Complex Intell. Syst. (2016) 2:285–291
DOI 10.1007/s40747-016-0030-8

ORIGINAL ARTICLE

An efficient identity-based QER cryptographic scheme

Chandrashekhar Meshram[1] · **P. L. Powar**[1]

Received: 29 September 2015 / Accepted: 24 October 2016 / Published online: 10 November 2016

Abstract Recently, an identity-based quadratic exponentiation randomized cryptosystem scheme using the discrete logarithm problem and the integer factorization problem has been developed. Their contribution lies in that they initiated an idea to create the identity-based cryptographic scheme without bilinear pair. This scheme can achieve the security goal of protecting data and prevent the adversary from snooping the encrypted data, and finding the secrete keys. In this paper, we have proposed some modification in setup phase using floor function and super-increasing sequence, and modified the encryption and decryption process in the identity-based quadratic exponentiation randomized cryptographic scheme. We also discuss how to enhance the security of proposed scheme and processing cost of the proposed scheme.

Keywords Cryptography · Identity-based quadratic exponentiation randomized cryptosystem · Discrete logarithm problem · Integer factorization problem · Quadratic exponentiation randomized

Introduction

Rapid advances in computer technology and the development of the Internet are changing the way of daily life. We also organize our daily and business lives according to Internet facility. Secrecy is an important issue with respect to sensitive data transferred over insecure public channels. In an open network environment, secret session key needs to be shared between two users before it establishes a secret communication [7,16–18]. As the number of users in the network is increasing, key distribution will become a serious problem. The public key cryptosystem can effectively solve the session key distribution problem in an open network environment, but each user should authenticate the public key of the partner before using it. The public key infrastructure (PKI) is proposed to implement the authentication of the public key, but it leads to large management overheads.

In 1984, the concept of the identity-based cryptographic scheme was introduced by Shamir [1]. According to his idea, the public key of each user is just extracted from his public identity information, such as e-mail address, identity number, etc. [1]. Using each user's public identity as his public key can escape the problem of authentication of the public key, and it enables users to establish the session key in the non-interactive form. However, Shamir only succeeded in constructing an Identity-based signature scheme. When Boneh et al. [17] constructed identity-based encryption using the property of Weil pairing, designed the Identity-based cryptographic scheme, and then only, it was practically implemented. However, the bilinear pair operations make the cryptographic scheme unsuitable to low-performance devices [20]. Tsujii and Itoh [21] also proposed an identity-based cryptographic scheme using the DLP with single discrete exponent which uses the ElGamal [22] public key cryptographic scheme. Recently, Meshram [8] used the variant of IFP and DLP to construct their identity-based encryption scheme and proposed many identity-based cryptographic techniques [9–12] which have been proposed. However, in these techniques, the public key of each entity is not only an identity, it is some random number selected either by the entity or by the trusted authority.

As above outline, the new identity-based cryptographic schemes always face security challenges and confidentiality

✉ Chandrashekhar Meshram
cs_meshram@rediffmail.com

[1] Department of Mathematics and Computer Science, Rani Durgavati University, Jabalpur, MP, India

worries. The main contribution of our new efficient identity-based QER cryptographic scheme is the key generation phase. In this study, we design an efficient identity-based QER cryptographic scheme using the property of DLP with distinct discrete exponent and IFP. We have also discussed enhancement of security and processing cost of efficient identity-based QER cryptographic scheme.

The rest of this paper is organized as follows: review of Meshram and Obaidat's identity-based QER cryptographic scheme is discussed in Sect. 2. An efficient identity-based QER cryptographic scheme is proposed in Sect. 3. The security analysis and security proof of our new scheme are presented in Sect. 4. Performance comparison of proposed identity-based cryptographic schemes and other six schemes are described in Sect. 5. Enhancement of security and processing cost of identity-based QER cryptographic scheme are explained in Sect. 6. Finally, in Sect. 7, we conclude the paper.

Review of Meshram and Obaidat's identity-based QER cryptographic scheme

To describe it briefly, Meshram and Obaidat's [13] identity-based QER cryptographic scheme can be summarized as four related sub-algorithms, such as Setup, Extraction, Encryption, and Decryption. The Setup algorithm is run by Private Key Generator (PKG) to generate its public and private keys. On receiving the registered application of a user, PKG will run the Extraction algorithm to generate the private key of this user if the user is identified to be legal. If some user wants to securely send a message to another user, he/she can run the Encryption algorithm to encrypt the message with the identity of the latter. On receiving the ciphertext, the receiver can run the Decryption algorithm to decrypt the ciphertext with his private key. Most of the existing identity-based cryptosystems are described in this form [7], so it is easy for readers to understand our QER description of Meshram and Obaidat's identity-based cryptographic scheme, which is shown as follows:

Setup

PKG carries out the following steps:

1. Selected p and q random prime numbers s.t. $N = pq$. Let $n = |N|$ be the bit number and compute Euler-phi function $\varphi(N) = (p-1)(q-1)$.
2. Select two arbitrary random integers e and d, $1 \leq e, d \leq \varphi(N)$ satisfying the conditions $\gcd(e, \varphi(N)) = 1$, and $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$.
3. Generate n-dimensional vector $\vec{b} = (b_1, b_2, \ldots, b_n)$ defined over multiplicative cyclic group $Z^*_{\varphi(N)}$, under the condition $1 \leq b_i \leq \varphi(N)$, $(1 \leq i \leq n)$ and $b_i \neq b_j (\mathrm{mod}\, \varphi(N))$, $(i \neq j)$.
4. Compute n-dimensional vector $\vec{h} = (h_1, h_2, h_3, \ldots, h_n)$, where $h_i = \alpha^{b_i} \mathrm{mod}\, N (1 \leq i \leq n)$.

PKG uses $(N, e, \alpha, \vec{h})$ as its public key and informs it to each entity, and at the same time, it uses $(\vec{b}, d)$ as its private key and keeps it secret.

Extraction

PKG carries out the following steps to compute the private key of the entity i, whose identity is a k-dimensional binary vector $\mathrm{ID}_i = (x_{i1}, x_{i2}, \ldots, x_{ik})$, $x_{ij} \in \{0, 1\}$, $(1 \leq j \leq k)$.

1. Compute the entity i's extended ID, R_i as follows:

$$\begin{aligned} R_i &= (\mathrm{ID}_i)^e (\mathrm{mod}\, N) \\ &= (y_{i1}, y_{i2}, y_{i3}, \ldots, y_{it}),\ y_{ij} \in \{0, 1\},\ (1 \leq j \leq t.) \end{aligned}$$

2. Entity $i's$ secrete keys s_i is computed by inner product of $\vec{b}$ and R_i as follows:

$$s_i = \vec{b} R_i (\mathrm{mod}\, \varphi(N)) = \sum_{1 \leq j \leq n} b_j y_{ij} \,\mathrm{mod}(\varphi(N)).$$

Note that ID_i is used as the public key of the entity i.

Encryption

Entity 2 wants to send the message M to entity 1, and then entity 2 can encrypt M as follows:

1. Compute the entity 1's extended ID, R_1 by the following form:

$$\begin{aligned} R_1 &= (\mathrm{ID}_1)^e (\mathrm{mod}\, N) \\ &= (y_{11}, y_{12}, y_{13}, \ldots, y_{1t}), \\ &\quad y_{1j} \in \{0, 1\},\ (1 \leq j \leq t). \end{aligned}$$

2. Compute

$$\begin{aligned} Y_1 &= \prod_{1 \leq i \leq n} h_i^{y_{1i}} (\mathrm{mod}\, N) \\ &= \prod_{1 \leq i \leq n} (\alpha^{b_i})^{y_{1i}} (\mathrm{mod}\, N) \\ &= \alpha^{\sum_{1 \leq i \leq n} b_i y_{1i} \mathrm{mod}(\varphi(N))} (\mathrm{mod}\, N) \\ &= \alpha^{s_1} (\mathrm{mod}\, N). \end{aligned}$$

Using Y_1 and PKG's public information $\vec{h}$, we follow the next steps:

3. Compute $C_1 = (\alpha^k)^e (\text{mod } N)$.
4. Compute $C_2 = (M(\alpha^{s_1})^k)^e (\text{mod } N)$.

Then, the ciphertext is given by $C = (C_1, C_2)$.

Decryption

Entity 1 does the following to recover the plaintext M from the ciphertext

1. Compute $C_1^{\varphi(N)-s_1} (\text{mod } N) = C_1^{-s_1} (\text{mod } N)$.
2. It uses secrete key s_1 to recover M as follows:

$$\begin{aligned}(C_1^{-s_1} * C_2)^d (\text{mod } N) &= (\alpha^{-s_1 ke} M^e \alpha^{s_1 ke})^d (\text{mod } N) \\ &= M^{ed} (\text{mod } N) \\ &= M (\text{mod } N).\end{aligned}$$

Propose an efficient identity-based QER cryptographic scheme

The efficient identity-based QER cryptographic scheme is more secure than the previous scheme presented by Meshram and Obaidat's [13] in terms of security. We used floor function and super-increasing sequence to develop the master key pair in this scheme. It is very difficult for attacker or adversary to find the private key and break the communication between different parties in low time period as compared with the scheme described in [13]. It is also very difficult to maintain the communication cost for breaking the system in view of our proposed scheme.

New efficient identity-based QER cryptographic scheme is described in four sub-algorithms, such as Setup, Extraction, Encryption, and Decryption, which are shown as follows.

Setup

The *Setup* algorithm is the same as only steps 1–4 in Sect. 2 [13] of this paper. The different steps from scheme [13] are as follows:

1. Select a natural number satisfying the conditions $\gcd(\beta, \varphi(N)) = 1$ and $\beta < \lfloor \varphi(N)/n \rfloor$, where $\lfloor x \rfloor$ denote the floor function which implies the largest integer smaller than x.
2. Choose super-increasing sequence corresponding to b as $\vec{b}'_i (1 \le i \le n)$ when satisfies $\sum_{j=1}^{i-1} \vec{b}'_j + \delta < \varphi(N)$ where $\delta < \lfloor \varphi(N)/\beta \rfloor$, and $\sum_{j=1}^{n} \vec{b}'_j < \varphi(N)$.
3. Compute $b_i = b'\beta (\text{mod } \varphi(N))$ and $c_i = b_i (\text{mod } \beta)$, $(1 \le i \le n)$
4. Compute n-dimensional vectors $v = (v_1, v_2, \ldots, v_n)$, where $v_l = d_l b_l (\text{mod } \varphi(N))$, $(1 \le l \le n)$.

PKG uses $(N, e, \vec{h})$ as his public key and informs it to each entity, and at the same time, it uses $(\vec{v}, d)$ as his private key and keeps it secret.

Extraction

PKG carries out the following steps to compute the private key of the entity i, whose identity is a k-dimensional binary vector $\text{ID}_i = (x_{i1}, x_{i2}, \ldots, x_{ik}), x_{ij} \in \{0, 1\}, (1 \le j \le k)$.

1. Compute as the extended of entity i's, by the following:

$$\begin{aligned}R_i &= (\text{ID}_i)^e (\text{mod } N) = (y_{i1}, y_{i2}, \ldots, y_{it}), \\ &\quad y_{ij} \in \{0, 1\}, (1 \le j \le t).\end{aligned}$$

2. Entity $i's$ secrete keys s_i is computed by inner product of $\vec{v}_l$ and R_i as follows:

$$s_i = \vec{v}_l R_i (\text{mod } \varphi(N)) = \sum_{1 \le j \le n} \vec{v}_l y_{ij} \text{mod } (\varphi(N))$$

Encryption

Entity 2 wants to send the message M to entity 1, and entity 2 can encrypt M as follows:

1. Compute the entity i's extended ID,$R_1$by the following:

$$R_1 = (y_{11}, y_{12}, \ldots, y_{1t}), y_{1j} \in \{0, 1\}, (1 \le j \le t).$$

2. Compute

$$\begin{aligned}Y_1 &= \prod_{1 \le i \le n} (h_i^{y_{1i}})^{d_i} (\text{mod } N) \\ &= \prod_{1 \le i \le n} ((\alpha^{b_i})^{y_{1i}})^{d_i} (\text{mod } N) \\ &= \alpha^{\sum_{1 \le i \le n} \vec{v}_l y_{1i} \text{mod}(\varphi(N))} (\text{mod } N) \\ &= \alpha^{s_1} (\text{mod } N).\end{aligned}$$

From Y_1 and PKG's public information $\vec{h}$

3. Compute $Y_2 = \alpha^{\varphi(N)-s_1} (\text{mod } N) = \alpha^{-s_1} (\text{mod } N)$.
4. Compute the ciphertext $C = (M\alpha^{s_1}.)^e (\text{mod } N)$

Decryption

Entity 1 does the following to recover the plaintext M from the cipher text:

1. Use his private key s_1 to recover M as $M = (Y_2^e * C)^d \pmod N$.

The correctness of the proposed scheme can be shown as follows:
Due to $Y_2^e = (\alpha^{-s_1})^e \pmod N$
We have $(Y_2^e * C)^d \pmod N \equiv (\alpha^{-s_1 e} M^e \alpha^{s_1 e})^d \pmod N \equiv M^{ed} \pmod N \equiv M \pmod N$.

Security analysis and discussions

The security of identity-based QER cryptographic scheme is based on the index problems, such as IFP and DLP, which define over multiplicative cyclic group Z_N^*. Applying Meshram and Meshram attacking method [14] to the proposed system, it may be noted that center's secret information may be disclosed.

Theorem 1 [14] *The* $(n+1)$ *entities'* $i, (1 \le i \le n+1)$ *can derive an n-dimensional vector* v_i' *over* $Z_{\varphi(N)}^*$ *which is equivalent (not necessarily identical) to the original PKG 's secret information.*

Proof When $(n+1)$ entities' $i, (1 \le i \le n+1)$ conspire, then system of linear congruence is as follows:

$$\begin{bmatrix} R_1 & 0 & \cdots & 0 & 0 \\ 0 & R_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & R_n & 0 \\ 0 & 0 & \cdots & 0 & R_{n+1} \end{bmatrix} \begin{bmatrix} v_1 & 0 & \cdots & 0 & 0 \\ 0 & v_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & v_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & v_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} \pmod{\varphi(N)}. \quad (1)$$

However, each R_i is an n-dimensional binary vector, there exists an $(n+1)$-dimensional vector c over the $Z_{\varphi(N)}$, such that

$$\sum_{1 \le i \le n+1} w_i R_i = 0. \quad (2)$$

Here, we have

$$\sum_{1 \le i \le n+1} w_i s_i = 0 (\bmod \varphi(N)) \quad (3)$$

and thus

$$\sum_{1 \le i \le n+1} w_i s_i = D\,\varphi(N). \quad (4)$$

The $(n+1)$ entities can have an integer multiple of $\varphi(N)$, if $D \ne 0$. Then, they can find out the factorization of N. A similar method with attack (Theorem 1) is applicable. Hence, the PKG's secret information can be derived by $(n+1)$-entities conspiracy.

Furthermore, Meshram developed a more general attacking method [2] for the modified system, such that $(n+2)$ entities conspiracy can derive the PKG 's secret information with high probability.

Theorem 2 [2] *The* $(n+2)$ *entities'* $i, (1 \le i \le n+2)$ *can derive the PKG 's secret information* v *with high probability.*

Proof When $(n+1)$ entities $i, (1 \le i \le n+1)$ conspire, they have the following system of linear congruence's defined by the following equation:

$$\begin{bmatrix} R_1 & 0 & \cdots & 0 & 0 \\ 0 & R_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & R_n & 0 \\ 0 & 0 & \cdots & 0 & R_{n+1} \end{bmatrix} \begin{bmatrix} v_1 & 0 & \cdots & 0 & 0 \\ 0 & v_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & v_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & v_n \end{bmatrix}$$

$$= \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} \pmod{\varphi(N)} \quad (5)$$

$$= Ba (\bmod \varphi(N)). \quad (6)$$

Assuming that the matrix B includes n linearly independent column vectors over $Z_{\varphi(N)}$, there exist some positive integers $w_i \quad (1 \le i \le n+1)$, such that

$$\begin{bmatrix} R_1 & 0 & \cdots & 0 & 0 \\ 0 & R_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & R_n & 0 \\ 0 & 0 & \cdots & 0 & R_{n+1} \end{bmatrix} \begin{bmatrix} v_1 & 0 & \cdots & 0 & 0 \\ 0 & v_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & v_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & v_n \end{bmatrix}$$

$$= \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} - \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_{n+1} \end{bmatrix} \varphi(N). \quad (7)$$

Then, Eq. (7) can be rewritten by the following form:

$$\begin{bmatrix} R_1 & 0 & \cdots & 0 & 0 & s_1 \\ 0 & R_2 & & 0 & 0 & s_2 \\ \vdots & & \ddots & \vdots & & s_3 \\ 0 & 0 & & R_n & 0 & \vdots \\ & & \cdots & & & \\ 0 & 0 & & 0 & R_{n+1} & s_{n+1} \end{bmatrix} \begin{bmatrix} v_1 & 0 & \cdots & 0 & 0 \\ 0 & v_2 & & 0 & 0 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & & v_{n-1} & 0 \\ & & \cdots & & \\ 0 & 0 & & 0 & v_n \end{bmatrix}$$

$$= -\begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_{n+1} \end{bmatrix} \varphi(N) \tag{8}$$

$$= B' v_i'. \tag{9}$$

The matrix B in Eq. (6) includes n linearly independent column vectors over $Z_{\varphi(N)}$ by supposition, it follows that the matrix B' is non-singular over $Z_{\varphi(N)}$ [i.e., det $(B') \neq 0$] with overwhelming probability, and thus, we have $v_i' \neq 0(\text{mod}\,\varphi(N))$. On the other hand, we have the following system of linear congruences:

$$\vec{B}' v_i' = 0(\text{mod}\,\varphi(N)). \tag{10}$$

If the matrix B' is non-singular over $Z^*_{\varphi(N)}$, then $v_i' = 0(\text{mod}\,\varphi(N))$, and this contradicts the above results. Thus, the matrix D' is singular over $Z^*_{\varphi(N)}$, and we have det $(B') = 0(\text{mod}\,\varphi(N))$ with high probability. It shows that det $(B'))$ is divisible by $\varphi(N)$ with high probability. Furthermore, consider the case where the other $(n+1)$ entities among $(n+2)$ conspire, and define the matrix D'' in a way similar to the above. Then, det (B'') is divisible by $\varphi(N)$ with high probability. Hence, gcd (det(B'), det (B'')) gives $d\varphi(N)$, where d is a small positive integer. By the above procedure, we can evaluate $\varphi(N)$ efficiently. An additional procedure to find the center's secret information is completely the same as attack (Theorem 2).

Performance comparison of identity-based cryptographic schemes

In this section, we have discussed six most widely used identity-based cryptographic schemes and compared their performance. These eight identity-based cryptographic schemes are: cocks identity-based cryptographic scheme [5], authenticated identity-based cryptographic scheme [3], selective-identity secure identity-based cryptographic scheme without random oracles [15], hierarchical identity-based cryptographic scheme [6], water's identity-based cryptographic scheme [4], Meshram and Obaidat's identity-based QER cryptographic scheme [13], and our proposed efficient Identity-based QER cryptographic scheme. These schemes have different performances on server for evaluating Encryption algorithm performance, Decryption algorithm performance, and computational cost.

Notations used in this computation are as follows:

T_{P} = The time of executing a paring operation.
T_{M} = The time of executing a modular multiplication.
T_{e} = The time of executing a modular exponentiation in group.
T_{m} = The time of executing a scalar or point multiplication in group.
T_{x} = The time of executing an XOR operation.
T_{H} = The time of executing a map to point hash function.
T_{h} = The time of executing a one-way hash function.
T_{a} = The time of executing a modular addition operation.
T_{i} = The time of executing a modular inverses operation.
T_{j} = The time of executing a Jacobi symbol operation.

As we all know, the time of executing a paring operation T_{P} is more time-consuming than other operations. Some performance simulation results [17] demonstrate that T_{a} and T_{h} are trivial in comparison with T_{e}, T_{M}, T_{x}, T_{H} , T_{i}, and T_{j}.

It is to be noted that encryption algorithmic phase and decryption algorithmic phase are the dominating process in terms of computation cost than setup and extract phases as they are executed only once. Thus, we consider only the encryption and decryption phase and accordingly compare the proposed identity-based cryptographic scheme with [3–6,13,15]. We demonstrate the comparative result in Table 1 in terms of computational cost and security properties.

It is quite clear from the above table that the proposed efficient identity-based QER cryptographic scheme bears lower computational cost than [3–6,13,15].

Enhancement of security and processing cost

The PKG's secret information for the original system is derived by n entities conspiracy in Sect. 3. Now, we consider the practical countermeasure for the enhancement of the security of the system. Here, we used the partitioning strategy [19] for enhancement the security of present scheme. The basic idea is to divide the identity-space into two disjoint segments, depending upon the outcome of a biased coin. For simplicity, we assume that n = 512 throughout this section. The PKG partitions a 512-dimensional binary vector A into 256 segments, every two bits, such as

$$A = (\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3, \ldots\ldots a_{511}, \mathrm{a}_{512}) = (\mathrm{seg}_1, \mathrm{seg}_2, \mathrm{seg}_3, \ldots\ldots \mathrm{seg}_{511}, \mathrm{seg}_{512}). \tag{11}$$

Table 1 Comparisons among our proposed identity-based cryptographic scheme and previously proposed identity-based cryptographic schemes

Identity-based cryptographic schemes	F_1	F_2	F_3
Scheme [3]	$T_P + T_H + 3T_h + T_x$	$T_P + T_H + 3T_h + T_x$	$2T_P + 2T_H + 6T_h + 2T_x$
Scheme [4]	$2T_P + 3T_m$	$2T_P + T_m + T_i$	$4T_P + 4T_m + T_i$
Scheme [5]	$T_J + 2T_a + 2T_M + 2T_i$	$T_J + T_a$	$2T_j + 3T_a + 2T_M + 2T_i$
Scheme [6]	$T_P + T_H + T_h + T_e + T_m + T_x$	$T_P + T_h + T_x$	$2T_P + T_H + 2T_h + T_e + T_m + 2T_x$
Scheme[13]	$4T_e + T_m$	$2T_e + T_m + T_i$	$6T_e + 2T_m + T_i$
Scheme [15]	$T_P + 4T_e + 2T_M$	$T_P + T_e + T_M + T_i$	$2T_P + 5T_e + 3T_M + T_i$
Proposed scheme	$2T_e + T_m + T_i$	$2T_e + T_m + T_i$	$4T_e + 2T_m + 2T_i$

F_1: computational cost for encryption phase, F_2: computational cost for decryption phase, F_3: overall computational cost for encryption and decryption phases

Table 2 Example of $h(i;\ jk)$ for $i = 1, 2, 3, 4$ and $jk \in \{0, 1\}$

$h(1: 11) = 9$	$h(2: 11) = 11$	$h(3: 11) = 18$	$h(4: 11) = 22$
$h(1: 00) = 5$	$h(2: 00) = 21$	$h(3: 00) = 4$	$h(4: 00) = 16$
$h(1: 01) = 13$	$h(2: 01) = 17$	$h(3: 01) = 23$	$h(4: 01) = 2$
$h(1: 10) = 12$	$h(2: 10) = 7$	$h(3: 10) = 15$	$h(4: 10) = 8$

Then, the PKG defines $v(i;\ jk)(1 \le i \le 256;\ j, k \in \{0, 1\})$ appropriately, computes $h(i;\ jk)$, $(1 \le i \le 256;\ j, k \in \{0, 1\})$,

$$h(i;\ jk) = \alpha^{v(i;jk)} (\text{mod } N) \tag{12}$$

for each seg_i, and publishes the table, including every $h(i;\ jk)$ to all entities. Furthermore, the center computes each entity's secret key s_k by

$$s_k = \sum_{1 \le i \le 256} v(i; \text{seg}_{ki}) (\text{mod } \varphi(N)) \tag{13}$$

depending on Sect. 3. The entity k's extended identity, R_k, where R_k is partitioned into 256 segments. Every two bits, such as:

$$R_k = (\text{seg}_{k1}, \text{seg}_{k2}, \text{seg}_{k3}, \ldots \text{seg}_{k255}, \text{seg}_{k256}).$$

Then, the center distributes it to each entity through a highly secure channel. Table 2 gives an example of $h(i;\ jk)$.

It is quite clear from the above table that the partitioning strategy enhances the security of proposed scheme using the pairing of two difference bit segments as compare the previous scheme [13].

Encryption

Entity 2 computes Y_1',

$$Y_1' = \prod_{1 \le i \le 256} h(i; \text{seg}_{1i})^{e_i} (\text{mod} N) \tag{14}$$

from Y_1 and the published table. Entity 2 uses γ' as γ in the original system (in Sect. 3) to encrypt the message M.

Decryption

It is exactly the same as in the original system in Sect. 3.

In the original system in Sect. 3, the PKG's secret information is derived by 512 entities conspiracy, while in the above system, it is derived by 1024 (=4 × 256) entities conspiracy. Furthermore, the running cost for encryption-key generation in the above system is about half of the original system. However, the KAC's public information in the above system is about twice than the original system. Further generalizations, e.g., each Y_i is partitioned into 128 segments every four bits, etc., are possible and such schemes are regarded as the hybrid system of the identity-based cryptosystem and the conventional public key cryptosystem.

Conclusion

In this study, the proposed efficient identity-based QER cryptographic scheme must satisfy Shamir's original concepts in a strict sense, i.e., it does not need any interactive earliest communications in, respectively, data transmission. It provides longer and higher levels of security than the schemes using IFP and the general formulation of DLP. The presented scheme needs nominal operations in encryption and decryption proses, thus makes it is very efficient. The offered out comes provides the special result from the security point of view, because we face the problem of solving IFP and DLP simultaneously in the multiplicative group define over finite fields as compared with the other identity-based cryptographic scheme. Using our propose scheme, we can develop an identity-based encryption model based on lightweight public key management techniques. It has small sizes key pair's private and public keys as compared with other Identity-based cryptographic schemes available in literature. It is more benefited in grid security architecture. The grid

environment may have a large number of members that join and leave over time and that certificates are used extensively for every job submission. This would inevitably complicate key management and increase the bandwidth requirement of a grid system. It was also noted that these problems could be simplified using certificate-free identity-based cryptographic scheme. Moreover, in the identity-based cryptographic setting, a user's public key can be created and used immediately without the need for a public key certificate to be forwarded to the intended recipient [normally via a Transport Layer Security (TLS) handshake]. However, the supposedly dynamic use of identity-based keys was hindered by some traditional limitations of identity-based cryptographic scheme, such as key escrow, and the need to distribute private keys through secure channels. More importantly, some of the essential security requirements desired in the Globus Toolkit (GT) require using proxy credentials for single sign-on and delegation, but our developed efficient identity-based QER cryptographic scheme is free from certificate and key escrow problems.

Acknowledgements This work was supported by Dr. D.S. Kothari fellowship awarded by University Grants Commission, New Delhi, India, to the first author and second author under DSA-I grant of UGC New Delhi, India.

References

1. Shamir A (1985) Identity-based cryptosystem and signature scheme, advances in cryptology: proceedings of crypto' (lecture notes in computer science 196), vol 84. Springer, Berlin, pp 47–53
2. Meshram C (2015) Factoring and discrete logarithm using IBC. Int J Hybrid Inf Technol 8(3):121–132
3. Lynn B (2002) Authenticated ID-based encryption. Cryptology ePrint Archive, Report 2002/072. http://eprint.iacr.org/2002/072
4. Waters B (2005) Efficient identity-based encryption without random oracles, advances in cryptology-CRYPTO 2005, lecture notes in computer science, vol 3494. Springer, Berlin, pp 114–127
5. Cocks C (2001) An identity based encryption scheme based on quadratic residues, international conference on cryptography and coding (proceedings of IMA), lecture notes in computer science, vol 2260. Springer, Berlin, pp 360–363
6. Gentry C, Silverberg A (2002) Hierarchical ID-based cryptography, in advances in cryptology-Asiacrypt'02, lecture notes in computer science, vol 2501. Springer, Berlin, pp 548–566
7. Meshram C, Meshram S (2013) An identity based cryptographic model for discrete logarithm and integer factoring based cryptosystem. Inf Process Lett 113(10):375–380
8. Meshram C (2015) An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. Inf Process Lett 115(2):351–358
9. Meshram C, Meshram S, Zhang M (2012) An ID-based cryptographic mechanisms based on GDLP and IFP. Inf Process Lett 112(19):753–758
10. Meshram C, Meshram S (2015) Constructing new an ID-based cryptosystem for IFP and GDLP based cryptosystem. J Discret Math Sci Cryptogr. doi:10.1080/09720529.2015.1032621
11. Meshram C (2015) An efficient ID-based beta cryptosystem. Int J Secur Appl 9(2):189–202
12. Meshram C, Meshram S (2011) An identity based beta cryptosystem, IEEE proceedings of 7th international conference on information assurance and security (IAS 2011) Dec. 5–8, pp 298–303
13. Meshram C, Obaidat M (2015) An ID-based quadratic-exponentiation randomized cryptographic scheme. IEEE proceedings of international conference on computer, information, and telecommunication systems (CITS 2015), July 15–17 (Accepted)
14. Meshram C, Meshram SA (2011) Some modification in ID-based cryptosystem using IFP & DDLP. Int J Adv Comput Sci Appl 2(8):25–29
15. Boneh D, Boyen X (2004) Efficient selective-ID secure identity based encryption without random oracles, advances in cryptology-EUROCRYPT 2004, lecture notes in computer science, vol 3027. Springer, Berlin, pp 223–238
16. Boneh D, Canetti R, Halevi S, Katz J (2007) Chosen-ciphertext security from identity-based encryption. SIAM J Comput 36(5):1301–1328
17. Boneh D, Franklin MK (2003) Identity based encryption from the Weil pairing. SIAM J Comput 32(3):586–615
18. Okarnoto E, Tanaka K (1989) Key distribution system based on identification information. IEEE J Sel Areas Commun 7:481–485
19. Coron J (2003) On the exact security of full domain hash. Advances in cryptology-CRYPTO' 2000, lecture notes in computer science, vol 1880. Springer, Berlin
20. Pang L, Li H, Wang Y (2013) nMIBAS: a novel multi-receiver ID-based anonymous signcryption with decryption fairness. Comput Inform 32(3):441–460
21. Tsujii S, Itoh T (1989) An ID-based cryptosystem based on the discrete logarithm problem. IEEE J Sel Areas Commun 7:467–473
22. ElGmal T (1995) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31:469–472