FACTA UNIVERSITATIS (NIŠ)
Ser. Math. Inform. Vol. 35, No 5 (2020), 1451–1460
https://doi.org/10.22190/FUMI2005451B

AN IDENTITY-BASED ENCRYPTION SCHEME USING ISOGENY OF ELLIPTIC CURVES

Mojtaba Bahramian* and Elham Hajirezaei

Abstract. Identity-Based Encryption is a public-key cryptosystem that uses the receiver identifier information such as email address, IP address, name, etc, to compute a public and a private key in a cryptosystem and encrypt a message. A message receiver can obtain the secret key corresponding with his privacy information from private key generator and he can decrypt the ciphertext. In this paper, we review Boneh-Franklin's scheme and use a bilinear map and Weil pairing's properties to propose an identity-based cryptography scheme based on isogeny of elliptic curves.

Keywords: Identity-based encryption; elliptic curves; isogeny of elliptic curves.

1. Introduction

Public key encryption (PKE), involves two distinct keys, public key, and private key. The public key can be widely distributed without compromising its corresponding private key. Identity-Based Encryption (IBE) is a public-key encryption scheme in which the public key can be an arbitrary string. Identity-based encryption is a cryptographic scheme, which enables any pair of users to communicate securely without exchanging secret or public keys. Actually by the identity-based scheme, if you know somebody's name or email address you can send him a message which only he can read. This issue has now been particularly attended by cryptographic researchers and so far, many cryptography schemes are based on it has been presented.

The basic identity scheme was first proposed by Shamir [11] in 1984. The scheme is specified by four phases:

1. **Setup:** In this phase, general system parameters and master-key are created.

2. **Extraction:** In this algorithm, the private key associated with an arbitrary public key string $ID \in \{0,1\}^*$ is created by using the master-key.

Received May 20, 2020; accepted November 25, 2020
2020 *Mathematics Subject Classification.* Primary 11T71; Secondary 11G07, 14K02

3. **Encryption:** A message is encrypted using the public key ID.
4. **Decryption:** An encrypted message is decrypted having the corresponding private key.

When the sender, Alice, sends an e-mail to the receiver, Bob, at bob@email.com, she simply encrypts her message having the public key string "bob@email.com". In this method, we need a trusted third party known as "Private Key Generator" (PKG), which computes a master private key and a public key. The PKG has a privileged position by knowing some secret information that enables it to compute the private keys for all the users in the system. Thus, when Bob receives the encrypted message by his e-mail, he contacts to the PKG, authenticates himself to it in the same way, then he obtains his private key from the PKG, and he can read his e-mail [1,6]. The problem of constructing an IBE was an open problem for many years. Finally, Boneh and Franklin [1] proposed an IBE scheme using bilinear maps in 2001. Soon after Boneh and Franklin's announcement, it was detected that Clifford Cocks, had designed a simple IBE years earlier.

Boneh and Franklin presented a functional IBE scheme in which the performance of their approach is similar to the performance of ElGamal encryption in $\mathbb{F}_q^*$, and the security of their scheme is based on the Computational Diffie-Hellman (CDH) hypothesis on elliptic curves.

In this paper, we propose an identity-based encryption scheme based on the isogenies between elliptic curves. The security of our scheme is based on the hardness of the isogeny problem that is finding an isogeny between two given isogenous elliptic curves. In our proposed scheme we use the endomorphism ring of an ordinary elliptic curve E, (End(E)), and some its properties such as the commutativity of $End(E)$.

Basic Concepts of IBE. As mentioned earlier, in the IBE scheme Alice can use the receiver's identifier information which is presented by any string, such as email address or IP address, even a digital image [10], to encrypt a message. Bob obtains a private key corresponding to his identifier information from the trusted third party, then he can decrypt the ciphertext (Fig. 1.1).

Universally an identity-based encryption scheme is specified by four randomized algorithms:

1. **Setup:** First, the PKG creates a public key pk_{PKG} and a master private key sk_{PKG}, then he publishes pk_{PKG} as a public key.
2. **Extraction:** Bob authenticates himself to the PKG and receives his private key sk_{Bob} corresponding to his identity, ID_{Bob}.
3. **Encryption:** Alice encrypts her message, M to the ciphertext C using ID_{Bob} and pk_{PKG}.
4. **Decryption:** Bob decrypts the ciphertext C, using his private key, sk_{Bob} and reconstruct the message M.

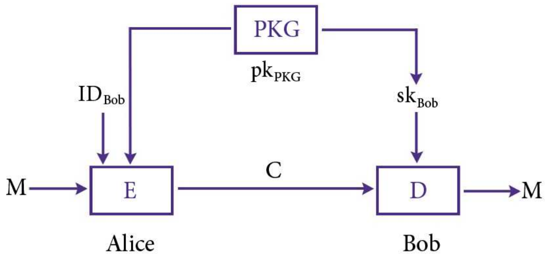

Fig. 1.1: Identity-based encryption scheme

The rest of the paper is organized as follows: Section 2 contains a summary of some preliminaries on elliptic curves, isogenies, and basic properties of the Weil pairing. In section 3, we give a review of Boneh and Franklin's IBE scheme. Our proposed identity-based encryption scheme is given in Section 4. Finally, we dedicate the security analysis of our scheme in Section 5.

2. Preliminaries

In this section, we first briefly introduce elliptic curves, isogenies and Weil pairing (see [12, 15]).

2.1. Elliptic Curves

Elliptic Curve Cryptography (ECC) was introduced by Koblitz [5] and Miller [8] in 1985. They proposed completely different cryptographic use of elliptic curves. The main reason for the attractiveness of ECC is the fact that there is no subexponential algorithm known for solving the Discrete Logarithm Problem (DLP) on a properly chosen elliptic curve. We will refer to it later.

Definition 2.1. Let K be a field of characteristic not equal to 2 and 3. An elliptic curve E over K is a curve given by a (short) Weierstrass equation of the form

$$y^2 = x^3 + Ax + B \tag{2.1}$$

where $A, B \in \overline{K}$, and its discriminant, $\Delta = -16(4A^3 + 27B^2)$ is nonzero. The j-invariant of the elliptic curve E is defined by

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

furthermore, any elliptic curve E can be determined by its j-invariant. In other words, two elliptic curves with the same j-invariant are isomorphic over K.

We say that the elliptic curve $E : y^2 = x^3 + Ax + B$ is defined over K, where $A, B \in K$. For the elliptic curve E defined over K, the set of K-rational points of E is defined by

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

where, $\mathcal{O}$ is the point at infinity.

The set $E(K)$ forms an abelian additive group with identity element $\mathcal{O}$. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on the curve. The sum of P and Q is defined as $R = P + Q = (x_R, y_R)$ where,

1. If $x_P \neq x_Q$, then $x_R = m^2 - x_P - x_Q$ and $y_R = m(x_P - x_R) - y_P$, where $m = (y_Q - y_P)/(x_Q - x_P)$.
2. If $x_P = x_Q$ and $y_P \neq y_Q$, then $R = \mathcal{O}$.
3. If $P = Q$ and $y_P \neq 0$, then $x_R = m^2 - 2x_P$ and $y_R = m(x_P - x_R) - y_P$, where, $m = (3x_P^2 + A)/2y_P$.
4. If $P = Q$ and $y_P = 0$, then $R = \mathcal{O}$.
5. If $Q = \mathcal{O}$, then $R = P$.

For the Weierstrass equation described by (2.1), if $P = (x, y)$, then $-P = (x, -y)$.

Suppose E is an elliptic curve defined over a field K and Let n be a positive integer, the n-torsion subgroup of E defined as follows

$$E[n] = \{P \in E(\overline{K}) \mid nP = \mathcal{O}\}.$$

If the characteristic of K does not divide n, or is zero, then $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$, and if the characteristic of K is $p > 0$, $n = p^r n'$ with $p \nmid n$, then $E[n] \cong \mathbb{Z}_{n'} \times \mathbb{Z}_n$ or $\mathbb{Z}_{n'} \times \mathbb{Z}_{n'}$. For the elliptic curve E defined over the finite field $\mathbb{F}_q$, $q = p^r$ for some prime p, we say that E is supersingular if $E[p] = \{\mathcal{O}\}$, and E is called ordinary if $E[P] \cong \mathbb{Z}_p$.

Let the elliptic curve E defined over the field $\mathbb{F}_q$. Then $E(\mathbb{F}_q) \cong Z_n$ for some integer $n \geq 1$, or $E(\mathbb{F}_q) \cong Z_{n_1} \times Z_{n_2}$ for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2. By Hasse's theorem, for elliptic curve E over the finite field $\mathbb{F}_q$, the order of E satisfies $\mid q + 1 - \#E(\mathbb{F}_q) \mid \leq 2\sqrt{q}$. The trace of the elliptic curve E denoted by a_q, is $a_q = q + 1 - \#E(Fq)$. The elliptic curve E is supersingular if and only if $a_q \equiv 0 \pmod p$, it means that $\#E(\mathbb{F}_q) \equiv 1 \pmod p$.

Discrete Logarithm Problem: Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$, $P \in E$ and $Q \in \langle P \rangle$. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem of finding integer n such that $Q = nP$. It is Well-known that the fastest known algorithm to solve the ECDLP over an arbitrary curve is Pollard's rho method, which has exponential time complexity. [9].

2.2. Isogeny of Elliptic Curves

Definition 2.2. Let K be a field and let E_1 and E_2 be two elliptic curves defined over K. An isogeny is a non-constant morphism $\varphi : E_1(\overline{K}) \to E_2(\overline{K})$ satisfying $\varphi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. The isogeny φ can be displayed by

$$\varphi : (x, y) \to \left(\frac{p(x)}{q(x)}, \frac{r(x)}{s(x)}y\right)$$

with polynomials $p(x)$, $q(x)$, $r(x)$ and $s(x)$ such that $p(x)$ and $q(x)$ do not have a common factor. The degree of isogeny φ denoted by $\deg(\varphi)$, is the maximum degree of the polynomials $p(x)$ and $q(x)$. Also, we define $\deg(\mathbf{0}) = 0$. The isogeny φ is called separable, if $\deg(\varphi) = \#ker(\varphi)$. We say that two elliptic curves E_1 and E_2 are l-isogenous when there exists a nonzero isogeny of degree l from E_1 to E_2. If $\varphi : E_1 \to E_2$ is an isogeny of degree l, then the dual of φ denoted by $\hat{\varphi}$, is a unique isogeny from E_2 to E_1 of the same degree l, such that $\hat{\varphi} \circ \varphi = [l]_{E_1}$, the multiplication by l map on E_1 and also, $\varphi \circ \hat{\varphi} = [l]_{E_2}$. By Tate's theorem [9], two elliptic curves E_1 and E_2 are isogenous over the finite field $\mathbb{F}_q$, if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. We denote the set of isogenies from E_1 to E_2 by $Hom(E_1, E_2)$. The sum of two isogenies φ and ψ is defined by $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$, for each $P \in E$. It implies that $\varphi + \psi$ is an isogeny, and thus $Hom(E_1, E_2)$ is a group. If $E_1 = E_2$, then we can also compose isogenies. If E is an elliptic curve, we let $End(E) = Hom(E, E)$ be the ring whose addition law is as given above and whose multiplication is composition, $(\varphi\psi)(P) = \varphi(\psi(P))$. The ring $End(E)$ is called the endomorphism ring of E. The Frobenius endomorphism τ_q is defined by $\tau_q(x, y) = (x^q, y^q)$. It is an endomorphism of E (see [15]).

2.3. Bilinear Map

Let G_1 be an additive group of order r and G_2 be a multiplicative group of the same order. A function $e : G1 \times G1 \to G_2$ is said to be a bilinear pairing if the following properties hold

1. **Bilinearity**: for all $P, Q \in G_1$ and $a, b \in \mathbb{Z}_r^*$, $e(aP, bQ) = e(P, Q)^{ab}$.
2. **Non-degeneracy**: there exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. **Computability**: for all $P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

As we will say in section 2.4, the example of an efficiently computable non-degenerate the bilinear map is the Weil pairing.

2.4. Weil Pairing

As already mentioned if E be an elliptic curve over a field K and let n be an integer not divisible by the characteristic of K, Then $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$. Let

$$\mu_n = \{x \in \overline{K} | x^n = 1\},$$

be the group of n-th roots of unity in K.Since n is not divided by the characteristic of K, the equation $x^n = 1$ has no multiple roots so, it has n distinct roots in $\overline{K}$, Therefore, μ_n is a cyclic group of order n. Any generator γ of μ_n is called a primitive nth root of unity. This is equivalent to saying that $\gamma^k = 1$ if and only if k divided by n.

Definition 2.3. Let E be an elliptic curve over a field K and let n be a positive integer not divisible by the characteristic of K. Then there is a pairing

$$e_n = E[n] \times E[n] \to \mu_n \tag{2.2}$$

called the Weil Pairing. This concept satisfies the following properties:

1. e_n is bilinear in each variable. This means that

   $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T) \tag{2.3}$$

   and

   $$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2) \tag{2.4}$$

   for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. e_n is nondegenerate in each variable. This means that if $e_n(S, T) = 1$ for all $T \in E[n]$ then $S = \infty$ and also that if $e_n(S, T) = 1$ for all $S \in E[n]$ then $T = \infty$.

3. $e_n(T, T) = 1$ for all $T \in E[n]$.

4. $e_n(S, T) = e_n(T, S)^{-1}$ for all $S, T \in E[n]$.

5. $e_n(\sigma(S), \sigma(T)) = \sigma(e_n(S, T))$. For all automorphism σ of $\overline{K}$ such that σ is the identity map on the coefficient of E (if E is in Weiratrass form, this means that $\sigma(A) = A$ and $\sigma(B) = B$).

6. $e_n(\alpha(S), \alpha(T) = e_n(S, T)^{\deg(\alpha)}$ for all separable endomorphisms α of E.

If the coefficient of E lie in a finite field $\mathbb{F}_q$, the statement also holds when α is the Frobenius endomorphism τ_Q. (Actually, the statement holds for all endomorphism α, separable or not.)

Now we say that the isogenies φ and $\hat{\varphi}$ are dual (or adjoint) concerning the Weil pairing. Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves and let $\hat{\varphi}$ be its dual, and let e_n be a Weil pairing. Then $e_n(\varphi(S), T) = e_n(S, \hat{\varphi}(T))$ for all n-torsion points $S \in E_1[n]$ and $T \in E_2[n]$ (see [7]).

3. Boneh-Franklin Scheme

Boneh and Franklin's Scheme can be built from any bilinear map $\hat{e} : G_1 \times G_1 \to G_2$ between two groups G_1 and G_2 as long as a variant of the computational Diffie-Hellman problem in G_1 is hard. They use the Weil pairing on elliptic curves as an example of such a map. They describe the scheme in four phases:

1. **Setup:** The PKG specifies an elliptic curve E over $\mathbb{F}_p$. It Chooses an arbitrary $P \in E/\mathbb{F}_p$ of order q. The PKG also specifies two hash functions $H_1 : \mathbb{F}_{p^2} \to \{0,1\}^n$ and $H_2 : \{0,1\}^* \to \mathbb{F}_p$. The PKG picks a random $s \in Z_q^*$ as a master key and denoted it by pk_{PKG}. Then it computes a public key $pk_{PKG} = sP$. The PKG publishes $\{E, \mathbb{F}, P, H_1, H_2, pk_{PKG}\}$.

2. **Extraction:** Bob contacts the PKG to get his private key. The PKG first maps, Bob's identity, $ID_{Bob} \in \{0,1\}^*$ to a point $Q_{ID} \in E/\mathbb{F}_p$ of order q, then it computes $sk_{Bob} = sQ_{ID}$ where $Q_{ID} = H_1(ID)$ and s is the master key.

3. **Encryption:** Alice encrypt her message $M \in \{0,1\}^l$ (where l denotes the length of M). under the public key, pk_{PKG} and ID_{Bob} which is mapped to a point $Q_{ID} \in E/\mathbb{F}_p$ of order q. She computes $U = rP$ and $V = H_2(\hat{e}(Q_{ID}, pk_{PKG})^r) \oplus M$, where r is chosen at random from Z_q and $Q_{ID} = H_1(ID)$. The resulting ciphertext $C = (U, V)$ is sent to Bob.

4. **Decryption:** Bob receives the ciphertext C, and checks it. If $U \in E/\mathbb{F}_p$ is not a point of order q rejects the ciphertext. Otherwise, to decrypt C using his private key, sk_{Bob} and computes:

   $$V \oplus H_2(\hat{e}(sk_{Bob}, U)) = M \tag{3.1}$$

   This completes the description as follows:

   $$\begin{aligned} \hat{e}(sk_{Bob}, U) &= \hat{e}(sQ_{ID}, rP) \\ &= \hat{e}(Q_{ID}, P)^{sr} \\ &= \hat{e}(Q_{ID}, pk_{PKG})^r \end{aligned}$$

   Thus, applying decryption after encryption produces the original message M as required.

4. Proposed Scheme

This section details our newly proposed identity-based encryption using isogeny of elliptic curves.

Let $\mathbb{F}_q$ be the field of order q, where q is a power of a prime number p and n be a positive integer coprime to p. Let E be an ordinary elliptic curve over $\mathbb{F}_q$, and let

$e_n : E[n] \times E[n] \to \mu_n$ be the Weil e_n-pairing. In our scheme, we use an algorithm $\mathcal{A}$ to convert a string $ID_{Bob} \in \{0,1\}^*$ to a point $Q_{ID} \in E$ of order n.

The phases in the proposed scheme are Setup phase, Extraction phase, Encryption phase and Decryption phase. The procedure of our scheme is described in detail as follows:

1. **Setup:** The PKG randomly chooses an isogeny $\varphi \in End(E)$ as its master key and maps $ID_{Bob} \in \{0,1\}^*$ to a point $Q_{ID} \in E[n]$ by using algorithm $\mathcal{A}$. The PKG computes a public key as follows:

$$pk_{PKG} = \varphi(Q_{ID}),$$

   and publishes $\{E, q, \varphi(Q_{ID})\}$.

2. **Extraction:** The PKG computes Bob's private key $sk_{Bob} = \hat{\varphi}(Q_{ID})$, and sends it to Bob.

3. **Encryption:** Alice encrypts the message M using Bob's public key, ID_{Bob}, by performing the following steps:

   a) She uses algorithm $\mathcal{A}$ to map ID_{Bob} into the point $Q_{ID} \in E[n]$.

   b) She chooses an isogeny $\psi \in End(E)$.

   c) She sets the ciphertext to be $C = (u, v)$, where

$$u = \psi(Q_{ID}),\ v = e_n(\varphi(Q_{ID}), \hat{\psi}(Q_{ID})) + M,$$

   then she sends $C = (u, v)$ to Bob.

4. **Decryption:** Upon receiving $C = (u, v)$, Bob computes

$$\begin{aligned} e_n(u, sk_{Bob}) &= e_n(\psi(Q_{ID}), \hat{\varphi}(Q_{ID})) \\ &= e_n(Q_{ID}, \hat{\psi}(\hat{\varphi}Q_{ID})) \\ &= e_n(Q_{ID}, \hat{\varphi}(\hat{\psi}(Q_{ID})) \\ &= e_n(\varphi(Q_{ID}), \hat{\psi}(Q_{ID})), \end{aligned}$$

   and extracts the original message $M = v - e_n(\psi(Q_{ID}), \hat{\varphi}(Q_{ID}))$ as required.

5. Security analysis

In this section, we analyze the security of our proposed scheme, which is based on the hardness of some isogeny problems as stated in the following.

> **Problem 1** (Isogeny Problem): For two given isogenous elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.
>
> **Problem 2** (Isogeny Logarithm Problem): Let E_1 and E_2 be two isogenous elliptic curves, $P \in E_1$ and $Q \in E_2$. Find an isogeny $\varphi : E_1 \to E_2$ such that $Q = \varphi(P)$.

Problem 1 is a hard problem that has been studied by many researchers [2, 3, 4, 6, 13]. The hardness of this problem over ordinary curves is as hard as the discrete logarithm problem, so its security is at the same level. Problem 2 is even harder than problem 1 because it must satisfy the extra term $Q = \varphi(P)$.

Generally, as mentioned earlier, there is no efficient algorithm to find an isogeny between two elliptic curves and it seems hard to determine the structure of $Hom(E_1, E_2)$ and also $End(E)$. Furthermore according to isogeny logarithm problem there is no efficient algorithm to find an isogeny φ by having P and $Q = \varphi(P)$.

Forward secrecy: Recall that in our proposed scheme, the public parameters are $\{E, \mathbb{F}_q, \varphi(Q_{ID})\}$. Suppose Eve (the adversary) knows $pk_{PKG} = \varphi(Q_{ID})$. To extract a message M, he must compute $e(\varphi(Q_{ID}), \hat{\psi}(Q_{ID}))$. But having E, he could get no knowledge of isogeny $\varphi \in End(E)$. Without the knowledge, this is exactly an isogeny problem that Eve is not able to solve, hence he cannot compute $e(\varphi(Q_{ID}), \hat{\psi}(Q_{ID}))$.

Acknowledgments

This research is partially supported by the University of Kashan under grant number 890195/007.

REFERENCES

1. D. Boneh, M. Franklin, Identity-Based Encryption from the Weil Pairing, Proceedings of CRYPTO 2001, LNCS 2139, Springer-Verlag, 2001, 213-229.
2. A. Childs, D. Jao, V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, J. Math. Cryptol. 8134 (2014), no. 1, 1-29.
3. S. D. Galbraith, Constructing isogenies between elliptic curves over finite fields, LMS J. Comput. Math. 2 (1999) 118-138.
4. S. D. Galbraith, A. Stolbunov, Improved algorithm for the isogeny problem for ordinary elliptic curves, Appl. Algebra Engrg. Comm. Comput. 24 (2013), no. 2, 107-131.
5. N. Koblitz, Elliptic curve cryptosystems, Mathematics of computation, 48(177), (1987), 203-209.
6. D. Kohel, Endomorphism rings of elliptic curves over finite fields, PhD Thesis, University of California at Berkeley, 1996.
7. A. J. Menezes, S. A. Vanstone, Elliptic curve cryptosystems and their implementation. Journal of Cryptology, 6(4): (1993), 209-224.
8. V. S. Miller, Use of elliptic curves in cryptography, In Advances in Cryptology CRYPTO85 Proceedings, Springer (1986), 417-426.
9. J.M. Pollard, Monte Carlo Methods for index Computation (mod p). Math. Comp. 32(143) (1978) 918–924.
10. A. Sahai, B. Waters, Fuzzy Identity Based Encryption, IACR ePrint Archive, Report 2004/086. (http://eprint.iacr.org/).

11. A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO '84, LNCS 196, Springer-Verlag (1984), 47-53.

12. J. H. Silverman, The arithmetic of elliptic curves, Vol. 106 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1986.

13. A. Stolbunov, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, Adv. Math. Commun. 4 (2010), no. 2, 215-235.

14. J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math 2 (1966) 134-144.

15. L.C. Washington, Elliptic Curves, Number Theory and Cryptography, CRC Press, 2nd edition, 2008.

M. Bahramian
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
e-mail: bahramianh@kashanu.ac.ir

E. Hajirezaei
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
e-mail: elhamhajrezaei021@gmail.com