$$



and outputs the transformed ciphertext as $CT' = (\hat{T} = \hat{C}, T_1 = C_1, T_1', T_2 = C_2, T_2')$.

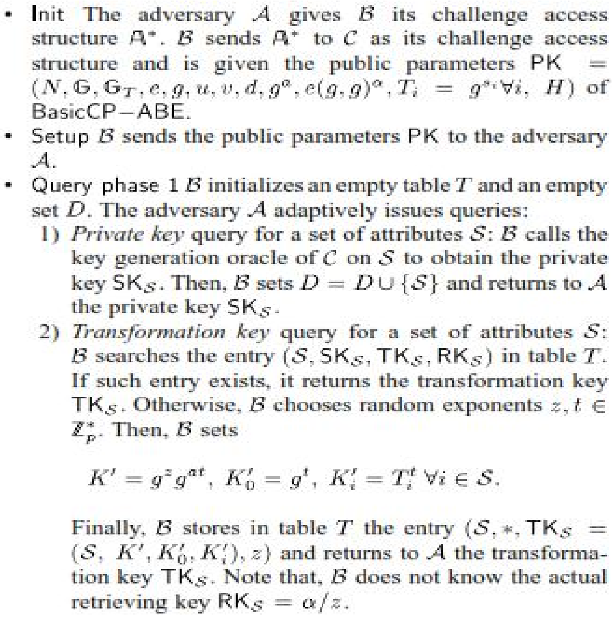
- $\mathsf{Decrypt}_{out}(\mathsf{PK}, CT, CT', \mathsf{RK}_{\mathcal{S}})$ This algorithm takes as input the public parameters PK, a ciphertext $CT = (\mathbb{A} = (\mathbf{A}, \rho),\ \hat{C},\ C_1, C_1', C_{1,i}, D_{1,i},\ C_2, C_2', C_{2,i}, D_{2,i})$, a transformed ciphertext $CT' = (\hat{T}, T_1, T_1', T_2, T_2')$ and a retrieving key $\mathsf{RK}_{\mathcal{S}} = z$ for a set of attributes $\mathcal{S}$. If $\hat{T} \neq \hat{C}$ or $T_1 \neq C_1$ or $T_2 \neq C_2$, it outputs $\perp$. Then, it computes $M = T_1/T_1'^{z}$ and $\tilde{M} = T_2/T_2'^{z}$. If $\hat{T} = u^{H(M)} v^{H(\tilde{M})} d$, it outputs the message M; otherwise, it outputs $\perp$.

Obviously, the above CP-ABE scheme with outsourced decryption satisfies correctness. In the above construction, a user runs the algorithm to recover the plaintext from the transformed ciphertext and computation cost incurred by the user is about three exponentiations, which is far less than the cost of running the algorithm to recover the plaintext from the original ciphertext directly. The input of algorithm includes the original ciphertext and the transformed ciphertext. In fact, the user only needs to know to verify the correctness of the transformation done by the cloud.

Theorem 2: Assume that $\mathsf{BasicCP-ABE}$.
is selectively CPA- secure. Then the above construction of CP-ABE scheme with outsourced decryption is selectively CPA-secure.

Proof: Suppose there exists an adversary that can attack the above CP-ABE scheme with outsourced decryption in the selectively CPA-secure model with nonnegligible advantage. We build an algorithm that can attack the CP-ABE scheme $\mathsf{BasicCP-ABE}$ in the selectively CPA-secure model with non negligible advantage. Let be the challenger corresponding to in the selectively CPA-secure game of the CP-

ABE scheme runs to execute the following steps.



- Init The adversary $\mathcal{A}$ gives $\mathcal{B}$ its challenge access structure $\mathbb{A}^*$. $\mathcal{B}$ sends $\mathbb{A}^*$ to $\mathcal{C}$ as its challenge access structure and is given the public parameters $\mathsf{PK} = (N, \mathbb{G}, \mathbb{G}_T, e, g, u, v, d, g^a, e(g,g)^\alpha, T_i = g^{s_i} \forall i, H)$ of $\mathsf{BasicCP-ABE}$.
- Setup $\mathcal{B}$ sends the public parameters PK to the adversary $\mathcal{A}$.
- Query phase 1 $\mathcal{B}$ initializes an empty table T and an empty set D. The adversary $\mathcal{A}$ adaptively issues queries:
  1) *Private key* query for a set of attributes $\mathcal{S}$: $\mathcal{B}$ calls the key generation oracle of $\mathcal{C}$ on $\mathcal{S}$ to obtain the private key $\mathsf{SK}_\mathcal{S}$. Then, $\mathcal{B}$ sets $D = D \cup \{\mathcal{S}\}$ and returns to $\mathcal{A}$ the private key $\mathsf{SK}_\mathcal{S}$.
  2) *Transformation key* query for a set of attributes $\mathcal{S}$: $\mathcal{B}$ searches the entry $(\mathcal{S}, \mathsf{SK}_\mathcal{S}, \mathsf{TK}_\mathcal{S}, \mathsf{RK}_\mathcal{S})$ in table T. If such entry exists, it returns the transformation key $\mathsf{TK}_\mathcal{S}$. Otherwise, $\mathcal{B}$ chooses random exponents $z, t \in \mathbb{Z}_p^*$. Then, $\mathcal{B}$ sets

$$K' = g^z g^{at},\ K'_0 = g^t,\ K'_i = T_i^t\ \forall i \in \mathcal{S}.$$

Finally, $\mathcal{B}$ stores in table T the entry $(\mathcal{S}, *, \mathsf{TK}_\mathcal{S} = (\mathcal{S},\ K', K'_0, K'_i), z)$ and returns to $\mathcal{A}$ the transformation key $\mathsf{TK}_\mathcal{S}$. Note that, $\mathcal{B}$ does not know the actual retrieving key $\mathsf{RK}_\mathcal{S} = \alpha/z$.

•The adversary A submits two (equal length)

messages M_0, M_1 and an access structure. A, B sends M_0, M_1 and A to B to obtain the challenge ciphertext CT^*. Then, B sends CT^* to the adversary A as its challenge ciphertext.

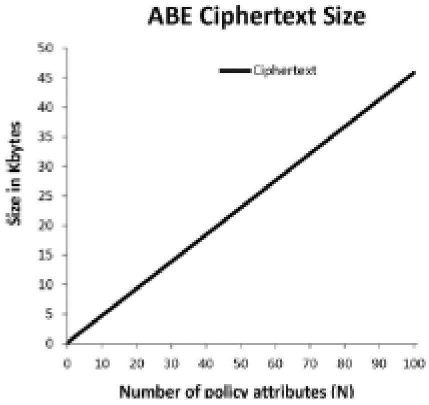
• continues to adaptively issue private key queries as in Query phase 1, and responds the queries as in Query phase 1.

• The attacker results a bit also results. So, we develop a criteria that can strike in the precisely CPA-secure design with non minimal benefits, if can strike the above CP-ABE plan with contracted decryption in the precisely CPA-secure design with non minimal benefits.

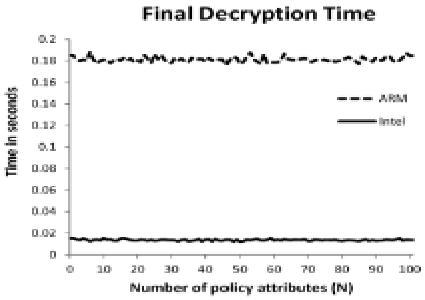
V. PERFORMANCE EVALUTION

In order to evaluate the performance of our CP-ABE scheme with verifiable outsourced decryption presented, we implement our scheme in software based on the libfenc library [18] and using a 224-bit MNT elliptic curve from the Stanford Pairing-Based Crypto library [34]. Although our implementation based the MNT curve implies the use of asymmetric pairing; only a small change need to be made on our scheme of symmetric setting in the implementation.

Specifically, suppose that an asymmetric pairing takes elements from and as inputs. Then, according to the description



of our scheme in Section, we generate two's, one from and another from , and compute two corresponding. We further set u, v, d, T_i as group elements in .As a consequence, among the ciphertext and private key components, ,$\hat{C}, C'_1, C'_2, C_{1,i}, C_{2,i}, K_i$ are group elements in while $D_{1,i}, D_{2,i}, \hat{K}, \hat{K}_0$ are group elements. The reason why we apply our suggested plan using asymmetric coupling is that: compared to symmetrical combinations, asymmetric combinations are much quicker and more lightweight to apply [35]–[37]. We gather our rule on two devoted components platforms:



s

Discussion: The ABE ciphertext size and decryption/transformation time increase linearly as the ciphertext policy's complexity grows. An encryption under a ciphertext policy with 100 attributes results in an ABE ciphertext of nearly 46 KB and it takes about 5 seconds for the Intel platform to decrypt this ciphertext. On the other hand, decryptio The ABE ciphertext size and decryption/transformation time increase linearly as the ciphertext policy's complexity grows. An encryption under a ciphertext policy with 100 attributes results in an ABE ciphertext of nearly 46 KB and it takes about 5 seconds for the Intel platform to decrypt this ciphertext. On the other hand, decryption time degrades considerably on the ARM platform: it requires more than 1 second to decrypt a ciphertext under a policy with one attribute, 5 seconds under a policy with ten attributes and almost 50 seconds under a policy with one hundred attributes. As expected, outsourcing substantially reduces the computation time required for devices with limited computing resource to recover the plaintext. The bulk of the decryption operation is now handled by the proxy. The transformed ciphertext is not only much efficient to decrypt but also much smaller in size. In our implementation, each partially-decrypted ciphertext has a constant size of 392 bytes, regardless the complexity of its corresponding ciphertext policy. The final decryption and verification of the transformed ciphertext requires only 13 milliseconds on the Intel platform and approximately 180 milliseconds on the ARM platform n time degrades considerably on the ARM platform: it requires more than 1 second to decrypt a ciphertext under a policy with one attribute, 5 seconds under a policy with ten attributes and almost 50 seconds under a policy with one hundred attributes. As expected, outsourcing substantially reduces the computation time required for devices with limited computing resource to recover the plaintext. The bulk of the decryption operation is now handled by the proxy. The transformed ciphertext is not only much efficient to decrypt but also much smaller in size. In our implementation, each partially-decrypted ciphertext has a constant size of 392 bytes, regardless the complexity of its corresponding ciphertext policy. The final decryption and verification of the transformed ciphertext requires only 13 milliseconds on the Intel platform and approximately 180 milliseconds on the ARM platform.

VI. CONCLUSION

In this paper, we design a secure information discussing plan, Mona, for powerful groups in an untrusted reasoning. In Mona, a customer is able to work together with others in the group without exposing identification comfort to the reasoning. Additionally, Mona facilitates effective customer cancellation and new customer becoming a member of. More specially, effective customer cancellation can be carried out through a public cancellation list without upgrading the private important factors of the staying customers, and new customers can directly decrypt data files saved in the reasoning before their contribution. Moreover, the storage expense and the security calculations cost are continuous. Comprehensive studies show that our suggested plan meets the preferred security requirements and assures performance as well.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, 2005, pp. 457–473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Computer and Communications Security*, 2006, pp. 89–98.
[3]R.Ostrovsky,A.Sahai,andB.Waters,"Attribute-basedencryption with non-monotonic access structures," in *Proc. ACM Conf. Computerand Communications Security*, 2007, pp. 195–203.
[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Public Key Cryptography*, 2011, pp. 53–70.
[5] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. EUROCRYPT*, 2010, pp. 62–91.
[6] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Proc. CRYPTO*, 2010, pp. 191–208.
[7] A. B. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," in *Proc. EUROCRYPT*, 2011, pp. 547–567.
[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in *Proc. IEEE Symp. Security and Privacy*, 2007, pp. 321–334.
[9] L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Computer and Communications Security*, 2007, pp. 456–465.
[10] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, 2012.
[11] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. Public Key Cryptography*, 2013, pp. 162–179.
[12] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. USENIX Security Symp.*, San Francisco, CA,USA,2011.
[13] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. ACM Conf. Computer and Communications Security*, 1993, pp. 62–73.
[14] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited (preliminary version)," in *Proc. STOC*, 1998, pp. 209–218.
[15] J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in *Proc. CRYPTO*, 2002, pp. 111–126.
[16] S. Goldwasser and Y. T. Kalai, "On the (in)security of the fiat-shamir paradigm," in *Proc. FOCS*, 2003, pp. 102–113.
[17] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable randomoracle-model scheme for a hybrid-encryption problem," in *Proc. EUROCRYPT*, 2004, pp. 171–188.
[18] M. Green, A. Akinyele, and M. Rushanan, Libfenc: The Functional Encryption Library.
[19] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verIfiable computing: Outsourcing computation to untrusted workers," in *Proc. CRYPTO*, 2010, pp. 465–482.
[20] K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in *Proc. CRYPTO*, 2010, pp. 483–501.
[21] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. STOC*, 2009, pp. 169–178.
[22] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Proc. EUROCRYPT*, 2011, pp. 129–148.
[23] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in *Proc. TCC*, 2012, pp. 422–439.
[24] S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich, "Succinct functional encryption and applications: Reusable garbled circuits and beyond," *IACR Cryptology ePrint Archive*, vol. 2012, p. 733, 2012.

[25] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, “Secure delegation of e lliptic-curve pairing,” in *Proc. CARDIS*, 2010, pp. 24–35.
[26] B. G. Kang, M. S. Lee, and J. H. Park, “Efficient delegation of pairing computation,” *IACR Cryptology ePrint Archive*,vol.2005,p.259, 2005.
[27] P. P. Tsang, S. S. M. Chow, and S. W. Smith, “Batch pairing delegation,” in *Proc. IWSEC*, 2007,
pp. 74–90.
[28] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in *Proc. EUROCRYPT*, 1998, pp. 127–144.
[29] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in *Proc. NDSS*,SanDieg o, CA, USA, 2005.
[30] A. Beimel, “Secure Schemes for Secret Sharing and Key Distribution,” Ph.D. dissertation, Israel Inst. of Technology, Technion City, Haifa, Israel, 1996.
[31] A. B. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in *Proc. EUROCRYPT*, 2011, pp. 568–588. [32] R. Canetti, H. Kra wczyk, and J. B. Nielsen, “Relaxing chosen-ciphertext security,” in *Proc. CRYPTO*, 2003, pp. 565–582.
[33] T. Okamoto and K. Takashima, “Fully secure unbounded inner-product and attributebased encryption,” in *Proc. ASIACRYPT*, 2012, pp. 349–366.
[34] B. Lynn, The Stanford Pairing Based Crypto Library.
[35] S. Chatterjee and A. Menezes, “On cryptographic protocols employing asymmetric pairings—The role of revisited,” *Discrete Appl. Math.*, vol. 159, no. 13, pp. 1311–1322, 2011.
[36]SD.Galbrith,K.G.Paterson,andN.P.Smart,“Pairingsforcryptographers,” *Discrete Appl. Math.*, vol. 156, no. 16, pp. 3113–3121, 2008.
[37] N. P. Smart and F. Vercauteren, “On computable isomorphisms in efficient asymmetric pairing-based systems,” *Discrete Appl. Math.*, vol. 155, no. 4, pp. 538–547, 2007.