ID-Based Deniable Authentication Protocol Suitable for Mobile Devices

Jayaprakash Kar

Department of Information Systems,
Faculty of Computing and Information Technology,
King Abdulaziz University, Kingdom of Saudi Arabia
jayaprakashkar@yahoo.com

Abstract. This paper describes a secure identity based deniable authentication protocol whose security is based on difficulty of breaking Diffie-Hellman Problem on Elliptic Curve (ECDHP) and hash function. Elliptic curve cryptosystem (ECC) has significant advantages like smaller key sizes, faster computations compared with other public-key cryptography. Since it is an ECC based authentication protocol, it can be implimented in mobile devices such as smart card, PDA etc. Deniable authentication protocol enables a receiver to identify the true source of a given message, but not to prove the identity of the sender to a third party. This property is very useful for providing secure negotiation over the Internet.

Keywords: deniable authentication, ECDLP, ECDHP, HDDH, mobile device.

1 Introduction

Authentication can be realized by the use of digital signature in which the signature (signers private key) is tied to the signer as well as the message being signed. This digital signature can later be verified easily by using the signers public key. Hence, the signer will not be able to deny his articipation in this communication. Generally, this notion is known as non-repudiation. However, under certain circumstances such as electronic voting system, online shopping and negotiation over the Internet, the non-repudiation property is undesirable. It is important to note that in these applications, the senders identity should be revealed only to the intended receiver. Therefore, a significant requirement for the protocol is to enable a receiver to identify the source of a given message, and at the same time, unable to convince to a third party on the identity of the sender even if the receiver reveal his own secret key to the third party. This protocol is known as deniable authentication protocol.

2 Applications to Mobile Devices

With the rapid development of the development of electronic technology, various mobile devices (e.g., cell phone, PDA, and notebook PC) are produced and

R. Prasad et al. (Eds.): MOBISEC 2011, LNICST 94, pp. 160–171, 2012.

peoples life is made more convenient. More and more electronic transactions for mobile devices are implemented on Internet or wireless networks. In electronic transactions, remote user authentication in insecure channel is an important issue. For example, when one user wants to login a remote server and access its services, such as on-line shopping, both the user and the server must authenticate the identity with each other for the fair transaction. Generally, the remote user authentication can be implemented by the traditional public-key cryptography (Rivest et al., 1978; ElGama, l985). The computation ability and battery capacity of mobile devices are limited, so traditional public-key cryptograph, in which the computation of modular exponentiation is needed, cant be used in mobile devices.

Fortunately, Elliptic Curve Cryptosystem (ECC) (Miller, 1986; Koblitz, 1987) has significant advantages like smaller key sizes, faster computations compared with other public-key cryptography. Thus, ECC-based authentication protocols are more suitable for mobile devices than other cryptosystem. However, like other public-key cryptography, ECC also needs a key authentication center (KAC) to maintain the certificates for users public keys. When the number of users is increased, KAC needs a large storage space to store users public keys and certificates.

ECC has the highest strength-per-bit compared to other public key cryptosystems. Small key sizes translate into savings in bandwidth, memory and processing power. This makes ECC the obvious choice in this situation. However, there are other aspects that need to be taken into account. When it comes to choosing which public key cryptosystem to employ in a mobile environment, one has to keep in mind restrictions on bandwidth, memory and battery life. In constrained environments such as mobile phones, wireless pagers or PDAs, these resources are highly limited. Thus, a suitable public key scheme would be one that is efficient in terms of computing costs and key sizes.

When it comes to choosing which public key cryptosystem to employ in a mobile environment, one has to keep in mind restrictions on bandwidth, memory and battery life. In constrained environments such as mobile phones,wireless pagers or PDAs, these resources are highly limited. Thus, a suitable public key scheme would be one that is efficient in terms of computing costs and key sizes. This protocol can be implemented in low power and small processor mobile devices such as smart card, PDA etc which work in low power and small processor. Since the proposed protocol is based on ECC, can be implimented to mobile devices especially Smart card.

3 Preliminaries

3.1 Notations

We first introduce common notations used in this paper as follows.

- p is the order of underlying finite field;
- F_p is the underlying finite field of order p

- E is an an elliptic curve defined on finite field F_p with large order.
- G is the group of elliptic curve points on E.
- P is a point in $E(F_p)$ with order n , where n is a large prime number.
- $\mathcal{H}(\cdot)$ is a secure one-way hash function.
- $\|$ denotes concatenation operation between two bit stings.
- S be the Sender with identity ID_s, $ID_s \in \{0,1\}^*$.
- R be the Receiver with identity ID_r, $ID_r \in \{0,1\}^*$.

4 Diffie-Hellman Problem

This section briefs overview of Computational Diffie-Hellman (CDH) problem, Decisional Diffie-Hellman and Hash Diffie-Hellman problem in $\mathbb{G}$.

Definition 1. Diffie-Hellman Problem: *Let $(q, \mathbb{G}, P)$ be a 3-tuple generated by polynomial time algorithm $\mathcal{G}(k)$,and let $a, b \in \mathbb{Z}_q^*$, the CDH problem in $\mathbb{G}$ is as follows: Given (P, aP, bP), compute abP. The (t, ϵ)-CDH assumption holds in $\mathbb{G}$ if there is no algorithm $\mathcal{A}$ running in time t such that*

$$\mathbf{Adv}_{\mathbb{G}}^{CDH}(\mathcal{A}) = Pr[\mathcal{A}(P, aP, bP) = abP] \geq \epsilon$$

where the probability is taken over all possible choices of (a, b).

$\underline{\mathbf{Exp}_{\mathcal{G}(k)}^{CDH}}$

1. $(\mathbb{G}, q, P) \leftarrow \mathcal{G}(1^k)$
2. $a, b, c \leftarrow \mathbb{Z}_q^*$
3. $U_1 = aP, U_2 = bP$
4. if $W = abP$ return 1 else return 0

Definition 2. Decisional Diffie-Hellman Problem: *Let $(q, \mathbb{G}, P)$ be a 3-tuple generated by polynomial time algorithm $\mathcal{G}(k)$,and let $a, b, c \in \mathbb{Z}_q^*$, the DDH problem in $\mathbb{G}$ is as follows: Given (P, aP, bP, cP), decide whether it is a Diffie-Hellman tuple.*

Definition 3. Hash Decisional Diffie-Hellman Problem: *Let $(q, \mathbb{G}, P)$ be a 3-tuple generated by polynomial time algorithm $\mathcal{G}(k)$,$\mathcal{H} : \{0,1\}^* \to \{0,1\}^l$ be a secure cryptographic hash function, whether l is a security parameter, and let $a, b \in \mathbb{Z}_q^*, h \in \{0,1\}^l$, the HDDH problem in $\mathbb{G}$ is as follows: Given (P, aP, bP, h), decide whether it is a hash Diffie-Hellman tuple $((P, aP, bP, \mathcal{H}(abP))$. If it is right, outputs 1; and 0 otherwise. The (t, ϵ)-HDDH assumption holds in $\mathcal{G}$ if there is no algorithm $\mathcal{A}$ running in time at most t such that*

$$\mathbf{Adv}_{\mathbb{G}}^{HDDH}(\mathcal{A}) = |Pr[\mathcal{A}(P, aP, bP, \mathcal{H}(abP) = 1] - Pr[\mathcal{A}(P, aP, bP, h) = 1]| \geq \epsilon$$

where the probability is taken over all possible choices of (a, b, h).

5 Deniable Property

Deniable authentication protocol is a new security authentication mechanism. Compared with traditional authentication protocols, it has the following two features:

1. It enables an intended receiver to identify the source of a given message.
2. However, the intended receiver can not prove to any third party the identity of the sender

In 1998, Dwork et al. [10] developed a notable deniable authentication protocol based on the concurrent zero-knowledge proof, however the protocol requires a timing constraint and the proof zero-knowledge is subject to a time delay in the authentication process. Auman and Rabin [11] proposed some other deniable authentication protocols based on the factoring problem. In 2001, Deng et al. [15] also proposed two deniable authentication protocols based on the factoring and the discrete logarithm problem respectively.

The proposed protocol will be achieving the following properties.

- **Deniable Authentication:** The intended receiver can identify the source of a given message, but cannot prove the source to any third party.
- **Authentication:** During the protocol execution, the sender and the intended receiver can authentication each other.
- **Confidentiality:** Any outside adversary has no ability to gain the deniable authentication message from the transmitted transcripts.

6 Security Model

Security Notions In this subsection, we explain the security notions ofID-based deniable authentication protocol. We first recall the usual security notion: the unforgeability against chosen message attacks (Goldwasser et al., 1988), then we consider another security notion: the deniablity of deniable authentication protocol [2].

Player. Let $P = \{\mathcal{P}_0, \mathcal{P}_1, \ldots \mathcal{P}_n\}$ be a set of players who may be included in the system. Each player $\mathcal{P}_i \in P$ get his public-secret key pair (pk_i, sk_i) by providing his identity i to the **Extract** algorithm. A player $\mathcal{P}_i \in P$ is said to be fresh if $\mathcal{P}_i$'s secret key sk_i has not been revealed by an adversary; while if $\mathcal{P}_i$s secret key sk_i has been revealed, $\mathcal{P}_i$ is then said to be corrupted. With regard of the unforgeability against chosen-message attacks, we define the security notion via the following game played by a challenger and an adversary.

[**Game 1**]

- Initial: The challenger runs Setup to produce a pair $(params, master-key)$, gives the resulting $params$ to the adversary and keeps the master-key secretly.

- Probing: The challenger is probed by the adversary who makes the following queries.
- Extract: The challenger first sets $\mathcal{P}_0, \mathcal{P}_1$ to be fresh players, which means that the adversary is not allowed to make Extract query on $\mathcal{P}_0$ or $\mathcal{P}_1$. Then, when the adversary submits an identity i of player $\mathcal{P}_i, (i = \ 0, 1)$, to the challenger. The challenger responds with the public-secret key pair (pk_i, sk_i) corresponding to i to the adversary.
- Send: The adversary submits the requests of deniable authentication messages between $\mathcal{P}_0$ and $\mathcal{P}_0$. The challenger responds with deniable authentication messages with respect to $\mathcal{P}_0$ (resp. $\mathcal{P}_1$) to $\mathcal{P}_1$ (resp $\mathcal{P}_0$).
- Forging: Eventually, the adversary outputs a valid forgery $\tilde{m}$ between $\mathcal{P}_0$ and $\mathcal{P}_1$. If the valid forgery $\tilde{m}$ was not the output of a Send query made during the game, we say the adversary wins the game.

Definition 4. (Unforgeability). *Let A denote an adversary that plays the game above. If the quantity $Adv^{UF}_{IBDAP}[A] = \ Pr[Awins]$ is negligible we say that the ID-based deniable authentication protocol in question is existentially unforgeable against adaptive chosen-message attacks.*

To capture the property of deniablity of deniable authentication protocol, we consider the following game run by a challenger.

[Game 2]

- Initial: Let $\mathcal{P}_0$ and $\mathcal{P}_1$ be two honest players that follow the deniable authentication protocol, and let $\mathcal{D}$ be the distinguisher that is involved in the game with $\mathcal{P}_0$ and $\mathcal{P}_0$.
- Challenging: The distinguisher $\mathcal{D}$ submits a message $m \in \{0,1\}^*$ to the challenger. The challenger first randomly chooses a bit $b' \in \{0,1\}^*$, then invokes the player P_b to make a deniable authentication message $\tilde{m}$ on m between $\mathcal{P}_0$ and $\mathcal{P}_1$. In the end, the challenger returns $\tilde{m}$ to the distinguisher $\mathcal{D}$.
- Guessing: The distinguisher $\mathcal{D}$ returns a bit $b \in \{0,1\}^*$. We say that the distinguisher $\mathcal{D}$ wins the game if $b = \ b'$.

Definition 5. (Deniablity). *Let D denote the distinguisher that is involved the game above. If the quantity $Adv^{DN}_{IBDAP}[D] = \ |Pr[b = \ b'] - \frac{1}{2}|$ is negligible we say that the ID-based deniable authentication protocol in question is deniable.*

7 Proposed Protocol

The Protocol follows the followings steps.

- **Setup.** Let $\mathcal{H} : \{0,1\}^* \to \{0,1\}^l$ be a secure cryptographic hash function which is of collision free. In the proposed protocol the sender has a certificate issued by the certificate authority (CA). The CA contains the public key (π_{pub}) of the sender, and the signature of CA for the certificate. The receiver can obtain (π_{pub}) and verify the validity of it. The private key (π_{prv}) of sender is kept secret.

- **Extract.** During the extraction phase, the sender S with identity $ID_s \in \{0,1\}^*$ select t_s randomly from $[1, n-1]$ and computes the following

$$a_s = \mathcal{H}(ID_s) \oplus t_s \tag{1}$$

$$Q_s = a_s \cdot P \tag{2}$$

The key pair is (Q_s, a_s). Then concatenate Q_s with the time stamp $T \in \mathbb{Z}_q^*$. Encrypts the concatenated value $(Q_s \| T)$ using his own private key π_{prv}.

$$\tilde{Q}_s = E_{\pi_{prv}}(Q_s \| T)$$

Similarly the receiver R with identity $ID_r \in \{0,1\}^*$ selects random number $t_r \in [1, n-1]$. Then computes the following:

$$a_r = \mathcal{H}(ID_r) \oplus t_r \tag{3}$$

$$Q_r = a_r \cdot P \tag{4}$$

So the key pairs of receiver R is (a_r, Q_r).

- **Send.** It follows the following steps.
  1. **Step 1:** During this phase the sender S sends the cipher $\tilde{Q}_s$ to the the receiver R. After getting, R will decrypt using the public key π_{pub} as $Q_s = D_{\pi_{pub}}(\tilde{Q}_s)$, where D denotes decryption algorithm.
  2. **Step 2:** Receiver R use the calculated value a_r from Eq.(3) and computes the session key α_1 as by the following equation.

$$\alpha_1 = a_r \cdot Q_s \tag{5}$$

Receiver R sends the computed Q_r to S. Similarly Sender also compute the session key as

$$\alpha_2 = a_s \cdot Q_r \tag{6}$$

In fact $\alpha = \alpha_1 = a_r \cdot Q_s = a_r a_s \cdot P = a_s \cdot Q_r = \alpha_2$

  3. **Step 3:** When Sender S authenticates the deniable message $M \in \{0,1\}^l$, computes $\gamma_1 = \mathcal{H}(\alpha_2, M \| T)$.
  4. **Step 4:** The resulting deniable authenticated message is tuples $\psi = (ID_s, T, \gamma_1)$.
  5. **Step 5:** Finally S sends ψ to the recipient R.

- **Receive**
  1. **Step 1:** After receiving $\psi = (ID_s, T, \gamma_1)$, the recipient R computes $\gamma_2 = \mathcal{H}(\alpha_1, M \| T)$
  2. **Step 2:** If the time stamp T is valid and $\gamma_1 = \gamma_2$, accepts M otherwise reject.

The protocol is illustrated in the following fig.

Sender S		Receiver R
Select random number $t_s \in [1, n-1]$ Computes $a_s = \mathcal{H}(ID_s) \oplus t_s$ where $ID_s \in \{0,1\}^*$ Computes $Q_s = a_s \cdot P$ Encrypt Q_s as $\tilde{Q}_s = E_{\pi_{prv}}(Q_s \| T)$ where $T \in \mathbb{Z}^*$ is the time stamp		
	$\xrightarrow{\tilde{Q}_s}$	
		Decrypt as $D_{\pi_{pub}}(\tilde{Q}_s \| T) = Q_s$ Select random number $t_r \in [1, n-1]$ $a_r = \mathcal{H}(ID_r) \oplus t_r$ where $ID_r \in \{0,1\}^*$ Computes $\alpha_1 = a_r \cdot Q_s$ Computes $Q_r = a_r \cdot P$
	$\xleftarrow{Q_r}$	
Compute $\alpha_2 = a_s \cdot Q_r$ and $\gamma_1 = \mathcal{H}(\alpha_2, M \| T)$ $\psi = (ID_s, T, \gamma_1)$		
	$\xrightarrow{\psi}$	
		Computes $\gamma_2 = \mathcal{H}(\alpha_1, M \| T)$ if time stamp T is valid and $\gamma_1 = \gamma_2$ accept M otherwise reject

8 Correctness

Theorem 1. *If $\psi = (ID_s, T, \gamma_1)$ is a authentication message produced by the Sender S honestly, then the recipient R will always accept it.*

Proof: The proposed protocol satisfies the property of correctness. In effect, if the deniable authetication message ψ is correctly generated, then

$$\gamma_1 = \mathcal{H}(\alpha_2, M \| T) = \mathcal{H}(\alpha_1, M \| T) = \gamma_2$$
$$\text{Since } \alpha_1 = a_r \cdot Q_s = a_r a_s \cdot P = a_s \cdot Q_r = \alpha_2$$

9 Security Analysis

In this section, we analyze the security of our proposed deniable authentication protocol. The security of our protocol is based on Computational Diffie-Hellman (CDH), Decisional Diffie-Hellman (DDH) and the Hashed Diffie-Hellman (HDDH) Problems.

9.1 Security Model

The protocol is defined by the following game between an adversary A and a challenge C

- **Setup:** On input of security parameters, C runs the algorithm to generate the system parameters and public key and private key pairs $(pk_i, sk_i), 1 \leq i \leq n$, of n users $\{U = \ U_1, U_2, \ldots U_n\}$, and sends the system parameters and all public keys $pk_1, pk_2 \ldots pk_n$ to A.
- **Corrupt Queries:** A can corrupt some users in U and obtain their private keys.
- **User Authentication Queries:** A also can make several user authentication queries on some uncorrupted users in U.
- **Impersonate:** In the end, A impersonates an uncorrupted user in U by outputting a valid login authentication message.

The success probability of A to win the game is defined by $\mathbf{Succ}(\mathbf{A})$.

Definition 6. *A user authentication scheme is secure if the probability of success of any polynomial bounded adversary A in the above game is negligible.*

Theorem 2. *Assume that the collision-free hash function $\mathcal{H}$ behaves as a random oracle. Then the proposed authentication scheme is secure provided that the Diffie-Hellman algorithm assumption holds in $\mathbb{G}$.*

Proof: Assume that A is an adversary, who can with non-negligible probability, break the proposed authentication scheme. Then, we can use A to construct another algorithm $\tilde{A}$, which is having parameters $(q, \mathbb{G}, P)$ and $\mathcal{H}$, where $\mathcal{H} : \{0,1\}^* \to \{0,1\}^l$ be a secure cryptographic hash function, behaves a random oracle [7] and a DH instance (P, aP, bP), where $a, b \in \mathbb{Z}_q^*$ as her challenge, and her task here is to compute $(ab) \cdot P$. Let $U = \ U_1, U_2 \ldots U_n$ be a set of n users who may participate in the system. $\tilde{A}$ first picks a random number j from $\{1, 2 \ldots n\}$, and sets the user U_j's public key $Q_j = \ t_j \cdot P$. Then, $\tilde{A}$ chooses another $n-1$ random numbers $t_i \in \mathbb{Z}_q^*$ as user U_i's secret key, where $1 \leq i \leq n$ and $i \neq j$, and computes the corresponding public key $Q_i = \ t_i \cdot P$. Finally, $\tilde{A}$ sends all public key $Q_1, Q_2 \ldots Q_n$ to the adversary A.

Theorem 3. *The proposed Protocol achieves the authentication between the sender and the intended receiver.*

Proof: In our proposed protocol, if the receiver accepts the authentication message ψ, receiver R can always identify the source of the message. If an adversary wants impersonate the sender S, he can obtain a time stamp $T \in \mathbb{Z}_q^*$, a message M. But, he could not construct the α_2. If the adversary tries to compute α_2 he has to know the sender's private key a_s for that it needs to solve ECDLP.

Definition 7. *Informally, a deniable authentication protocol is said to achieve the property of confidentiality, if there is no polynomial time algorithm that can distinguish the transcripts of two distinct messages.*

Theorem 4. *The proposed protocol achieves the property of confidentiality provided that the HDDH problem is hard in $\mathbb{G}$.*

Proof : $\gamma_1 = \mathcal{H}(\alpha_2, M\|T)$ is actually a hashed ElGamal cipher text [14]. Hashed ElGamal encryption is semantically secure in the random oracle model under the Computational Diffie-Hellman (CDH) assumption. This is the assumption that given P, aP, bP, it is hard to compute $ab \cdot P$ in $\mathbb{G}$, where a, b are random elements of $\mathbb{Z}_q^*$. The CDH assumption is more precisely formulated as follows.
Let $\mathbb{A}$ be an algorithm that takes as input a pair of group elements, and outputs a group element. CDH-advantage of $\mathcal{A}$ to be

$$[a, b \leftarrow \mathbb{Z}_q^* : \mathcal{A}(aP, bP) = ab \cdot P]$$

The CDH assumption on $(\mathbb{G})$ is that any efficient algorithms CDH advantage is negligible. As a result, the proposed protocol can achieves the confidentiality.

Theorem 5. *The proposed protocol also achieves the property of deniability.*

Proof : To prove that the proposed protocol has deniable property, first we should prove that it enables an intended receiver R to identify the source of the given message M. Since the authenticated message $\psi = (ID_s, T, \gamma_1)$ contains the sender identity ID_s, R can easily identify the source of the message. After verifying $\gamma_1 = \gamma_2$, R can be assured that the message is originated from S. If R intends to expose the message's identity to third party, S would be repudiate as he would argue that S could also generate ψ, since R can compute γ_2 and $\gamma_1 = \gamma_2$, *i.e* transcripts transmitted between the sender S and the receiver R could be simulated by the receiver R himself in polynomial time algorithm. Hence the deniable property is satisfied.

Also we can prove considering the security model describe in section-5. Let us consider a distinguisher $\mathcal{D}$ and two honest players $\mathcal{P}_0$ and $\mathcal{P}_1$ involved in **Game** 2. The distinguisher $\mathcal{D}$ first submits a message $m \in \{0,1\}^*$ to the challenger. Then, the challenger chooses a bit $b \in \{0,1\}$ uniformly at random, and invokes the player $\mathcal{P}_b$ to make a deniable authentication message $\psi = (ID_b, T_b, MAC_b, C)$ on m between $\mathcal{P}_0$ and $\mathcal{P}_1$. In the end, the challenger returns $\psi = (ID_b, T_b, MAC_b, C)$ to the distinguisher $\mathcal{D}$. Since both $\mathcal{P}_0$ and $\mathcal{P}_1$ can generate a valid deniable authentication message $\psi = (ID_b, T_b, MAC_b, C)$, which can pass the verification equation, in an indistinguishable way, when $\mathcal{D}$ returns the guessed value b, we can sure that the probability $\Pr[b = b']$ is $\frac{1}{2}$, and the quantity $Adv_{IBDAP}^{DN}[D] = |Pr[b = b'] - \frac{1}{2}| = |\frac{1}{2} - \frac{1}{2}| = 0$ Based upon the analysis above, we can conclude that the proposed protocol can achieve the deniable authentication.

Theorem 6. *The Protocol authenticates the source of the message.*

Proof: If someone proves $\mathcal{H}(\alpha_2, M\|T)$ to R, where $\alpha_2 = a_s \cdot Q_r$, he must be S. If an adversary gets all the information Q_s in **Extract** phase, he can not compute the session key α_1. It is as difficult as solving Elliptic Curve Discrete Logarithm Problem.

Definition 8. Secure against Man-in-the-middle. *An authentication protocol is secure against an Man-in-the-middle, if Man-in-the-middle can not establish any session key with either the sender or the receiver.*

Theorem 7. *The proposed protocol is secure with respect to the man-in-the-middle (MIA) attack.*

Proof: In the extraction phase, the message is encrypted with the private key π_{prv}. It is difficult for the adversary to get the key π_{prv}. An intruder can intercept the message from S and act as R to negotiate the session key α with S. If he wants execute MIA attack, he must act as the sender S to cheat R. To construct the cipher $\tilde{Q_s}$, first he has to find out π_{prv} and a_s. For that he has to solve ECDLP, which is computationally infeasible takes fully exponential time. If he fakes an $\tilde{Q_s}$, R can not get correct Q_s. so it resist MIA attack.

10 Computational Complexity

The computation cost for the performance of this new protocol is as follows: the sender needs to compute a point multiplication, a pairing evaluation, an encryption, as well as a hash evaluation. In addition, the most expensive work for the sender is the use of a public-key digital signature algorithm.Since the receiver and the sender stand in the symmetric position, so the receiver shares the same computation costs. The communication cost of the proposed protocol is that the sender and the receiver carry out two rounds for communications in order for the receiver to obtain a message from the sender.

Let T_M : is the time taken for executing a scalar multipication over Elliptic Curve.
T_H : is the time for executing one-way hash function.
$T_{\oplus}$: is the time taken for Exclusive OR operation.
$T_{Encyp\&Decrp}$: is the time taken for encryption and decryption in Public Key cryptosystem.
Execution time, Sender has to take is $T_S = 2T_M + 2T_H + T_{\oplus} + T_{Encrp}$.
Execution time, Receiver has to take is $T_R = 2T_M + 2T_H + T_{\oplus} + T_{Decrp}$.
Total time $T = T_S + T_R$.

In practical implementation, we can use some existing tools for these computations including point multiplication, bilinear pairing evaluation, and hash function evaluation over elliptic curves. The protocol is based on the elliptic curve cryptography (ECC) and thus it has high security complexity with short key size.

11 Implimentation Issues

ECC requires the use of two types of mathematics:

- Elliptic curve point arithmetic
- The underlying finite field arithmetic.

For implimentation of ECC based protocol, we have to select the underlying finite field. An elliptic curve is a set of points specified by two variables that are elements over a field. A field is a set of elements with two custom-defined arithmetic operations, usually addition and multiplication.) Most of the computation for ECC takes place at the finite field level. The two most common choices for the underlying finite field are:

- $\mathbb{F}_{2^m}$, also known as characteristic two or even (containing 2m elements, where m is an integer greater than one)
- $\mathbb{F}_p$, also known as integers modulo p, odd, or odd prime (containing p elements, where p is an odd prime number).

12 Conclusion

The security of the proposed protocol is based on difficulty of breaking the Elliptic Curve Diffie-Hellman problem and one way hash function. It archives deniable authentication as well as confidentiality. Also it is resistant against Man-in-Middle attack. It is an non-interactive protocol. The attractiveness of ECC will increase relative to other public-key cryptosystems as computing power improvements force a general increase in the key size. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates. Therefore it can be easy to implemented in mobile devices such as PDA, smart card etc. Since the protocol is based on the elliptic curve cryptography (ECC) and thus it has high security complexity with short key size.

References

1. Dwork, C., Naor, M., Sahai, A.: Concurrent zero-knowledge. In: Proc. 30th ACM STOC 1998, Dallas TX, USA, pp. 409–418 (1998)
2. Kar, J.P., Majhi, B.: A Novel Deniable Authentication Protocol based on Diffie-Hellman Algorithm using Pairing techniques. In: ACM International Conference on Communication, Computing and Security (ICCCS 2011), NIT, Rourkela, India, pp. 493–498 (2011)

3. Fan, L., Xu, C.X., Li, J.H.: Deniable authentication protocol based on Diffie-Hellman algorithm. Electronics Letters 38(4), 705–706 (2002)
4. Jiang, S.Q.: Deniable Authentication on the Internet, Cryptology ePrint Archive: Report (082) (2007)
5. Koblitz, N.: A course in Number Theory and Cryptography, 2nd edn. Springer (1994)
6. Menezes, A., Van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. CRC Press (1997)
7. Bellar, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of the 1st CSS, pp. 62–73 (1993)
8. Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer (2004)
9. Certicom ECC Challenge and The Elliptic Curve Cryptosystem, `http://www.certicom.com/index.php.`
10. Dwork, C., Naor, M., Sahai, A.: Concurrent zero-knowledge. In: Proceedings of 30th ACM STOC 1998, pp. 409–418 (1998)
11. Aumann, Y., Rabin, M.O.: Authentication, Enhanced Security and Error Correcting Codes. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 299–303. Springer, Heidelberg (1998)
12. Diffie, W., Hellman, M.E.: Directions in cryptography. IEEE Transactions on Information Theory 22, 644–654 (1976)
13. Shi, Y., Li, J.: Identity-based deniable authentication protocol. Electronics Letters 41, 241–242 (2005)
14. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs, in Cryptology ePrint Archive: Report 2004/332, `http://eprint.iacr.org/2004/332`
15. Deng, X., Lee, C.H., Zhu, H.: Deniable authentication protocols. IEE Proceedings. Computers and Digital Techniques 148, 101–104 (2001)