PAIRING-FRIENDLY ELLIPTIC CURVES OF EMBEDDING DEGREE 1 AND APPLICATIONS TO CRYPTOGRAPHY

Rajeev Kumar*
Dyal Singh College,
University of Delhi,
Delhi, India
rajeev82verma@gmail.com

S.K. Pal
DRDO,
Delhi, India
skptech@yahoo.com

Arvind
Hansraj College,
University of Delhi,
Delhi, India
arvind_ashu12@rediffmail.com

Abstract. Recently, Wang et al. [1] proposed a new method for constructing pairing-friendly elliptic curves of embedding degree 1. Authors claim that this method significantly improves the efficiency of generating elliptic curves. In this paper, we give the arithmetic of pairing-friendly elliptic curves of embedding degree 1. We prove that conventional classification of pairings into Type 1, 2, 3 and 4 is applicable for the elliptic curves of embedding degree 1 proposed by Wang et al. We highlight the selection of pairing-friendly elliptic curves of embedding degree 1 for design of efficient cryptosystems. We compare security and efficiency of cryptosystems based on these pairing-friendly elliptic curves with the existing cryptosystems. By using these elliptic curves we propose a new asymmetric group key agreement (ASGKA) scheme from Tate pairing. We discuss the security and efficiency of the proposed ASGKA scheme.

Keywords: Public key cryptography, pairing-friendly elliptic curves, embedding degree, Tate pairing, asymmetric group key agreement scheme.

1. Introduction

Since its applications to cryptography [2, 3], elliptic curves over finite fields have an important role in public key cryptography. Elliptic Curve Cryptography (ECC) [4] is becoming accepted as an alternative to cryptosystems such as RSA and ElGamal over finite field, because it requires less bandwidth and computational efforts when performing key exchange and/or constructing a digital signature. Pairing based cryptography is one of the recent research directions in public key cryptography. To improve the efficiency of cryptosystems based

∗. Corresponding author

on pairings, constructing pairing-friendly elliptic curves with various embedding degrees has been the subject of ongoing research. Pairing-friendly elliptic curves with various embedding degree [5, 6, 7] have been proposed in last few years. If embedding degree k of an elliptic curve is 1, then computation of pairing is related to the base field $\mathbb{F}_p$ rather than the extension field $\mathbb{F}_{p^k}$ .This helps to improve the computation efficiency of pairing.

There are many pairing-friendly elliptic curves of embedding degree 1 in cryptographic literature. Recently, Wang et al. [1] proposed a new method for constructing pairing-friendly elliptic curves of embedding degree 1. Authors claim that in their method the parameters are computed under a given expression, which significantly improves the efficiency of generating elliptic curves. Since the discovery of identity-based encryption in the year 2000, pairings have been used in design of hundreds of cryptographic schemes. But computational requirements complicate the practical application of pairing-based cryptography. In this paper, we address the issue of efficiency of pairing-based cryptography. A necessary condition for the security of pairing-based cryptosystems is that the discrete logarithm problem (DLP) in $\mathbb{F}_{p^k}$ is intractable. Experiments conducted by Barbulescu et al. [8] in 2015 illustrated that the DLP is significantly easier in $\mathbb{F}_{p^2}$ than in prime order fields $\mathbb{F}_p$. In this paper, we also highlight the selection of pairing-friendly elliptic curves of embedding degree 1 for design of secure and efficient cryptosystems. By using these curves, we implement some pairing-based protocols and compare the efficiency and security of these protocols with the existing ones.

Many cryptographic protocols rely on the existence of a confidential channel among the users. A major goal of Group Key Agreement (GKA) [9] protocols is to establish a confidential broadcast channel for the users of the group. GKA protocols allow a group of users to establish a common secret key from which a session key can be derived. So these protocols are likely to be used in any group-oriented communication applications to achieve secure broadcasting at the network layer. In GKA protocols, all users should be connected in order to share the secret encryption key. However if users are located in different cities with different time zone, it is very difficult for them to be connected concurrently. To settle this issue, the concept of Asymmetric Group Key Agreement (ASGKA) was introduced in 2009 by Wu et al. [10].

Asymmetric group key agreement is a versatile cryptographic primitive which allows a group of users to negotiate a common encryption key. This encryption key is accessible to any entity and each user only holds her respective decryption key. This primitive not only enables the confidential communication among group users but also permits any outsider to send message to group. Zhang et al. [11] presented asymmetric group key agreement protocol for open networks. The authors of [12] extended this scheme to design a new ASGKA scheme. We further extend the work of Zhang et al. but in a different flavour. In this paper, we propose a new elliptic curve based asymmetric group key agreement (ASGKA) scheme from Tate pairing.

Rest of the paper is organized as follows. In section 2, we briefly describe elliptic curves and pairings. In section 3, we give arithmetic of pairing-friendly elliptic curves of embedding degree 1. Section 4 defines the proposed ASGKA scheme. In section 5, we discuss the security issues and efficiency of the proposed scheme. We finally draw our conclusion in section 6.

2. Preliminaries

In this section we briefly describe the elliptic curves and Tate pairing on elliptic curves. We also define k-Bilinear Diffie-Hellman Exponent (k-BDHE) problem in (G_1, G_2).

2.1 Elliptic curve

An elliptic curve [13] E over a finite field $\mathbb{F}_p$ is defined by an equation

$$y^2 = x^3 + ax + b; a, b \in \mathbb{F}_p, \tag{1}$$

with the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. The set of all points on the curve E together with O, called the "point at infinity" forms a group under the operation point addition. This group is denoted by $E(\mathbb{F}_p)$. If $P(x_1, y_1)$ and $Q(x_2, y_2)$ be two points from $E(\mathbb{F}_p)$ such that $P, Q \neq O$, then $R(x_3, y_3) = P + Q$ and $2P(x_3, y_3) = P + P$ are defined as:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \pmod p \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p, \end{cases} \tag{2}$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p, \text{ if } \quad P \neq Q \quad \text{(point addition)} \tag{3}$$

$$\text{and} \quad \lambda = \frac{3x_1^2 + a}{2y_1} \pmod p, \text{ if } \quad P = Q \quad \text{(point doubling)}. \tag{4}$$

Scalar multiplication in elliptic curve group $E(\mathbb{F}_p)$ can be computed as follows:

$$kP = P + P + P + \cdots + P \quad (k \text{ times}).$$

Hasse's theorem gives a bound on the number of points on an elliptic curve over a finite field. According to this theorem if $E(\mathbb{F}_p)$ has order N, then we have

$$|N - (p + 1)| \leq 2\sqrt{p}.$$

The subgroup $E[r] = \{P \in \bar{E} | [r]P = O\}$ i.e. the subgroup of points of order r on $E(\bar{\mathbb{F}}_p)$, called r-torsion subgroup of $E(\mathbb{F}_p)$.

2.2 Tate pairing

Let G_1, G_2 and G_T be finite groups of prime order. A cryptographic pairing $e : G_1 \times G_2 \longrightarrow G_T$ is a map that satisfies the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, for all $P \in G_1, Q \in G_2$ and for all $a, b \in \mathbb{Z}_p$.
2. Non-Degeneracy: For all $P \in G_1$, with $P \neq 1_{G_1}$, there is some $Q \in G_2$ such that $e(P, Q) \neq 1_{G_T}$. For all $Q \in G_2$, with $Q \neq 1_{G_2}$, there is some $P \in G_1$ such that $e(P, Q) \neq 1_{G_T}$
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P \in G_1, Q \in G_2$.

Cryptographic pairings are constructed from elliptic curves of small embedding degree. More precisely, let $E(\mathbb{F}_p)$ be an elliptic curve defined over the finite field $\mathbb{F}_p$. Let r be a prime divisor of $\#E(\mathbb{F}_p)$ with gcd $(r, p) = 1$, and let k be the smallest positive integer such that $r|p^k - 1$. This number k is called embedding degree of $E(\mathbb{F}_p)$ with respect to r. Then G_1 is an order-r subgroup of $E(\mathbb{F}_p)$, G_2 is an order-r subgroup of $E(\mathbb{F}_{p^k})$, G_T is the order-r subgroup of $\mathbb{F}^*_{p^k}$, and the map e is derived from the classical Weil and Tate pairings.

Tate pairing [14] is a mapping $e_T : E(\mathbb{F}_{p^k}) \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r$ defined by $e_T(P, Q) = (f_{r,P}(Q))^{\frac{p^k-1}{r}}$, where $f_{r,P}$ is a normalized Miller function. Tate pairing widely used to design pairing-based protocols because it is twice as efficient as Weil pairing. It is clear from the definition of Tate pairing that if embedding degree $k \neq 1$, then the computation of Tate pairing is related to the extension field $\mathbb{F}_{p^k}$ and hence the computation process will be time consuming. However, if $k = 1$ then the computation of Tate pairing is related to the base field $\mathbb{F}_p$ rather than extension field $\mathbb{F}_{p^k}$. This will significantly improve efficiency of Tate pairing.

2.3 k-Bilinear Diffie-Hellman Exponent (k-BDHE) problem in (G_1, G_2)

Let G_1, G_2 be two elliptic curve groups. Given P in G_1, Q in G_2 and $R_i = \alpha^i P$ for $i = 1, 2, ..., k, k + 2, \ldots, 2k$ as input, compute $e_T(P, Q)^{\alpha^{k+1}}$. Since the input lacks the point $\alpha^{k+1}P$, so the bilinear pairing does not seem to help to compute $e_T(P, Q)^{\alpha^{k+1}}$.

k-BDHE assumption is that there is no polynomial-time algorithm that can solve k-BDHE problem in (G_1, G_2) with non-negligible probability.

3. Arithmetic of pairing-friendly elliptic curves of embedding degree 1

In this section we give arithmetic of pairing-friendly elliptic curve of embedding degree 1. We highlight the ρ-value of pairing-friendly elliptic curves of embed-

ding degree 1 proposed by Wang et al. We also highlight security, performance and functionality of pairings on these curves. We discuss some subtleties with using these curves to implement pairing based protocols.

3.1 Pairing-friendly elliptic curves of embedding degree 1

Pairing-friendly elliptic curves of embedding degree 1 were first mentioned in [15, 16, 17] and further studied in [18, 19]. Koblitz and Menezes [18] proposed ordinary elliptic curves of embedding degree 1 with trace 2. In these curves the prime number p is of the form $p = A^2 + 1$, where $A \equiv 2 \pmod 4$ and the elliptic curve is $E : Y^2 = X^3 - 4X$ over $\mathbb{F}_p$. As it is shown in [18], $\#E(\mathbb{F}_p) = p - 1$, so E is an ordinary elliptic curve of trace 2. Also since $E(\mathbb{F}_p) \cong \mathbb{Z}_A \oplus \mathbb{Z}_A$, so we have $E[n] \subseteq E(\mathbb{F}_p)$, where $n \equiv 3 \pmod 4$ is a prime. This shows that $E(\mathbb{F}_p)$ has embedding degree $k = 1$ with respect to n. Note that Chatterjee et al. [20] observe that conventional classification of pairings into Type 1, 2, 3 and 4 is not applicable for the elliptic curves of embedding degree 1. Elliptic curves with embedding 1 and trace different 2 can be generated using the Complex Multiplication (CM) method [19, 21]. In these common methods to construct elliptic curves, the equation $u = p + 1 \pm W$ is used to generate parameters of the elliptic curves.

Recently, Wang et al. proposed a new method to construct pairing-friendly elliptic curves of embedding degree 1. In their method, they present a new equation $p = u \pm W + 1$ to generate the parameters of elliptic curves. In the new equation, the order u of elliptic curve is known, and we need to obtain prime p from the order u rather than the order u from p. In other words, this method can generate an elliptic curve under arbitrary order r, while the order u of an elliptic curve E can be trivially obtained using $u = r * r$ (from the security requirement), where r is a large prime and has a low hamming with weight 4. As they claimed, this method improves efficiency of generating elliptic curves significantly.

This method can be summarized in the following three algorithms.

1. The first algorithm is to generate a large prime r of a low hamming with weight 4.

2. The second algorithm is used to generate the characteristic of finite field $\mathbb{F}_p$, the order u of non-supersingular elliptic curve over $\mathbb{F}_p$ and order r of a point on the elliptic curve.

3. The final algorithm is used to construct pairing-friendly elliptic curves of embedding degree 1.

The ρ-value of an elliptic curve E is defined as $\rho(E) = (\log p)/(\log r)$. Also as $\#E \neq p - 1$, so trace of these elliptic curves is different from 2.

3.2 Pairings on elliptic curves of embedding degree 1

In this subsection we will discuss security, performance and functionality characteristics of pairings on pairing-friendly elliptic curves of embedding degree 1 proposed by Wang et al. Chatterjee et al. in their paper proved that conventional classification of pairings into Type 1, 2, 3 and 4 is not applicable for elliptic curves of embedding degree 1. In this subsection we prove that this classification of pairings is applicable for the elliptic curves of embedding 1 proposed by Wang et al.

It is clear from the definition given in section 2 that if embedding of elliptic curve is $k = 1$, then pairings are constructed on the base field $\mathbb{F}_p$ rather than the extension field $\mathbb{F}_{p^k}$. This may improve significantly the computation of pairings. Also since Tate pairing in general is twice as efficient as Weil pairing. So Tate pairing is widely used to design pairing- based cryptosystems.

The function $f_{r,P}(Q)$ in definition of Weil or Tate pairing is a Miller function of length n and we use Miller's algorithm [22] to compute this function. Miller function computation can only fail if $Q \in \langle P \rangle$. In cryptographic protocols it is necessary to have an efficient method for testing whether $Q \in \langle P \rangle$. The properties of Weil pairing imply that $Q \in \langle P \rangle$ if and only if $e_W(P, Q) = 1$. So, subgroup testing can be done by using Weil pairing. But it cannot be done in the same manner by using Tate pairing. Chatterjee et al. highlight in their paper that for elliptic curves of embedding degree 1, there is no natural way of distinguishing any order-r subgroup of $E[r]$ from the other order-r subgroups. So they gave an observation that classification of pairings into Type 1, 2, 3 and 4 is not applicable for elliptic curves of embedding degree 1. They defined three new pairings called Type A, Type B and Type C for elliptic curves of embedding degree 1.

However, third algorithm of the method proposed by Wang et al. for the construction of pairing-friendly elliptic curves of embedding degree 1, ensures that the constructed subgroups G_1 and G_2 satisfy that $G_1 \cap G_2 = \{O\}$, where G_1 is the subgroup generated by P_1, G_2 is subgroup generated by P_2 and G_1, G_2 are two different subgroups of elliptic curve E with the same order r. Since by construction we get two distinguishing order-r subgroup in $E[r]$, so now we may classify the pairings on these curves into Type 1, 2, 3, and Type 4.

Also in these curves, order r of the subgroups G_1 and G_2 is a prime of low hamming with weight 4 i.e. there are only two '1' bits in addition to the highest bit and lowest bit in the binary representation of the large prime. So it may be more efficient to compute Tate pairing from Miller's algorithms on these elliptic curves of embedding degree 1.

3.3 Implementation of cryptosystems based on elliptic curves proposed by Wang et al.

Information confidentiality is an essential requirement for security in critical infrastructure. Identity-based cryptography [23], which is an increasingly popular

branch of cryptography, widely used to protect the information confidentiality in critical infrastructure due to the ability of directly computing the user's public key from user's identity. However computational requirements complicate the practical application of Identity-based cryptosystems.

Use of pairing-friendly elliptic curves of embedding degree 1 proposed by Wang et al. may improve efficiency of not only identity-based protocols but also of other protocols. In this subsection, we implement some prominent protocols using these pairing-friendly elliptic curves of embedding degree 1.

3.3.1 Boneh-Franklin IBE

Boneh-Franklin IBE [24] is an example of a prominent identity-based encryption scheme. This scheme was designed by using Type 1 Weil pairing. The security of this protocol is based on computational Diffie-Hellman problem in Type 1 setting. We give implementation of this protocol by using Type 3 Tate pairing on pairing-friendly elliptic curves proposed by Wang et al.

Definition 1: Computational Diffie-Hellman Problem (Co-DHP*) in $(\mathbf{G_1}, \mathbf{G_2})$

Let G_1 and G_2 be two elliptic curves groups. For $k \in \mathbb{Z}_q^*$, given P, kP_1 in G_1 and kP_2 in G_2, compute kP.

This IBE scheme can be described in following four algorithms.
Setup: For security parameter $m \in \mathbb{Z}^+$, the algorithm works as follows:

1. The algorithms of Wang et al. run on m to generate a large prime q, two elliptic curve groups G_1, G_2 of order q, an arbitrary generator P for G_1, a multiplicative group G_T of order q, and Tate pairing $e_T : G_1 \times G_2 \longrightarrow G_T$. Note that since G_1 and G_2 be two distinct subgroups of order q and $G_1 \cap G_2 = \{O\}$, so we can hash onto G_2.

2. Pick a random $s \in \mathbb{Z}_q^*$ and compute public key $P_{pub} = sP$.

3. Choose cryptographic hash functions $H_1 : \{0,1\}^* \longrightarrow G_2$ and $H_2 : G_T \longrightarrow \{0,1\}^n$ for some n.

The message space is $\mathcal{M} = \{0,1\}^*$ and the ciphertext space is $\mathcal{C} = G_2 \times \{0,1\}^n$. The system parameters are $\langle q, G_1, G_2, G_T, e_T, n, P, P_{pub}, H_1, H_2 \rangle$. The master key is s.
Extract: For a given $ID \in \{0,1\}^*$, the algorithm computes $Q_{ID} = H_1(ID) \in G_2$ and sets the private key d_{ID} as $d_{ID} = sQ_{ID}$, where s is master key.
Encrypt: To encrypt a message $M \in \mathcal{M}$ it first computes $Q_{ID} = H_1(ID) \in G_2$, after that choose a random number $t \in \mathbb{Z}_q^*$ and sets the ciphertext to be $C = \langle tP, M \oplus H_2(g_{ID}^t) \rangle$, where $g_{ID} = e_T(P_{pub}, Q_{ID}) \in G_T$.
Decrypt: To decrypt the ciphertext C using the private key $d_{ID} \in G_2$, compute $V \oplus H_2(e_T(tP, d_{ID})) = M$.

Masks used in encryption and decryption are the same because

$$\begin{aligned} e_T(tP, d_{ID}) &= e_T(tP, sQ_{ID}) \\ &= e_T(P, Q_{ID})^{ts} \\ &= e_T(sP, Q_{ID})^t \\ &= e_T(P_{pub}, Q_{ID})^t = g_{ID}^t. \end{aligned}$$

The security of Boneh-Franklin IBE from Type 3 Tate pairing depends on (Co-DHP*) in (G_1, G_2). It is clear from the definition of Co-DHP* that the intractability of DLP in G_1 and DLP in G_2 are both necessary for the hardness of Co-DHP*. So Boneh-Franklin IBE may be more secure in this setting.

3.3.2 BLS signature scheme

Among the short signature schemes from bilinear pairings, the Boneh-Lynn-Shacham (BLS) [25] signature scheme is one of the most important schemes and has been used as a building block for many other protocols. The security of this signature scheme is also based on computational Diffie-Hellman problem. We also give implementation of this protocol by using Tate pairing on pairing-friendly elliptic curves proposed by Wang et al. Sanjeet et al. observe that BLS signature scheme cannot instantiated in Type 1 and Type 3 setting because there is no efficient method for hashing onto G_2. Now as for the subgroups G_1 and G_2 proposed by Wang, we can hash onto G_2 efficiently. So we can instantiate this scheme in Type 3 setting without any difficulty.

Let G_1 and G_2 be two order-r subgroups of elliptic curve group E with embedding degree 1 proposed by Wang et al. and let $e_T : G_1 \times G_2 \longrightarrow G_T$ be Tate pairing where $G_1 = \langle P \rangle$. Let $H : \{0,1\}^* \longrightarrow G_2$ be a hash function. The public parameters are E, P, e_T and H.

Alice's private key is an arbitrary integer $a \in \mathbb{Z}_r^*$, while her public key is $A = aP$. To sign a message m, Alice computes $M = H(m) \in G_2$ and $\sigma = aM$. Her signature on message m is σ. To verify the signed message (m, σ), Bob computes $M = H(m)$, verifies that $\sigma \in \langle M \rangle$ and accepts if and only if $e_T(P, \sigma) = e_T(A, M)$.

This verification is correct due the following properties of pairing $e(P, \sigma) = e_T(P, aM) = e_T(P, M)^a = e_T(aP, M) = e_T(A, M)$. The security of BLS signature scheme in Type 3 setting depends on (Co-DHP*) in (G_1, G_2), which is a strong assumption than the Co-DHP in Type 1 setting.

Apart from Boneh-Franklin IBE and BLS signature schemes, some other prominent schemes, for examples Boneh-Gentry-Lynn-Shacham aggregate signature scheme [26], Xun Yi identity-based signature scheme [27], Sakai-Oghishi-Kasahara identity-based key agreement scheme [28], can be instantiated by using Tate pairing on elliptic curves of embedding degree 1 proposed by Wang et al.

The computation cost of a pairing-based cryptosystem can be divided mainly into five heads: elliptic curve representation, pairing computation, point multiplication, hashing, and last subgroup membership testing. It is clear from

Wang's method that as the order of the subgroup is a large prime of low hamming with weight 4, so efficiency of generating elliptic curve is improved. More specifically this method requires about 200 ms to generate a suitable elliptic curve. However, the method of Izuta, Nogami and Morikaw [15] takes about 20 hours. Also since the constructed subgroups G_1 and G_2 are distinct subgroups of order r and $G_1 \cap G_2 = \{O\}$, so it is easy to hash onto G_2 and there is no need of subgroup membership test.

It is clear from the paper of Wang et al. that for the order r of the subgroup of 160 bits in PBCs with the parameters of Wang, we need to compute only 2593 multiplications and 1135 inverse operations. However in ordinary PBCs, we need to compute 3429 multiplications and 1515 inverse operations. As inverse operation is estimated to be 5.18 multiplication operations, so may save 24.9% of the time required to compute Tate pairing because

$$\frac{2593 + 1135 \times 5.18}{3429 + 1515 \times 5.18} = 0.751 = 75.1\%.$$

So the computation cost for all the heads mentioned above reduced significantly. Hence implementation of the Boneh-Franklin IBE, BLS signature scheme and other schemes based on elliptic curves of embedding degree 1 is significantly efficient.

4. Proposed Asymmetric Group Key Agreement (ASGKA) scheme

In this section, we propose an identity based asymmetric group key agreement scheme motivated by [11]. We design this scheme by using Tate pairing on pairing-friendly elliptic curve of embedding degree 1 proposed by Wang et al. We considered a group of n members who wanted to receive secure messages from the other participants, who may or may not be group members. Each participant is armed with a private-public key pair for authentication purposes. The algorithm for the scheme works as follows:

System setup: The group controller (U) generates the system parameters $(G_1, G_2, G_T, e_T, H, P, r)$ at this stage. In this tuple, $H : \{0,1\}^* \longrightarrow G_2$ is a cryptographic hash function, G_1 and G_2 are elliptic curve groups of prime order r, $e_T : G_1 \times G_2 \longrightarrow G_T$ is a bilinear Tate pairing and P is a generator of G_1. Also generate and propagate securely the private key (s_i) and public key (p_i) to each user.

Key establishment: At this stage, the participants of the group generate and publish the messages which will be used in generation of group encryption and decryption keys. Let $U_1, U_2, \ldots, U_n$ be the participants involved in the group. A participant U_i with identity ID_i for $1 \leq i \leq n$ in group communication will perform the following steps:

1. Randomly choose $a_i \in \mathbb{Z}_r^*, Q_i \in G_2$ and compute $R_i = a_i P \in G_1$, $E_i = e_T(P, H(ID_i) + Q_i) \in G_T$.

Table 1: Message obtained by the participants

User	U_1	U_2	U_3	...	U_n	All
U_1	-	$\sigma_{1,2}$	$\sigma_{1,3}$	...	$\sigma_{1,n}$	(R_1, E_1, ID_1, ρ_1)
U_2	$\sigma_{2,1}$	-	$\sigma_{2,3}$	...	$\sigma_{2,n}$	(R_2, E_2, ID_2, ρ_2)
U_3	$\sigma_{3,1}$	$\sigma_{3,2}$	-	...	$\sigma_{3,n}$	(R_3, E_3, ID_3, ρ_3)
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
U_n	$\sigma_{n,1}$	$\sigma_{n,2}$	$\sigma_{n,3}$	...	-	(R_n, E_n, ID_n, ρ_n)

2. For $1 \leq j \leq n$, compute $\sigma_{i,j} = Q_i + a_i H(ID_j) \in G_2$.

3. Generate a signature ρ_i on R_i by using private key s_i. In order to make the protocol efficient, one may choose an identity based signature scheme on elliptic curve.

4. Publish $\{\sigma_{i,1}, \sigma_{i,2}, \ldots, \sigma_{i,i-1}, \sigma_{i,i+1}, \ldots, \sigma_{i,n}, (R_i, E_i, ID_i, \rho_i)\}$.

When this stage is completed, each participant can get the messages as shown in table 1, where $\sigma_{i,i} = h_i + H(ID_i)^{r_i}$ is not be published to any other user in the group, but it is kept secret by the user U_i. Since the subgroups G_1 and G_2 are subgroups of an elliptic curve group, so the size of keys will reduce. Hence the key generation becomes more efficient.

Encryption key derivation: A user can compute the group encryption key $(R, E, \mathcal{H})$, where

$$R = \sum_{i=1}^{n} R_i, \quad E = \prod_{i=1}^{n} E_i \quad \text{and} \quad \mathcal{H} = \sum_{i=1}^{n} H(ID_i).$$

The group encryption key $(R, E, \mathcal{H})$ is accepted if all the signature pairs (R_1, ρ_1), $(R_2, \rho_2), \ldots, (R_n, \rho_n)$ are valid.

Decryption key derivation: To get the group decryption key, the user U_i computes $d_i = \sum_{l=1}^{n} \sigma_{l,i}$ and accepts d_i if the signature pairs $(R_1, \rho_1), (R_2, \rho_2)$, $\ldots, (R_n, \rho_n)$ are valid.

Encryption: After knowing the public parameters and the group encryption key $(R, E, \mathcal{H})$, anyone can encrypt any message $m \in G_T$ by performing the following steps:

1. Select a random integer $t \in \mathbb{Z}_r$.

2. Compute $C_1 = tP, C_2 = tR$ and $C_3 = mE^t$.

3. Communicate the ciphertext $C = (C_1, C_2, C_3)$ to the receiver.

Decryption: To find the plaintext from the ciphertext, each participant U_i can decrypt

$$m = \frac{C_3}{e_T(C_1, d_i + \mathcal{H}) e_T(C_2, H(ID_j)^{-1})}.$$

The correctness of the decryption procedure follows from a direct verification by putting the values of $C_1, C_2, C_3, d_i, \mathcal{H}, H(ID_j)$ and properties of pairing.

5. Security and performance analysis of proposed scheme

In this section, we describe the security and performance analysis of our proposed ASGKA scheme.

5.1 Security analysis

Security of proposed ASGKA scheme depends on k-Bilinear Diffie-Hellman Exponent (k-BDHE) problem in (G_1, G_2), which is defined in subsection 2.3. Some desirable security attributes of key agreement protocols are identified in [29, 30, 31, 32, 33]. These are known-key security, unknown key-share and key-compromise impersonation etc. Similar to the protocol [11], our ASGKA scheme satisfies these security attributes. Diffie-Hellman problem is believed to be harder for elliptic curves than for finite fields because the subexponential algorithms that apply to finite fields do not translate to the elliptic curve setting, where the best available attacks remain generic, exponential algorithms like Pollard rho are applicable. This means that elliptic curve groups of relatively small size achieve the same security as multiplicative groups in much larger finite fields. Also our proposed scheme is identity based ASGKA scheme in type 3 setting and an identity based protocol is used to protect information confidentiality in critical infrastructure. So our proposed ASGKA scheme is more secure than the existing ASGKA protocols.

5.2 Performance analysis

In this subsection, we give the performance analysis of our proposed ASGKA scheme. Studying the process needed to carryout encryption and decryption in the scheme, we see that we need to do addition and subtraction on the elliptic curve. Although these operations are computationally harder than the corresponding operations on a finite field but the smaller key sizes used for elliptic curve cryptosystems more than make up for this difference. So in our protocol computational overheads and storage overheads are less than that in protocols based on standard pairings.

In our proposed ASGKA scheme the subgroups G_1 and G_2 are elliptic curve subgroups and we have proved in section 3 that the construction of subgroups of prime order-r of a pairing-friendly elliptic curve of embedding degree 1 is efficient. Our proposed ASGKA scheme is based on Type 3 Tate pairing on

subgroups G_1, G_2 and we have also proved that computation of improved Tate pairing for these subgroups is more efficient. We can save 24.9% of the time required to compute Tate pairing on these subgroups. Number of pairing operations in our protocols is less than the number of pairing operations in Zhang et al.'s scheme, which is based on Type 1 pairing. So if we implement proposed ASGKA scheme with improved Tate pairing on pairing-friendly elliptic curves of embedding degree 1 proposed by Wang et al., this scheme may become more efficient than the existing asymmetric group key agreement protocols based on standard pairings.

6. Conclusion

Design and implementation of efficient pairing-based cryptosystems has been the subject of ongoing research. In this paper, we studied pairing-friendly elliptic curves of embedding degree 1 for pairing-based cryptography. We proved that conventional classification of pairings into Type 1, 2, 3 and 4 is applicable for elliptic curves of embedding 1 proposed by Wang et al. We highlighted the selection of pairing-friendly elliptic curves of embedding degree 1 for design of efficient cryptosystems. We developed cryptosystems using these pairing-friendly elliptic curves of embedding degree 1 and compared the security and efficiency aspects of these cryptosystems with the standard cryptosystems. We also proposed a new asymmetric group key agreement scheme from Tate pairing on the selected pairing-friendly elliptic curves of embedding degree 1. The optimal trade off between security and efficiency of the proposed scheme makes it suitable for many of the current practical applications.

References

[1] M. Wang, G. Dai, K-Kr. Choo, P.P. Jayaraman, R. Ranjan, *Constructing pairing-friendly elliptic curves under embedding degree 1 for securing critical infrastructures*, PLOS ONE, 11(8) (2016), 1-13.

[2] V.S. Miller, *Use of elliptic curves in cryptography*, Advanced in Cryptology-Crypto, Springer-Verlag, New York, 417-426, 1985.

[3] M. Kumar, P. Gupta, *Cryptographic Schemes Based on Elliptic Curves over the Ring* $\mathbb{Z}_p[i]$, Applied Mathematics, 7 (2016), 304-312. http://dx.doi.org/1010.4236/am.2016.73027.

[4] N. Koblitz, *Elliptic Curve Cryptosystem*, Journal of Mathematics Computation, 48(1987), 203-209.

[5] C. Cocks, R. Pinch, *Identity-based cryptosystems based on the Weil pairing*, unpublished manuscript, 2001.

[6] D. Freeman, *Constructing pairing-friendly elliptic curves with embedding degree 10*, Proc. Of algorithmic number theory, Berlin, Germany, 452-465, 2006.

[7] P. Barreto, M. Naehrig, *Pairing-friendly elliptic curves of prime orer*, Proc. of Selected Areas in Cryptography-12th International Workshop, Kingston, Canada, 319-331, 2005.

[8] R. Barbulescu, P. Gaudry, A. Guillevic, F. Morain, *Improving NFS for the discrete logarithm problem in non-prime finite fields*, Advances in Cryptology-EUROCRYPT, 9056 (2015), 129-155.

[9] R. Dutta, R. Barua, *Password-based encrypted group key agreement*, International Journal of Network Security, 3(1) (2006),23-34.

[10] Q. Wu, Y. Mu, W. Susilo, B. Qin, J. Domingo-Ferrer, *Asymmetric group key agreement*, Proc. of 'EUROCRYPT'09, 5479 (2009), 153-170.

[11] L. Zhang, Q. Wu, U.G. Nicolas, B. Qin, J. Domingo-Ferrer, *Asymmetric group key agreement protocol for open networks and its application to broadcast encryption*, Computer Networks, 55 (15) (2011), 3246-3255.

[12] R.S. Ranjani, D.L. Bhaskari, P.S. Avadhani, *An extended identity based authenticated asymmetric group key agreement protocol*, International Journal of Network Security, 17(5) (2015), 510-516.

[13] A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publisher, 1993.

[14] A.J. Menezes, *An Introduction to Pairing Based Cryptography*, https://www.math.uwaterloo.ca/ ajmeneze/publications/pairings.pdf.

[15] T. Izuta, Y. Nogami, Y. Morikawa, *Ordinary pairing-friendly curve of embedding degree 1 whose order has two large prime factors*, Proc. of IEEE Region 10 Conference on TENCON 2010, Fukuoka, Japan, 769-772.

[16] H. Lee, C. Park, *Generating Pairing-Friendly Curves with the CM Equation of Degree 1*, Proc. of 3rd International Conference on Pairing-Based Cryptography, Palo Alto, California, USA, 2009, 66-77.

[17] E. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, Journal of Cryptology, 17(2004), 277-296.

[18] N. Koblitz, A. Menezes, *Pairing-based cryptography at high security levels*, Cryptography and Coding: 10th IMA International Conference, 3796 (2005), 543-571.

[19] Z. Hu, L. Wang, M. Xu, G. Zhang, *Generation and Tate pairing computation of ordinary elliptic curves with embedding degree one*, ICICS, 8233(2013), 393-403.

[20] S. Chatterjee, A. Menezes, F. Rodrigues-Henriquez, *On Instantiating Pairing-Based Protocols with Elliptic Curves of embedding Degree one*, IEEE Transactions on Computers, PP(99)(2016), 1-1.

[21] D. Boneh, K. Rubin, A. Silverberg, *Finding composite order ordinary elliptic curves using the Cocks-Pinch method*, Journal of Number Theory, 131(2011), 832-841.

[22] V.S. Miller, *Short programs for functions on curves*, 1986 [online], Available: http://crypto.stanford.edu/miller/miller.ps.

[23] A. Shamir, *Identity based cryptosystems and signature schemes*, Advances in Cryptology-Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 196 (1985), 47-53.

[24] D. Boneh, M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal on Computing, 32 (2003), 586-615.

[25] D. Boneh, B. Lynn, H. Shacham, *Short Signatures from Weil Pairing*, Advances in Cryptology-Asiacrypt 2001, 2248 (2003), Springer-Verlag, 514-532.

[26] D. Boneh, C. Gentry, B. Lynn, H. Shacham, *Aggregate and verifiably encrypted signatures from bilinear maps*, Advances in Cryptology-EUROCRYPT'03, 2656 (2003), 416-432.

[27] X. Yi, *An Identity-Based Signature Scheme from Weil Pairing*, IEEE Communication Letters, 7(2)(2003), 76-78.

[28] R. Sakai, K. Oghishi, M. Kasahara, *Cryptosystems based on pairing over elliptic curve*, The 2000 Symposium on Cryptography and Information Security, 2000.

[29] M. Burmester, Y. Desmedt, *A secure and efficient conference key distribution system*, Proc. of EUROCRYPT'94, 950 (1995), 275-286.

[30] S. Blake-Wilson, D. Johnson, A. Menezes, *Key agreement protocols and their security analysis*, Cryptography and Coding, 1355(1997), 30-45, Springer-Heidelberg.

[31] W. Diffie, P. Oorschot, M. Wiener, *Authentication and Authenticated Key Exchanges*, Designs, Codes and Cryptography, 2(2) (1992), 107-125.

[32] C. Mitchell, M. Ward, P. Wilson, *Key Control in Key Agreement Protocols*, Electronic Letters, 34(10) (1998), 980-981.

[33] M. Kumar, P. Gupta, A. Kumar, *A novel and secure multi party key exchange scheme using trilinear pairing map based on elliptic curve cryptography*, International Journal of Pure and Applied Mathematics, 2016.

Accepted: 16.05.2017