Journal of Computer Science

Original Research Paper

A Secure Key Authentication Scheme Based on the Hardness of Solving Elliptic Curve Discrete Logarithm Problem

Izzmier Izzuddin Zulkepli and Eddie Shahril Ismail

Department of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia

Article history
Received: 24-01-2020
Revised: 29-03-2020
Accepted: 06-05-2020

Corresponding Author:
Eddie Shahril Ismail
Department of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
Email: esbi@ukm.edu.my

Abstract: A key authentication scheme is a scheme that protects a user's public key from modification and counterfeiting by an adversary. The new development and improvement of key authentication schemes should be made continuously so that the systems are safe and practical to be used. To the best of our knowledge, there is no key authentication using the elliptic curve so far. Thus, in this paper, we propose the first secure elliptic curve-based key authentication scheme with its security, relying on the difficulty of solving the elliptic curve discrete logarithm problem. We show that the proposed scheme is secure against various defined cryptographic attacks such as public keyword modification and keyword guessing attacks. Next, we analyze the computational time complexity of the algorithms by computing the number of modular operations needed in these algorithms together with asymptotical analysis of running time using $O(g(n))$ notation. It turns out that our scheme requires the least amount of time complexity of $203.36T_{mul} + T_h$ for user registration phase, $58.12T_{mul}$ for key authentication phase, and offers less running time compared to some existing key authentication schemes.

Keywords: Cryptography, Key Authentication Scheme, Elliptic Curve, Elliptic Curve Discrete Logarithm Problem

Introduction

Diffie and Hellman (1976) solved a key distribution problem of secret key cryptography and proposed a novel idea of modern cryptography that is now called the public-key cryptography. Specifically, they proposed that any two communicating users need not be shared a common secret key, but instead, each user needs to generate two keys, namely public and private keys. In public-key cryptographic systems, the private key or sometimes called the secret key will be kept secret from other people. In contrast, the public key will be made public to anyone, including to adversary or enemy. Then the user publishes the public key in a public-key directory. One of the main components in public-key cryptographic systems is a cryptosystem. In a cryptosystem, two communicating parties, a sender and a receiver, are needed to complete the communication processes. The sender encrypts a confidential message or document by using the receiver's public key and submits the encrypted message to the known receiver. The receiver who has the private key can decrypt the encrypted message and later read the original message. One of the main issues in designing any public-key cryptographic systems is the security of its public key. The key question is, how do we protect the public key from alteration or modification by an adversary? The cryptographic solution to this problem is via Key Authentication Scheme (KAS). KAS provides a mechanism of authenticating the validity of the receiver's public key. KAS consists of three algorithms: (1) key generation algorithm, (2) user registration phase, and (3) key authentication phase. The organization of this paper is as follows. In the next section, we discuss some past and related works of KAS. Then we present our proposal of a key authentication scheme based on elliptic curve discrete logarithm problem. We next discuss the security analysis and efficiency consideration of our new scheme. Finally, we make a comparison of the new and existing schemes in terms of attacks and time complexity.

Related Works

Horng and Yang (1996) designed the first KAS whose security is based on the hardness of solving a discrete logarithm problem. Their scheme needs a

Science Publications

© 2020 Izzmier Izzuddin Zulkepli and Eddie Shahril Ismail. This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license.

certificate but requires no authority. The certificate is computed using the user's private key and password. However, a study by Zhan *et al*. (1999) found that Horng-Yang's scheme is not secure against the password guessing attack. If an enemy successfully finds the actual password, he or she can further generate a valid false public key. Zhan *et al*. proposed an improvement to the Horng and Yang's scheme. However, the improved scheme, as shown by Lee *et al.* (2003) does not achieve the non-repudiation property. A dishonest user can successfully deny his or her public key. Lee *et al.* fixed the problem and proposed a modified version of the Zhan *et al.* scheme.

Later, Peinado (2004) and Zhang and Kim (2005) separately showed that Lee *et al*. (2003) scheme had some security flaws. They showed that the scheme is not secure as the attacker can easily recover the user's private key from the user's public key certificate. Also, Peinado (2004) proved that the verification procedure presented in the scheme is not valid. Both Peinado (2004) and Zhang and Kim (2005) then have suggested a modification to improve the security of the scheme. Meanwhile, Wu and Lin (2004) also showed that Lee *et al.*'s scheme is vulnerable to the key substitution attack and provided a modified version of Lee *et al.*'s.

Sun and Cao (2005) proved that the improved version by Peinado (2004) does not achieve non-repudiation property. A dishonest user can forge his public key via the verification procedure and deny his signature. Sun and Cao (2005) next proposed modification and proved that the version has now achieved the non-repudiation property. Meanwhile, Sun and Cao (2005) also proved that Zhang and Kim (2005) did not achieve non-repudiation property. Shao (2005) showed that Peinado's scheme is insecure as an attacker can obtain the user's private key through a guessing attack. Shao (2005) also showed that Zhang and Kim (2005) scheme is vulnerable to public key substitution attacks and modified a new version based on the discrete logarithmic problem.

Yoon and Yoo (2005) demonstrated that Lee *et al*. (2003), Peinado (2004), and Wu and Lin (2004) are prone to key substitution attacks. They then proposed an improvement of Lee *et al*. (2003) and claimed that the version is resistant to public key substitution attacks. Two years later, Yoon and Yoo (2007) have performed some cryptanalysis toward Sun and Cao (2005) scheme and concluded that the Sun-Cao's is still vulnerable to public key substitution attack. They later proposed a highly secure improvement of the scheme.

One common feature of the above schemes is that all schemes were designed based on a single hard cryptographic problem. Soon, if one finds a solution to the hard problem, all these schemes will no longer be secure. Thus, there is an urgent need to develop key authentication schemes based on multiple hard problems. Suparlan *et al*. (2016), Meshram *et al*. (2016), and Kumaraswamy *et al*. (2016) respectively developed their schemes based on factoring with discrete logarithm problems, factoring with generalized discrete logarithm and discrete logarithm problem with Chinese remainder theorem. The idea is that even if one of the underlying hard problems is solvable, the designated scheme is still secure due to the security of the other underlying hard problem. Unfortunately, Peinado (2017) managed to reveal the weaknesses of Kumaraswamy *et al*. (2016)'s scheme in which the scheme has several mathematical inconsistencies that led to the vulnerability attack. To the best of our knowledge, there is no known key authentication scheme of which security depends on Elliptic Curve Discrete Logarithm (ECDLP), which was first introduced independently by Miller (1985) and Koblitz (1987). Applying the ECDLP to the scheme will offer some added values to the proposed scheme in terms of efficiency while maintaining an adequate level of security.

Materials and Methods

The proposed scheme makes use of the elliptic curve from computational number theory (Ismail and Hijazi, 2012; Koblitz, 1987; Miller, 1985). The equation of the elliptic curve in a general form is defined by:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where, a, b, c, d, $e \in \mathbb{F}$ and $\mathbb{F}$ is a field. We define on this curve an elliptic curve addition operation with a point at infinity (we denote this point as ∞). Now, suppose that q is a 160-bits prime with the corresponding field has characteristics neither two nor three. For cryptographic purposes, we now consider an elliptic curve E over the Galois Field $E(\mathbb{F}_q)$ as below:

$$y^2 = x^3 + ax + b \bmod q \; where \; 0 \le x \le q.$$

The coefficients $a,b< q$ are non-negative integers and satisfy the condition $4a^3 + 27b^2 \neq 0 \bmod q$, which defines the elliptic curve with no multiple roots of unity.

The terminology of point addition can be extended to point multiplication where in this operation, a point P on the elliptic curve is multiplied with a scalar k using the elliptic curve equation to obtain another point Q on the elliptic curve and this is defined by $kP = Q$. If $k = 2$, the point multiplication is called the point doubling. The point multiplication kP is computed by performing multiple point additions. Thus, point multiplication uses point addition and point doubling repeatedly to obtain the result. This method is called "double and add" for point multiplication. Mathematically, we have the

following: Point addition by adding two elliptic curve points J and K to obtain another point $L = J+K$ and point doubling by adding a point J to itself to obtain another point $L = 2J = J+J$. If we want to compute $L = 3J+5K$ then we can use the following formula $L = 3J+5K = 2J+2(2K)+J+K$ involving three point doublings and three point additions.

The Proposed Key Authentication Scheme

In this section, we present our new key authentication scheme for a cryptosystem based on the difficulty of solving the elliptic curve discrete logarithm problem. A key authentication consists of three phases that are key generation, user registration, and key authentication. The security of the proposed scheme heavily depends on the hardness of solving the elliptic curve discrete logarithm (Koblitz, 1987).

Definition 1

Given an elliptic curve E over the Galois Field $E(\mathbb{F}_q)$ defined by:

$$y^2 = x^3 + ax + b \bmod q$$

where, $0 \le x \le q$ and the coefficients a,b,q are non-negative integers and the curve contains no multiple roots of unity. Assume that P and Q are two elliptic curve point on E such that $Q = np$. Find integer n.

From the above definition, we create a corresponding public one-way function defined by $f(x) = xG \bmod q$ where, G is an elliptic curve point on E. We now give the description of the algorithms of the scheme.

Phase 1: Key Generation Phase

This phase is done by the trusted administrator (steps 1-4) and the receiver (steps 5-6):

1. Select a 160-bits prime p which determines the order of field $\mathbb{F}_p$
2. Choose two numbers a and b in $\mathbb{F}_p$. These values determine the elliptic curve, E
3. Pick a base elliptic curve point G from the defined elliptic curve with a large prime generator m such that $mG = \infty$
4. Choose a secure one-way hash function $h(\cdot)$ which maps an arbitrary length of input to a 160-bit of output
5. Choose at random an integer, $d \in \mathbb{F}_p$ with $d < m$
6. Calculate $Q = f(d) = dG \bmod p$

The public parameters of the scheme are given by (p,a,b,m,E,G,h). The public and private keys of the receiver are given by Q and d respectively.

Phase 2: User Registration Phase

This phase is done by the receiver (steps 1-5), the administrator (step 6) and the server (steps 7-10):

1. Choose two random integers $s,pwd \in \mathbb{F}_p$ with $s,pwd < m$.
2. Calculate $V = f(pwd) = (pwd)G \bmod p$
3. Compute $W = f(s) = Sg \bmod p$
4. Calculate $Y = f(pwd+s) = (pwd+s)G \bmod p$
5. Generate certificate, $C = (pwd+s+d) \bmod p$
6. Store the three components $(R_x(Q),Y,h(W))$ in a protected key directory, where $R_x(Q)$ represents the x-coordinate of the point Q and $h(W)$ is a hash value of W). We require that these components are protected by the access control (public can see and use but unable to modify the values/points in the directory). However, the other four components (C,Q,V,W) will be stored in the accessible public key directory. These directories will be monitored and protected by the administrator
7. The server validates if $Y = V+W \bmod p$ and $f(C) = Y+Q \bmod p$ holds
8. The server chooses α,β where $\alpha,\beta < m$ and computes $J = \alpha \cdot G \bmod p$ and $K = \beta \cdot G \bmod p$
9. The server generates a user secondary certificate, C' defined by $C' = R_x(Q)\alpha + C\beta \bmod p$
10. The server stores (C',J,K) in the accessible public key directory

Thus, each receiver has two directories; the protected access control directory $(R_x(Q),Y,h(W))$ and the accessible public directory (C,Q,V,W,C',J,K).

Phase 3: Key Authentication Phase

This phase is completely done by the sender:

1. The sender verifies if the equation $f(C') = R_x(Q) \cdot J + C \cdot K \bmod p$ is true or not
2. The sender accepts the public key Q as valid if the equation above holds otherwise rejects it

We next provide proof of the receiver's public key validity so that the sender is convinced to use the validated public key to encrypt any message to the receiver.

Proposition 1

Given the scheme's public parameter (p,a,b,m,E,G,h). If all receiver's public key, Q, certificate, C and (C',J,K) are generated correctly, then the receiver's public key is validated.

Proof

If all receiver's public key, Q, certificate, C and (C',J,K) are mathematically correct, then we have $C =$

(pwd+s+d) mod p, $C' = R_x(Q)\alpha + C\beta \bmod p$, $J = \alpha \cdot G \bmod p$ and $K = \beta \cdot G \bmod p$. Note that:

$$\begin{aligned} f(C') &= C'G \\ &= \left(R_x(Q)\cdot\alpha + C\cdot\beta\right)G \\ &= R_x(Q)\cdot\alpha G + C\cdot\beta G \\ &= R_x(Q)\cdot J + C\cdot K \bmod p. \end{aligned}$$

We now discuss the security and efficiency performances of the new designated key authentication scheme.

Security Analysis

We show that our scheme is heuristically secure by applying the scheme with common security cryptographic attacks. We define each attack and give the corresponding analysis of why this attack would fail. In general, the possible cryptographic attacks by the adversary are as follows.

Attack 1: Public Key Replacement and Public Keyword Modification Attacks

In this attack, the attacker tries to generate a false but valid public key and certificate and replace the original public key and certificate in the public key directory with the false ones. If the attacker succeeds with high probability, then the sender is unknowingly using the false public key to encrypt the message. If this cipher text falls into the attacker, he or she will be able to read the message using his or her own corresponding false but valid private key. There are two strategies of this attack.

First, the attacker calculates the false public key, $\bar{Q}$, chooses a false password, $\overline{pwd}$ and attempts to obtain the corresponding false certificate, $\bar{C}$. The attacker chooses the false key, $\bar{d}$, assuming $d \neq \bar{d}$ (this assumption is valid because of the hardness of ECDLP) and calculates $\bar{Q} = \bar{d}\cdot G \bmod p$ Next, the attacker computes $\bar{s} = C - (\overline{pwd} + \bar{d}) \bmod p$ where $C = pwd+s+d$ is the receiver's original certificate. The attacker next generates the value of false certificate $\bar{C}$ via:

$$\bar{C} = \overline{pwd} + \bar{s} + \bar{d} \bmod p$$

and publishes $\bar{Q}$ and $\bar{C}$ to replace Q and C in the public key directory. Then, the server has to verify whether the values of $\bar{C}$, $\bar{Q}$ and Y are valid components by checking whether $f(\bar{C}) = Y + \bar{Q} \bmod p$ is true or not. However, the server is unable to verify them, as the value of $f(\bar{C})$ is not equal to $Y + \bar{Q}$. This can be proven in the following theorem.

Theorem

Given the scheme's public parameter (p,a,b,m,E,G,h). If $\bar{Q} = \bar{d}$, $\bar{C} = \overline{pwd} + \bar{s} + \bar{d}$ and $\bar{s} = C - (\overline{pwd} + \bar{d}) \bmod p$ are computed by first randomly choosing the values $\overline{pwd}$ and $\bar{d} \neq d$ where $C = pwd+s+d$ is the receiver's original certificate, then the values $\bar{Q}$ and $\bar{C}$ are not valid public key and certificate of the receiver.

Proof

It is known that $\bar{C} = C$. Therefore:

$$\begin{aligned} &\overline{pwd} + \bar{s} + \bar{d} = (pwd + s) + d \\ &(\overline{pwd} + \bar{s}) - (pwd + s) = d - \bar{d} \neq 0. \end{aligned}$$

Notice that d-$\bar{d} \neq 0$ because the probability for the value to be zero is low, as the value of $\bar{d}$ is randomly chosen by two different users. Thus:

$$\begin{aligned} &\left(\overline{pwd} + \bar{s}\right) - \left(pwd + s\right) \neq 0 \\ &\overline{pwd} + \bar{s} \neq pwd + s. \end{aligned}$$

Note that:

$$\begin{aligned} &f(\bar{C}) = \left(\overline{pwd} + \bar{s} + \bar{d}\right)\cdot G = \left(\overline{pwd} + \bar{s}\right)G + \bar{d}G \bmod p \, and \\ &Y + \bar{Q} = \left(pwd + s + \bar{d}\right)\cdot G = \left(pwd + s\right)G + \bar{d}G \bmod p \end{aligned}$$

Subtracting these two equations, we obtain $f(\bar{C}) - \left(Y + \bar{Q}\right) = \left(\overline{pwd} + \bar{s}\right)\cdot G - \left(pwd + s\right)G$ and since $\overline{pwd} + \bar{s} \neq pwd + s$ we have $\left(\overline{pwd} + \bar{s}\right)G \neq \left(pwd + s\right)G$. We conclude that:

$$f(\bar{C}) \neq Y + \bar{Q} \bmod p.$$

This shows that the server is unable to verify $\bar{C}$, $\bar{Q}$ and Y and the attacker fails to replace the public key.

Second, the attacker chooses the false certificate, $\bar{C}$ and tries to obtain the corresponding false public key, $\bar{Q}$ such that $f(\bar{C}) = Y + \bar{Q} \bmod p$ following the original equation in the scheme. The attacker chooses $\bar{C}$, assuming that $\bar{C} \neq C$ (this assumption is valid because of the hardness of ECDLP). It can be shown that:

$$\begin{aligned} &f(\bar{C}) = Y + \bar{Q} \bmod p \\ &\bar{C}\cdot G = Y + \bar{Q} \bmod p \\ &\bar{Q} = \bar{C}\cdot G - Y \bmod p. \end{aligned}$$

Now the attacker successfully obtains the corresponding value of $\bar{Q}$ which satisfies the equation $f(\bar{C}) = Y+\bar{Q} \bmod p$. However, the value of $R_x(\bar{Q})$ is not equal to the value of $R_x(\bar{Q})$ stored in the public key directory which is protected by the access control technique. Therefore, $\bar{Q}$ will be rejected by the server. Otherwise, the attacker may choose $\bar{Q}$ and try to obtain $\bar{C}$ from $\bar{Q} = \bar{C}\cdot G-Y \bmod p$. This attempt might fail due to the difficulty of solving the elliptic curve discrete logarithm problem.

Attack 2: Keyword/Password Guessing Attack

The attacker attempts to obtain the password, *pwd*, of a specific user by guessing. If the attacker successfully obtains *pwd*, then the scheme is considered insecure. From equation $Y = f(pwd+s) \bmod p$, the attacker will try to guess the user password as $\overline{pwd}$ and verifies whether the following equation is true or false:

$$Y = f\left(\overline{pwd}\right) + W \bmod p$$

The above equation is only true when $\overline{pwd} = pwd$. The value of $\overline{pwd}$ is chosen from $\mathbb{F}_p$ where p is 160-bit and $2^{159} < p < 2^{160}$. Thus, the probability of having $\overline{pwd} = pwd$ is approximately $\frac{1}{p} = \frac{1}{2^{160}}$ and this is highly unlikely to happen. To obtain the password directly from equations V,W,Y and C, the attacker has to solve the elliptic curve discrete logarithm problem. This is impossible as this hard problem is cryptographically difficult to solve.

Attack 3: Achieving user Public Key Non-Repudiation

A dishonest user tries to repudiate his public key or signature on a received document. Therefore, after the user signs the document, the user tries to replace the public key, Q and the certificate, C, as well as the original server certificate, C', with the false but valid public key, $\bar{Q}$, certificate, $\bar{C}$ and server's certificate, $\bar{C}'$. Specifically, the user wants to calculate the key $\bar{Q} \neq Q$ such that it satisfies $R_x(\bar{Q}) = R_x(Q)$. This can be achieved by solving the equation:

$$\begin{aligned} y^2 &= x^3 + ax + b \\ &= \left(R_x(Q)\right)^3 + aR_x(Q) + b \bmod p \end{aligned}$$

For y. Next, the user tries to generate the new user certificate by first choosing $\bar{d}$ randomly and calculating:

$$\bar{C} = pwd + s + \bar{d} \bmod p\ .$$

Then, the user obtains the new server certificate from the equation $C' = R_x(Q)\alpha+C\beta \bmod p$. However, this is impossible as the values α and β are the server secret keys.

The user may also attempt to obtain the value of $\bar{C}'$ from the equation $f(C') = R_x(Q)\cdot J+C\cdot K \bmod p$. Note that:

$$\begin{aligned} f(\overline{C}') &= R_x(\overline{Q})\cdot J + \overline{C}\cdot K \bmod p \\ \overline{C}'\cdot G &= R_x(\overline{Q})\cdot J + \overline{C}\cdot K \bmod p \\ \overline{C}'\cdot G &= \lambda \bmod p. \end{aligned}$$

To obtain the value of $\bar{C}$, the user must solve the elliptic curve discrete logarithm problem of $\overline{C}'\cdot G = \lambda \bmod p$. This is impossible because elliptic curve discrete logarithm problems in cryptography are difficult to solve as to this day, no polynomial algorithms have been found.

Performance Analysis

We now discuss the efficiency performance of our key authentication scheme in terms of the number of keys, computational complexity and communication cost. Let T_{mul} and $T_{\exp}$ be the time necessary for performing a modular multiplication and a modular exponentiation, respectively. Let also $T_{ec\text{-}add}$, $T_{ec\text{-}mul}$ and T_h be the time taken for performing an elliptic curve addition, an elliptic curve scalar multiplication and a hashing, respectively. We further use the following standard conversion of various operation units to the time complexity for executing the modular multiplication (Ismail and Sakib, 2012) given by $T_{\exp} \approx 240T_{mul}$; $T_{ec\text{-}mul} \approx 0.12T$ and $T_{ec\text{-}mul} \approx 29T_{mul}$.

From the Table 1, for the key generation phase, time complexity $3T_{ec\text{-}mul}$ is required, user registration phase needed $3T_{ec\text{-}mul}+7T_{ec\text{-}mul}+T_h$ and key authentication phase needed $T_{ec\text{-}add}+2T_{ec\text{-}mul}$. By using the conversion, time complexity needed for key generation phase, user registration phase and key authentication phase are respectively given by $29T_{mul}$, $203.36T_{mul}+T_h$ and $58.12T_{mul}$. The overall communication cost of the scheme is $11|p|$ in total. This is considered smaller than Wu and Lin (2004), Zhang and Kim (2005) and Yoon and Yoo (2007).

We next compare our scheme with some other related schemes in Table 2. In Table 3, we provide the comparison in terms of time complexity, T_{mul}.

Based on Table 2 and Table 3, it shows that the time complexity of our scheme is the lowest and from Fig. 1,

we next compare the asymptotic upper bound of the running time, in terms of input size, n of the algorithm by using the standard conversion of $T_{mul} \approx O(\log n)^2$ and $T_{\exp} \approx O(\log n)^3$ following Menezes *et al*. (1997). It describes the worst-case scenario which can be used to describe the upper bound of the execution time required by an algorithm. Note that the running times of all the compared key authentication schemes are asymptotically bounded by $O(\log n)^2 + O(\log n)^3$ whereas our scheme is asymptotically bounded by $O(\log n)^2$. These would mean that all schemes work in poly-logarithmic time, but our scheme significantly needs the least.

Table 1: Efficiency of our proposed scheme

	Key generation phase	User registration phase	Key authentication phase
Computational complexity	$T_{ec\text{-}mul}$	$3T_{ec\text{-}mul} + 7T_{ec\text{-}mul} + T_h$	$T_{ec\text{-}add} + 2T_{ec\text{-}mul}$
Computational complexity T_{mul}	$29T_{mul}$	$203.36T_{mul} + T_h$	$58.12\ T_{mul}$
Communication cost	$\|p\|$	$9\|p\|$	$\|p\|$

Table 2: Time complexity in registration phase and authentication phase

The Schemes	User registration phase	Key authentication phase
Lee *et al*. (2003)	$4T_{mul}+3T_{\exp}+T_h$	$2T_{mul}+ 2T_{\exp}$
Wu and Lin (2004)	$2T_{mul}+3T_{\exp}+T_h$	$T_{mul}+T_{\exp}$
Peinado (2004)	$4T_{mul}+3T_{\exp}+T_h$	$T_{mul}+T_{\exp}$
Zhang and Kim (2005)	$2T_{mul}+3T_{\exp}+T_h$	$T_{mul}+T_{\exp}$
Yoon and Yoo (2007)	$3T_{mul}+3T_{\exp}+T_h$	$T_{mul}+2T_{\exp}$
Suparlan *et al*. (2016)	$4T_{mul}+6T_{\exp}+T_h$	$T_{mul}+2T_{\exp}$
Bong (2017)	$6T_{mul}+8T_{\exp}+T_h$	$T_{mul}+2T_{\exp}$
Our scheme	$3T_{ec\text{-}add}+7T_{ec\text{-}mul}+T_h$	$T_{ec\text{-}add}+2T_{ec\text{-}mul}$

Table 3: Conversion of time complexity in registration phase and authentication phase to T_{mul} operation

The Schemes	User registration phase	Key authentication phase
Lee *et al*. (2003)	$724T_{mul}+T_h$	$482T_{mul}$
Wu and Lin (2004)	$962T_{mul}+T_h$	$241T_{mul}$
Peinado (2004)	$724T_{mul}+T_h$	$482T_{mul}$
Zhang and Kim (2005)	$962T_{mul}+T_h$	$241T_{mul}$
Yoon and Yoo (2007)	$723T_{mul}+T_h$	$481T_{mul}$
Suparlan *et al*. (2016)	$1444T_{mul}+T_h$	$481T_{mul}$
Bong (2017)	$1926T_{mul}+T_h$	$481T_{mul}$
Our scheme	$203.36T_{mul}+T_h$	$58.12T_{mul}$

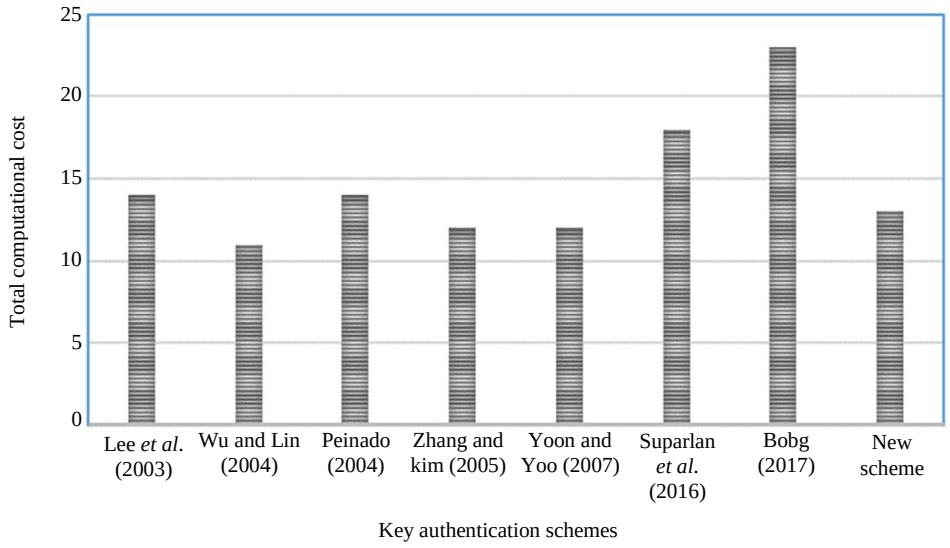

Fig. 1: Total computational costs in both registration phase and authentication phase for several key authentication scheme

Conclusion

One of the challenges in designing a key authentication scheme is its security analysis. If we want to create a secure scheme, the algorithms or phases in the designated scheme must be mathematically and cryptographically strong. In the literature, there are many key authentication schemes developed based on factoring and discrete logarithm problems. In this study, we design a key authentication scheme based on the hardness of solving the elliptic curve discrete logarithm problem. Our proposed scheme provides greater security and efficiency compared to existing key authentication schemes. The designated scheme is also shown to be heuristically secure against most of the common cryptographic attacks for key authentication such as public keyword modification and keyword guessing attacks. In terms of efficiency performance, our scheme requires the least amount of time complexity of $203.36T_{mul}+T_h$ for user registration phase, $58.12T_{mul}$ for key authentication phase and offers $O(\log n)^2$ poly-logarithmic running time compared to some existing key authentication schemes. Next, the overall communication cost of the scheme is $11|p|$ in total. For future work, one could strengthen the security of the scheme by applying provable security on it. One may also integrate the security of the scheme with other hard problems to make it harder for an adversary to break it.

Acknowledgement

The authors feel grateful to the anonymous reviewers for their valuable suggestions and comments toward improving the quality of the paper and would like to thank the editors of the journal from the core of our hearts.

Funding Information

The authors acknowledge Universiti Kebangsaan Malaysia (UKM) for funding this research under the grant GUP-2017-089.

Author's Contributions

Izzmier Izzuddin Zulkepli: Designed the algorithm of the key authentication scheme, provided efficiency performance of the algorithm and prepared the preliminary version of this manuscript.

Eddie Shahril Ismail: Prepared security analysis of the algorithm with efficiency performance and provided major modification and correction for the final preparation of this manuscript.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all other authors have read and approved the manuscript and no ethical issues are involved.

References

Bong, Y.L., 2017. Skema pengesahan kunci kebal terhadap penyangkalan berdasarkan masalah logaritma diskret dan masalah pemfaktoran. MSc Thesis, Universiti Kebangsaan Malaysia, Selangor, Malaysia.

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

Horng, G. and C.S. Yang, 1996. Key authentication scheme for cryptosystems based on discrete logarithms. Comput. Commun., 19: 848-850. DOI: 10.1016/S0140-3664(96)01112-7

Ismail, E.S. and M.S. Hijazi, 2012. Development of a new elliptic curve cryptosystem with factoring problem. Am. J. Applied Sci., 9: 1443-1447. DOI: 10.3844/ajassp.2012.1443.1447

Ismail, E.S. and E. Sakib, 2012. A new secure and efficient elliptic curve cryptosystem. Applied Math. Sci., 6: 5573-5579.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5

Kumaraswamy, P., C.V. Guru Rao, V. Janaki and K.V.T.K.N Prashanth, 2016. Key authentication scheme-based on discrete logarithms and Chinese remainder theorem. Defence Sci. J., 66: 590-593. DOI: 10.14429/dsj.66.9649

Lee, C.C., M.S. Hwang and L.H. Li, 2003. A new key authentication scheme based on discrete logarithms. Applied Math. Comput., 139: 343-349. DOI: 10.1016/S0096-3003(02)00192-3

Menezes, A.J., P.C. van Oorschot and S.A. Vanstone, 1997. Handbook of Applied Cryptography. 1st Edn., CRC Press, ISBN-10: 1439821917, pp: 810.

Meshram, C., C.C. Lee, C.T. Li and C.L Chen, 2016. A secure key authentication scheme for cryptosystems based on GDLP and IFP. Soft Comput.

Miller, V.S., 1985. Use of elliptic curves in cryptography. Adv. Cryptol., 218: 417-426. DOI: 10.1007/3-540-39799-X_31

Peinado, A., 2004. Cryptanalysis of LHL-key authentication scheme. Applied Math. Comput., 152: 721-724. DOI: 10.1016/S0096-3003(03)00590-3

Peinado, A., 2017. Cryptanalysis of a key authentication scheme based on the Chinese remainder theorem and discrete logarithms Alberto. Int. Joint Conf., 527: 632-636. DOI: 10.1007/978-3-319-47364-2_61

Shao, Z., 2005. A new key authentication scheme for cryptosystems based on discrete logarithms. Applied Math. Comput., 167: 143-152. DOI: 10.1016/j.amc.2004.06.109

Sun, D.Z., Z.F. Cao and Y. Sun, 2005. Remarks on a new key authentication scheme based on discrete logarithms. Applied Math. Comput., 167: 572-575. DOI: 10.1016/j.amc.2004.07.021

Suparlan, A., A.A. Nassir, N. Ismail, F. Shohaimay and E.S. Ismail, 2016. Secure key authentication scheme based on discrete logarithm and factoring problems. Proceedings of the Regional Conference on Science, Technology and Social Sciences, (TSS' 16), Springer, pp: 221-229. DOI: 10.1007/978-981-10-0534-3_21

Wu, T.S. and H.Y. Lin, 2004. Robust key authentication scheme resistant to public key substitution attacks. Applied Math. Comput., 157: 825-833. DOI: 10.1016/j.amc.2003.08.074

Yoon, E.J. and K.Y. Yoo, 2005. On the security of Wu-Lin's robust key authentication scheme. Applied Math. Comput., 169: 1-7. DOI: 10.1016/J.AMC.2004.10.027.

Yoon, E.J. and K.Y. Yoo, 2007. Improving the Sun-Cao's public key authentication scheme for non-repudiation. Proceedings of the Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques, Aug. 21-24, Springer, China, pp: 1103-1109. DOI: 10.1007/978-3-540-74282-1_123

Zhan, B., Z. Li, Y. Yang and Z. Hu, 1999. On the security of HY-key authentication scheme. Comput. Commun., 22: 739-741. DOI: 10.1016/S0140-3664(99)00032-8

Zhang, F. and K. Kim, 2005. Cryptanalysis of Lee-Hwang-Li's key authentication scheme. Applied Math. Comput., 161: 101-107. DOI: 10.1016/j.amc.2003.12.012