A Pairing Free Secure Identity-based Aggregate Signature Scheme under Random Oracle

Eman Abouelkheir
Electrical Department, Faculty of Engineering, Kafr Elsheikh University, Egypt
E-mail: emanabouelkhair@eng.kfs.edu.eg

Jolanda G. Tromp
Department of Computer Science, State University of New York Oswego, USA
E-mail: jolanda.tromp@oswego.edu

Keywords: information security, aggregate signature, without parings, security proof, random oracle

Received: November 15, 2016

The signature aggregation is efficient for the communication links as the time complexity is independent of n different users. The bilinear pairing requires super-singular elliptic curve groups that have a spacious range of elements. Also, the point multiplication over elliptic curve is less computational cost than the pairings, therefore, the pairing-based schemes expose more computational complexity than schemes that without pairings. This paper introduces a new efficient and secure pairing free signature scheme based on the idea of aggregation. Also, the proposed scheme without pairings offers lower computational cost than other schemes from pairings as it saves 68.69% from computations.

Povzetek: Ta prispevek se ukvarja s kriptografskimi algoritmi, konkretno s shemo digitalnih podpisov. Opisana je izboljšava obstoječega algoritma, ki dosega pohitritev za dve tretjini, hkrati ostaja varna.

1 Introduction

Cryptography has two primitive issues; confidentiality and authentication. Digital signature achieves the authentication issue. Also, for efficient communication links, schemes should provide low time complexity. Moreover, low time complexity is useful for battery and bandwidth saving of the channel in networks [1].

There are many cryptographic algorithms provide privacy, such as signature schemes, authentication schemes, and encryption schemes [2]. For providing privacy and anonymity to a user, these schemes have to be properly combined. Schemes and methods such as group signature schemes, blind signatures, aggregate signatures, zero-knowledge proof methods, homomorphic encryption schemes offer several useful privacy-enhancing properties, e.g. identity hiding, binding information, data confidentiality, unlinkability, intracebility, etc. Recently, many applications and services require privacy protection over communication systems. The current secure communication systems support authentication, data integrity, and non-repudiation. But, the communication systems users and providers can need different security properties that are out of basic security properties. These advanced properties are usually connected with user privacy. The following text summarizes the advanced security properties and requirements.

• Privacy/Anonymity - privacy protection is ensured for every user in the system who follows the rules. Users can communicate anonymously. Their identities can be revealed only in special cases, e.g. when a user breaks a rule, authority order, police order, emergency events etc. Two types of privacy protection can be distinguished: a basic anonymity to protect a user identity against passive attacks and a full anonymity to protect also against active attacks [3]. Signatures needed when an attacker gets access to all old messages. When the unlinkability property ensured, then the attacker is not able to connect certain signatures together.

- Responsibility/revocation - every user, has to be revealed and revoked using the certain key when breaking the rules of a system. The revocation assures that the revoked user has no rights in whole systems afterward. The revocation helps protect the system against repeated misusing. In some applications, the traceability of malicious users' messages is demanded.
- Efficient and secure key management - key exchange, revocation, and establishment in systems have to be efficient computationally/memory low cost and secure. In privacy-preserving solutions, key management has to keep user privacy.
- Efficient and secure execution of cryptographic protocols - the phases of a cryptographic protocol should be as efficient as possible to minimize the negative influence of a system, especially, if the restricted devices have been deployed.
- Exculpability - neither revocation or key manager, can be able to generate a valid signature behalf another user who hold trace keys. The user cannot be accused that makes signature which he does not make. This property is mainly needed in group signature schemes,

i.e exculpability that is ensured in [4] by Boneh, Boyen and Shacham.

The aggregate signature idea arises from those different signers aggregated into a concise aggregate signature on different documents[5]. Using the aggregate signatures instead of using n signature by n different users in many application such as key distribution in PKI reducing the communication overhead and offer efficient computational cost.

Another example, in router securing system, each router need to sign its part of a route in the communication link then transmits all the signatures to the following router. Without the aggregation concept, transmitting the different signatures exposes high communication overhead[6]. The aggregate signature could be used instead of individual signs for this goal. Recently, there are two signature schemes are proposed. The first one [5] provides flexible aggregation based on pairings. The second [7] provides only sequential aggregation using certified trapdoor permutations. For the schemes in [5,7], the authors proposed aggregates signature schemes which size is independent of n users. Specifying individual signers by some public information needed for public verification. Aggregate signature schemes that specify the signers with their public information may be similar as the traditional signatures and both are not efficient. Thus, specifying the signers with their identities is more useful than specifying them by their public keys.

Cryptography from pairings has many prime properties. It is supposed that Pairing-based cryptography with smaller parameters can present a desired security level as the general elliptic curve cryptography. Suppose that there is an elliptic curve E has elements defined over F_q. But the pairing-based cryptography is working with the functions and elements defined over F_q^k, where k is some random and chosen to be secure. Either the elliptic curve hard problem (ECDLP) defined over $E(F_q)$ or the discrete logarithm problem (DLP) defined over F_q^{k*} are basic problems that the cryptography from pairings security depends on [8]. Because of the previous clarification, this paper introduces a new pairing-free signature aggregation scheme based on the general elliptic curve cryptosystem depends on signers identities.

The idea behind the identity-based cryptography (IBC) [9], to use some information belongs to a signer (such as an email ID) as a user public key rather than using public-key and certificate management. Therefore, the IBC system requires Private Key Generator (PKG) that is called a trusted third party, that generates the private keys for all identities based on its master key and the signer identity. Boneh and Franklin [10] and Cocks [11] propose many identity-based encryption schemes. Also, old schemes in [9,12,13]; recent schemes and analyses include [14,15,16,17].

The concept of signature aggregation allows different signers to sign different messages. This leads to efficient communication and fewer computations. In any aggregate signature scheme n different signatures are considered as one single signature. The aggregation approach can be used instead of using public key certificates to satisfy efficient communication and computations. Aggregate signatures have many applications such as mutual authentication between vehicles in VANETs and in wireless sensor network.

The goal of my paper to introduce a new secure pairing-free aggregate signature scheme. The proposed scheme security is proven in the random oracle and assuming a hard Diffie-Hellman problem. Also, the proposed scheme saves the time complexity by 68.69% . The new aggregate signature and its analysis is the modified version of the scheme in [18].

The rest of the paper is organized as follow : section two presents the digital signature approach versus the water marking. Also, section three describes preliminaries. Then section four introduces the generic model for the proposed scheme. Moreover, section five presents the security requirements of any aggregate signatures based on user's identities. In section six and seven, the proposed scheme is presented with the formal security proof under random oracle respectively. In section eight, the results and discussion are introduced. The proposed scheme is compared with other in literature in section nine. Section ten concludes the proposed work. Finally, the future scope introduced in section eleven.

2 Digital signing versus watermarking

A digital signing is an approach of cryptography used for securing the communication links. The goal of the signature to verify the end to end communication system users.

The digital signing operation is similar to the handwritten signing operation and exactly as a paper signature. It used to verify the identity of a user using its digital certificate. This paper is concerned with the digital signature approach.

The goal of watermarking to hide the information into a digital signal that provides a copyright protection in a digital format[19]. Many watermarking schemes have been proposed. In 2012, Nilanjan Dey, Poulami Das, Sheila Sinha Chaudhuri, and Achintya Das, [20] used Alattar's method efficiently for watermark insertion and extraction for an EEG signal. In 2013, K. P. Arijit, D. Nilanjan, S. Sourav, D. Achintya, and S. Ch. Sheli [21] proposed a new technique for reversible watermarking is used for the color image .In 2014, Nilanjan Dey, Goutam Dey, Sheli Sinha Chaudhuri, and Sayn Chakraborty [22] proposed two novel blind-watermarking mechanisms are; 1- session key based blind-watermarking mechanism and 2- self-recovery based blind-watermarking mechanism, into the Electromyogram (EMG) signal. In 2015, Nilanjan Dey, Monalisa Dey , Sainik Kumar Mahanta ,and Achintya Das [23] proposed a technique is to prevent any modifications in a transmitted biomedical ECG signal. In 2016, Y. B. Amar, I. Trabelsi, D. Nilanjan and S.

Bouhlel [24] proposed watermarking scheme used for copyright protection purposes.

3 Preliminary

3.1 Bilinear pairing

Suppose G_1 is a cyclic group has an order q, q is prime. This group is generated by the point P over an elliptic curve E and defined over the prime field F_q. Let $\hat{e}$ be a pairing where $\hat{e}: G \times G \to G_T$. For any P, Q, R (points over an elliptic curve E) and $c, d \in F_q$, c, d are integers. The pairings satisfy the following properties:

- linearity: $\hat{e}(cP, dQ) = \hat{e}(P.Q)^{cd}$.
- NonDegenerate: $\hat{e}(P.P) \neq 1$.
- Easy to compute : $\hat{e}(P.Q)$ it must be easy and efficient computed.

3.2 Elliptic Curve Cryptography(ECC)

ECC is an public key cryptography approach based on the mathematics of elliptic curves. ECC is faster than RSA and uses smaller keys, but still, provides the same level of security .

Suppose $E_q(a,b)$ are the set of points over the elliptic curve E that defined over the prime field F_q, E defined by $y^2 \bmod q = (x^3 + ax + b) \bmod q$ and a, b must satisfy the equation $\Delta = (4a^3 + 27b^2) \bmod q \neq 0$. The cyclic group $G_q = \{(x,y) : x, y \in F_q\}$ $(x,y) \in E/F_q$, G_q is an elliptic curve additive group. The group identity element in G_q is O ; the infinity point; The scalar multiplication on G_q defined as $k.P = P + .. + ... + P + P$. For some integer $n > 0$, a point P of order n satisfy $n \cdot P = O$. ECC was proposed in 1985, by Miller [25] and Koblitz [26]. When comparing ECC with other public key cryptosystems, it was found that ECC-based public key cryptosystem has many advantages such as low computation cost, smaller key size, low storage space cost etc. It is known that the discrete logarithm problem based on ECC (ECDLP) of any elliptic curve element that has a public point known base point, is harder than the discrete logarithm problem (DLP) over the finite field F_q

Security is not the only cryptography objective goal but also, there are many factors as the problems associated with key management and protection, hash functions , defective use of random generators, and the incompact private key software. The ECC implementation issues are [27]:

- Used in Diffie Hellman cryptosystem and also, digital signing approach.
- There are many available standardized elliptic curves approved by NIST for the multiple security requirements.
- Elliptic curves cryptosystems enable comprehensive information on algorithms.

The Benefits of elliptic curve based cryptosystems over RSA cryptosystem:

- The elliptic curve based cryptosystem key takes significantly less memory for the same security level. Table I indicates the key size for RSA and ECC for the same security level.
- Smaller key size in ECC leads to faster digital signature generation and therefore saving resources.

In the other hand, ECC has disadvantages versus RSA crypto system. It is complicated in mathematical backgrounds.

NIST guidelines for key size of ECC , RSA, and AES			
ECC	RSA	Ratio	AES
163	1024	1:6	
256	3072	1:12	128
384	7680	1:20	192
512	15360	1:30	256

Table 1: Security level of various key sizes in ECC and RSA.

3.3 Computational problems

Here, a briefly review of some mathematical problems:

Definition 3.3.1. Suppose g be a group generator of the group G where $g \in G$. The CDH related to g is how to compute g^{cd} given by (g^c, g^d), $c, d \in Z_q^*$.

Definition.3.3.2. (Computational Diffie-Hellman (CDH) Problem) over an elliptic curve. Given P point over an elliptic curve and $c, d \in Z_q^*$ then for known $(P, cP, dP) \in G_p$, it is hard to compute of cdP over the group G_q

Definition.3.3.3. (Computational Diffie-Hellman (CDH) Assumption). Let A be an adversary able to break the CDH problem with a trivial probability, if given the tuple $(P, cP, dP) \in G_p$ of CDH problem where $c, d \in Z_q^*$, then A could solve the CDH with the trivial advantage $Adv_{A,G_p}^{CDH} = Pr[A(P, cP, dP) = cdP : c, d \in Z_q^*]$.

4 Aggregate signature model

An identity-based aggregate signature scheme model has composed six algorithms:

- **Setup phase**: with input k; the security parameter; the public key generator (PKG) generates the master mpk and private keys msk and the system parameters params . Finally, the PKG publishes params , mpk and keeps msk secret.
- **Key Extract**: PKG runs this algorithm using the signer identity ID_i ;delivered by the signer U_i, param and msk as an input. The output is the signer private key d_i and the PKG sends the signer private key d_i via secure channel to the user U_i.

- **Sign**: this algorithm takes the user identity ID_i, his private key d_i, message m_i and param as input to create a valid signature σ_i on m_i by the signer U_i.
- **Aggregate**: this algorithm takes $\{\sigma_i\}_{i=1}^n$ as an input, any third party can generate the signature aggregation σ_{agg} for all the messages with their identities $\{m_i, ID_i\}_{i=1}^n$.
- **Signature Verification**: with input σ_{agg} the user U_i performs two checking operation first; whether σ_i by ID_i is a valid signature on m_i and outputs "Valid" if true otherwise , "Invalid". Second; with input ID_i and $\{m_i, ID_i\}_{i=1}^n$ checks the validity of the aggregate signature σ_{agg} on σ_i and outputs "Valid" if true otherwise , "Invalid".

5 Security algorithm

5.1 Unforgeability

The proposed scheme security model follows the scheme proposed by [18] with slight variations. The security model follows a game with three phases: setup, training and forgery phase. Two attacks in this security model are considered; adaptive chosen message and identity attacks. Thus, the scheme is secure under those attacks against any forgery. if the adversary A has not a significant advantage in any probabilistic time algorithm in this game :

- **Setup:** by executing this algorithm the challenger C obtains the parameters param and the msk and deliver the param to the adversary A.
- **Training:** A query the following oracle after the setup algorithm:
  - Extract oracle: With ID_i A makes a query and C obtains the private key d_i with ID_i and deliver it to A
  - Signing oracle: A queries the signing oracle with ID_i, m_i then generates a valid signature σ_i on m_i.
- **Forgery:** A generates an aggregate signature σ_{agg} on $\{m_i\}_{i=1}^n$ for $\{ID_i\}_{i=1}^n$ with input $\{\sigma_i\}_{i=1}^n$ in which at least target identity $ID_T \in \{ID_i\}_{i=1}^n$. The adversary A forge the signature if there is a valid σ_{agg} for a pair (ID_T, m_T) with the advantage:

$$Adv_A\{Pr[A(Verify(\sigma_{agg}) = Valid)\}$$

6 The proposed scheme

6.1 Setup

- In this phase, the PKG selects three additive groups G_1, G_2, G_3 of order q (prime number) where $q > 2^k$, k is the security parameter. Then the PKG selects two pairs of integers (a, b) satisfying $(4a^3 + 27b^2) \bmod q \neq 0$. Also, the PKG selects a generator point P of G_1 on the elliptic curve E defined by $y = (x^3 + ax + b) \bmod q$ over the finite field F_q^* and chooses a the following hash functions $H_o : \{1,0\}^* \times G_1 \times G_2 \times G_3 \to F_q^*$, $H_1 : \{1,0\}^* \times G_1 \times G_2 \to F_q^*$, and $H_2 : \{1,0\}^* \to F_q^*$
- Then, the PKG randomly picks up $s \in F_q^*$, s is msk and calculates the mpk $P_{pub} = s.P$. The PKG keeps msk secrete and the $params = (G_1, G_2, G_3 n, q, P, P_{pub}, H_o, H_1, H_2)$ public.

6.2 Key extraction

This algorithm follows the following steps:

1. Picks up randomly $x_i \in F_q^*$ and calculates $X_i = x_i.P$
2. Computes $d_i = (x_i + s.q_i) \bmod q$, for the all users $q_i = H_o(ID_i || X_i), i = 1..n$.
3. The PKG sends the corresponding secrete key $< d_i >$ and the public key $< X_i, q_i >$ to the users through a secrete channel

6.3 Signing

With input (X_i, d_i, ID_i) :

1. Selects a random number $r_i \leftarrow_R F_q^*$ and calculates: $W_i = x_i P$
2. Computes : $h_{1i} = H_1(W_i, X_i, m_i, ID_i)$, and $h_{2i} = H_2(h_{1i}, W_i, X_i, m_i, ID_i)$
3. Computes: $v_i = (r_i h_{1i} + d_i h_{2i}) \bmod q$, $Z_i = v_i.P$.

The signature of ID_i on message m_i is $\sigma_i =< Z_i, X_i, h_{1i}, h_{2i} >$

6.4 Aggregate.

On input $(\{\sigma_i, ID_i\}_{i=1}^n)$ a set of signatures $\sigma_i =< Z_i, X_i, h_{2i}, h_{1i} >$, with the identity ID_i, $i = 1..n$, $\sigma_i =< Z_i, X_i, h_{2i}, h_{1i} >$ are the signatures of the messages m_i: $Z_{agg} = \sum_{i=1}^{n} Z_i$, $Z_i = v_i.P$, $i = 1..n$

The aggregate signature will be $\sigma_{agg} = \{< Z_i, X_i, h_{1i}, h_{2i} >\}_{i=1}^n, Z_{agg}$

6.5 Signature verification.

With the input from $\sigma_{agg} = \{< Z_i, X_i, h_{1i}, h_{2i} >\}_{i=1}^{n}, Z_{agg}$ any user can verify this signature. The verification process as follow:

- Computes $W_i' = h_{1i}^{-1}[Z_i - h_{2i}(X_i + q_i P_{pub})]$ to recover W_i
- Checks if the following equations holds: $h_{1i} \stackrel{?}{=} H_1(m_i, ID_i, X_i, W_i)$ and $h_{2i} \stackrel{?}{=} H_2(m_i, ID_i, X_i, W_i, h_{1i})$

6.6 Proof of correctness

$$W_i' = h_{1i}^{-1}[Z_i - h_{2i}(X_i + q_i P_{pub})]$$

$$= \sum_{i=1}^{n} h_{1i}^{-1}[v_i P - h_{2i}(X_i + q_i P_{pub})]$$

$$= \sum_{i=1}^{n} h_{1i}^{-1}[(r_i h_{1i} + d_i h_{2i})P - h_{2i}(X_i + q_i P_{pub})]$$

$$= \sum_{i=1}^{n} h_{1i}^{-1}[(r_i h_{1i} + (x_i + sq_i)h_{2i})P - h_{2i}(X_i + q_i P_{pub})]$$

$$= \sum_{i=1}^{n} h_{1i}^{-1}[(r_i h_{1i} P + h_{2i}(X_i + q_i P_{pub}) - h_{2i}(X_i + q_i P_{pub})] = W_i$$

7 The proposed scheme security proof

The security proof demonstrates that ECDLP could be solved without significant probability ε^o . Also, An adversary A may forge this scheme without significant probability ε^o against chosen message and identity attacks

7.1 Theorem1.

The signature scheme is secure against chosen message and identity attacks if there is an adversary A with a polynomially bounded (t, ε') query for q_{H_o}, q_{H_1}, q_{H_2}, q_S and q_E who can forge the proposed scheme with a non-negligible advantage ε', C may forge the signature with a non-significant advantage:

$$\varepsilon_o = \frac{1}{9} \cdot \frac{10.(q_{sign}+1)(q_{sign}+q_{H_2}+q_{H_1}).(1-\frac{q_{Extract}}{q_{H_0}})}{2^{k+1}} \cdot \frac{1}{q_{H_1}} \varepsilon \quad (1)$$

Proof:

a) Setup

The challenger C selects a group G_1 with a generator point P. Then, C randomly selects $a \in Z_q^*$ and calculate $P_{pub'} = a.P$. C obtains the following four hash oracles: H_o, H_1, H_2 then deliver the public $param = (G_1, G_2, H_o, H_1, H_2, a.P)$ to A

A asks C for different queries as follow:

b) H_o query

- Firstly, C delivers the system parameters to A, then C with input ID, X selects q randomly and returns it to A.
- In another case, A might know the public component X that corresponds to an identity ID. When A makes a query for ID, there are two cases:
  - In the case of : $ID \in \{ID\}_{i=1}^{n}$, the challenger C suits $ID = ID_i$, computes $X = x.P$, x is anonymous, C wants to solve the ECDLP for x, as it is part of ECDLP. After this, C stores $<\perp, q, ID>$ in $H_o$list.
  - If $i \neq 1$, C selects $x, q \in Z_q^*$ randomly, sets $X = x.P$, delivers $< q, X >$ to the signer such that $q = H_o(ID \| X)$ and stores $< x, q, ID >$

c) Extract query

When A queries for the private key of ID, C does the following

- C checks the $H_o$list to verify whether or not there is an entry for ID. If $H_o list$ does not contain an entry for ID, return $\perp$
- Otherwise, if the entry corresponding to ID in $H_o$list is of the form $< ID, X, x, q >$ and returns $< x, X, *, * >$, if $ID \notin \{ID\}_{i=1}^{n}$ then C recovers the tuple $< X, x, q, ID >$ from $H_o$list and returns $< X, q, ID >$ and compute $d = x + aq$ then returns d to A.

d) H_1 query

When (m, ID, W), is submitted to H_1 queries

for the first time C returns checks of H_1list whether the tuples (m, ID, W) in $H_1 list$ C returns h_1, otherwise C chooses a new random $h_1 \leftarrow_R F_q^*$ includes $< h_1, m, ID, W >$ to the $H_1 list$ then C returns h_1

e) H_2 queries

When $< h_1, m, ID, W >$, is submitted to H_2 queries

the first time C returns checks of H_2list whether the tuples $< h_1, m, ID, W >$ in H_2list, C returns h_2, otherwise C chooses a new random $h_2 \leftarrow_R F_q^*$ includes $< h_2, h_1, m, ID, W >$ to the $H_2 list$ then C returns h_2

f) Sign Oracle

For each new query (m, ID_i), C proceeds as follows:

- If $ID_i \neq ID_1$, C signs a message m as follows:
- If the public key of ID_i has been replaced:

1) Obtains $< X_i, q_i >$ by calling H_o query oracle on ID
2) Selects $r \leftarrow_R F_q^*$ randomly, calculates: $W = r.P$.

3) Computes: $h_1 = H_1(m_i, W, ID_i, X_i)$ by calling H_1 query on input $< m, W, ID_i, X_i >$, and $h_2 = H_1(m_i, W, ID_i, X_i, h_1)$ by calling H_2 query on input $< m_i, W, ID_i, X_i, h_1 >$, and

Obtains the secrete key d from the extract query and computes: $v = (rh_1 + dh_2) \bmod q$, $Z = v.P$.

The signature of ID on message m is $\sigma = < Z, X, h_1, h_2 >$. Otherwise, C signs m in the usual manner by using x_i (obtained from the H_o query) and d_i (obtained from extract query)

- If $ID_i = ID_1$, C does the following:

1) Generates a random $h_1, h_2, v \in F_q^*$
2) Sets $v_i = v, h_{1i} = h_1, h_{2i} = h_2$
3) Computes: $Z_i = v_i P$, and $W_i = h_{1i}^{-1}[Z_i - h_{2i}(X_1 + q_1 P_{Pub'})]$
4) Updates the lists H_1 list and H_2 list respectively with the following tuples $< h_{1i}, W_i, ID_i, m_i >$ and $< h_{2i}, W_i, ID_i, m_i, h_{1i} >$. Generate a different $h_1, h_2, v \in F_q^*$ then repeat steps 3 and 4 if any entry in the list H_1 list or H_2 list is similar as the tuples generated.
5) C returns the signature $< Z_i, X_i, h_{1i}, h_{2i} >$ on m_i by ID_i .

Note the generated signature is valid due to:

$$h_{2i}X_1 + h_{1i}W_i + h_{1i}q_1 P_{Pub'Pub'}$$
$$= h_{2i}X_1 + h_{1i}[h_{1i}^{-1}[Z_i - h_{2i}(X_1 + q_1 P_{Pub'})] + h_{1i}q_1 P$$
$$= h_{2i}X_1 + Z_i - h_{2i}X_1 - h_{2i}q_1 P_{Pub'} + h_{1i}q_1 P$$
$$= Z_i = v_i P$$

This shows that $< Z_i, X_i, h_{1i}, h_{2i} >$ will able to be a valid signature to the adversary A.

7.2 Forgery phase

7.2.1 Lemma 1

After the adversary A generate $< Z_1..Z_n, X_1..X_n, Z_{agg} >$ on the message $\{m_i\}_{i=1}^n$ by user identities $\{ID_i\}_{i=1}^n$. A can generate a valid $< Z_1..Z_n, X_1..X_n, Z_{agg} >$ with probability ξ' if there exists ID_1 where $l \in \{1,..,n\}$. The algorithm could be flunk in the following places :

- For the extract oracle if the adversary queries for the ID_1 then the algorithm flunks. If q_E is the maximum extract queries number made by the adversary. The probability of non-querying for the extract phase is:

$$P[q_{Extract}(ID_i) \neq ID_1] = 1 - \frac{q_{Extract}}{q_{H_o}^*} \quad (2)$$

where $q_{H_o}^*$ is the queries maximum number .

A may success if $ID_1 \notin \{ID_i\}_{i=1}^n$ or if the adversary A make a query for the signing oracle on m_i with user identity ID_1 . This happen if:

$$Pr[ID_i = ID_1, \ \forall i = 1,..,n \ \text{ and } D_i \neq ID_1 \forall l = 1,\ldots,n, l \neq i] = \frac{n}{2.q_{H_o}^*} \quad (3)$$

From the previous probabilities, A can break the scheme under adaptive chosen message and identity attack with the advantage:

$$\varepsilon' = \varepsilon.(1 - \frac{q_E}{q_{H_o}^*})\frac{n}{2.q_{H_o}^*} \quad (4)$$

The adversary A may generate a valid aggregate signature without signer secrete key with the probability

$$\varepsilon = \frac{10(q_{sign}+1)(q_{sign} + q_{H_2} + q_{H_1})}{2^k} \quad (5).$$

7.2.2 Lemma 2

A made queries for Extract , H_o query , H_1 query , H_2 query , Sign query as the previous queries. A may generate a valid aggregate signature with probability $\varepsilon'' \geq \frac{1}{9}$ for n users. C computes $W's$ as same as the previous, and then generate a valid signature $< Z_i, X_i, Z_{agg} >$. Using two valid signatures C does the following:

$$Z_{agg} = \sum_{i=1}^{n} v_i.P = (\sum_{i=1}^{n} r_i h_{1i} + \sum_{i=1}^{n} d_i h_{2i}).P$$

$$Z'_{agg} = (\sum_{i=1}^{n} r_i h_{1i} + \sum_{i=1}^{n} d_i h'_{2i}).P$$

$$Z_{agg} - Z'_{agg} = \sum_{i=1}^{n} d_i (h_{2i} - h'_{2i}).P$$

$$Z_{agg} - Z'_{agg} - \sum_{i=1, i\neq l}^{n} d_i (h_{2i} - h'_{2i}).P = d_l (h_{2l} - h'_{2l}).P$$

Thus C knows all the private keys multiplied the point P over the elliptic curve by $d_l(h_{2l} - h'_{2l}).P$. Also, C knows $d_l.P$ by multiplying the final equation by $(h_{2l} - h'_{2l})^{-1}$, but C cannot get d_l unless solving the ECDLP and it is hard under the assumption (ECDLP). C might solve ECDLP with probability:

$$\varepsilon_o = \frac{10(q_{sign}+1)(q_{sign} + q_{H_2} + q_{H_1})}{2^k}.(1 - \frac{q_{Extract}}{q_{H_o}^*}).\frac{n}{2q_{H_o}^*}.\frac{1}{9} \quad (6)$$

$$= \frac{1}{9}.\frac{10(q_{sign}+1)(q_{sign} + q_{H_2} + q_{H_1})(1 - \frac{q_{Extract}}{q_{H_o}^*}).n}{2^{k+1}}.\frac{1}{q_{H_o}^*} \quad (7)$$

By this, the proposed identity based aggregate signature over is secure against any forgery with a non-

significant probability ε_o. Under this assumption C might solve the ECDLP

8 Results and discussion

When analyzing time complexity of the proposed scheme, it is found that it consumes only two point multiplication over elliptic curve in an individual signing process. Through the verification process, the proposed scheme consumes two point multiplication, one modular inverse operation and two point addition over the elliptic curve. All the computations are relative to the modular multiplication process. The proposed scheme consumes 127.84 T_{ML} in one individual complete signing and verification process

9 Comparative study

This section shows the comparative study between the proposed signature scheme without pairing with the scheme with pairings in [28] in the case of individual signing. The computations are all relative to the modular multiplication. Table II indicates the definitions for the cryptographic operations.

Notation	Description
T_{ML}	The time complexity needed to execute the modular multiplication
T_{EM}	The time complexity needed to execute elliptic curve scalar point multiplication, $1T_{EM} \approx 29T_{ML}$
T_{BP}	The time complexity needed to execute the pairings operation, $1T_{BP} \approx 3T_{EM} \approx 87T_{ML}$
T_{PX}	The time complexity needed to execute pairing-based exponentiation, $1T_{PX} \approx \frac{1}{2}T_{BP} \approx 43.5T_{ML}$
T_{EA}	The time complexity needed to execute the point addition over elliptic curve, $1T_{EA} \approx 0.12T_{ML}$
T_{IN}	The time complexity needed to execute the modular inversion operation, $1T_{IN} \approx 11.6T_{ML}$

Table 2: Definition of different cryptographic operations.

The scheme in [28] uses the identity-based signature from pairings. Craig and Zulfikar scheme consumes 406.24 T_{ML} in an individual signing operation while, the proposed pairing free scheme consumes 127.84 T_{ML} in an individual operation and therefore the proposed scheme shows lower time complexity than in [28], as it saves 68.69% from the computations as in table III.

10 Conclusion

This paper introduces a new aggregate signature scheme without pairings. It saves 68.69% of computational cost than another scheme in [28] in pairings. The security proof of the proposed scheme shows that it is secure in random oracle model. The aggregate signature schemes are very useful when needing authentication in vehicular ad hoc network and e-commerce applications.

11 Future scope

The idea of the aggregate signature used in securing the communication networks such as vehicular area network VANETs and Mobile area networks MANETs. Also , aggregate signature used in the e-commerce applications. The proposed scheme should be used in VANETs to provide aggregate authentication with low computational cost.

	Signature				**Verification**				Total (in T_{ML})
	T_{EM}	T_{BP}	T_{IN}	T_{EA}	T_{EM}	T_{BP}	T_{IN}	T_{EA}	
Craig, and Zulfikar	4	-	-	-	1	3	-	2	406.24 T_{ML}
IDB-ASC	2	-	-	-	2	-	1	2	127.84 T_{ML}

Table 3: Comparison of computational cost.

12 References

[1] K. C. Barr and K. Asanovic. Energy Aware Lossless Data Compression. In Proceeding of Mobisya 2005

[2] A. Prace. Privacy Preserving Cryptographic Protocols For Secure Heterogeneous Networks. *Thesis of Doctoral, 2014*

[3] X. Boyen and B. Waters. Full Domain Subgroup Hiding and Constant Size Group Signatures In Public Key Cryptography. *Lecture notes in computer science, vol. 4450, pp.1-15, 2007*

[4] D. Boneh, X. Boyen and H. Shacham. Short Group Signatures. In Advances in Cryptology- CRYPTO 2004, Springer , pp. 227-242.

[5] D. Boneh, C. Gentry, B. Lynn and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. *In Proceeding of Eurocrypt 2003, vol. 2656 of LNCS, pp. 416–432.*

[6] S. Kent, C. Lynn and K. Seo. Secure border gateway protocol (secure-bgp). *IEEE Journal Selected Areas in Comm., pp.582–592, 2000.*

[7] A. Lysyanskaya, S. Micali, L. Reyzin and Shacham H. Sequential aggregate signatures from trapdoor permutations. *In Proceeding of Eurocrypt 2004, vol. 9999 of LNCS, pp. 74–90.*

[8] Z. Cao and L. Liu. On the Disadvantages of Pairing-based Cryptography. International Journal of Network Security, vol.17, no.4, pp.454-462, July 2015.

[9] A. Shamir. Identity-based Cryptosystems and Signature Schemes. *In Proceeding of Crypto 1984, vol. 196 of LNCS, pp 47–53.*

[10] D. Boneh and M. Franklin. Identity-based Encryption from the Weil Pairing. *SIAM Journal of Computing, vol.32, no.3, pp.586–615, 2003*

[11] C. Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. *In Proc. of IMA Int. Conf., vol. 2260 of LNCS, pp.360–363, 2001*

[12] Fiat A. and Shamir A., "How to prove yourself: Practical solutions to identification and signature problems", In Proceeding of Crypto 1986, vol. 263 of LNCS, pp. 186–194.

[13] L. C. Guillou and J. J. Quisquater. A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge. *In Proceeding of Crypto 1988, vol. 403 of LNCS, pp 216–231.*

[14] J. C. Cha and J. H. Cheon. An Identity-Based Signature From Gap Diffie-Hellman Groups. *In Proceeding of PKC 2003, vol. 2567 of LNCS, pp.18–30* .

[15] X. Boyen. Multipurpose Identity-Based Signcryption (A Swiss Army Knife For Identity-based Cryptography). *In Proceeding of Crypto 2003, vol. 2729 of LNCS, pp 383–399.*

[16] Libert B. and Quisquater J.-J., "*Identity based undeniable signatures*,". In Proc. of CT-RSA 2004, pp. 112–125.

[17] M. Bellare, CH. Namprempre and G. Neven. Security Proofs for Identity-Based Identification And Signature Schemes. *In Proceeding Proc. of Eurocrypt 2004, vol.3027 of LNCS, pp.268*-286.

[18] S. Sharmila, D. Selvi, S. S. Vivek, J. Shriram and C. P. Rangan. Identity Based Partial Aggregate Signature Scheme Without Pairing. *IACR Cryptology eprint Archive , 2010.*

[19] M. S. Murty, D. Veeraiah and A. S. Rao. Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis. *Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.2, June 2011.*

[20] N. Dey, P. Das, S. S. Chaudhuri , and A. Das. A Session Based Watermarking technique Within the NROI of Retinal Fundus Images for Authencation Using DWT Spread Spectrum and Harris Corner Detection. *In the Proceeding of the Fifth International Conference on Security of Information and Networks, 2012.*

[21] N. Dey, A. K. Pal, S. Samanta, A. Das, and S. S. Chaudhuri. Optimisation of Scaling Factors in Electrocardiogram Signal Watermarking using Cuckoo Search. *International Journal of Bio-Inspired Computation vol.5, no. 5, pp.315-326, 2013.*

[22] N. Dey, G. Dey, S. Chakraborty, and S. S. Chaudhuri. Feature Analysis of Blind Watermarked Electromyogram Signal in Wireless Telemonitoring. *In the series Annals of Information Systems vol. 16 pp. 205-229, 2014.*

[23] N. Dey, M. Dey, S. K. Mahata and D. Ach. Tamper Detection of Electrocardiographic Signal using Watermarked Bio-hash Code in Wireless Cardiology. *Inteligence International Journal of Signal and Imaging Systems Engineering , Vol.8, no.1-2 , 2015.*

[24] Amar, Y. B., I. Trabelsi, N. Dey, and S. Bouhlel. Euclidean Distance Distortion Based Robust And Blind Mesh Watermarking. *International Journal of Interactive Multimedia and Artificial , vo.4, No.2, pp.46-51,2016.*

[25] V. S. Miller. Use of elliptic curves in cryptography. In the Proceedings of the CRYPTO 1985, LNCS, Springer-Verlag vol.218,pp.417-426, 1985.

[26] N. Koblitz. Elliptic Curve Cryptosystem. Journal of Mathematics of Computation vol.48, pp. 203-209, 1987.

[27] K. Magons. Applications and Benefits of Elliptic Curve Cryptography. University of Latvia, Faculty of Computing, Rain¸a bulvaris 19, Riga, LV-1586, Latvia

[28] C. Gentry, and Z. Ramzan. Identity-Based Aggregate Signatures. In the Proceeding of 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, pp.24-26, 2006.