International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 3576~3583
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp3576-3583

A new digital signature scheme with message recovery using hybrid problems

Nedal Tahat[1], Rania Shaqboua[2], Emad E. Abdallah[3], Mohammad Bsoul[4], Wasfi Shatanawi[5]
[1,2]Department of Mathematics, Faculty of Sciences, The Hashemite University, Jordan
[3,4]Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Jordan
[5]Department of Mathematics and general courses Prince Sultan University, Saudi Arabia

Article Info

Article history:

Received Nov 15, 2018
Revised Apr 9, 2019
Accepted Apr 18, 2019

Keywords:

Digital signature
Elliptic curve
Authenticated encryption
Message recovery
One-way hash function
Finite field

ABSTRACT

We present a new digital signature scheme with message recovery and its authenticated encryption based on elliptic curve discrete logarithm and quadratic residue. The main idea is to provide a higher level of security than all other techniques that use signatures with single hard problem including factoring, discrete logarithm, residuosity, or elliptic curves. The proposed digital signature schemes do not involve any modular exponentiation operations that leave no gap for attackers. The security analysis demonstrates the improved performance of the proposed schemes in comparison with existing techniques in terms of the ability to resist the most common attacks.

Corresponding Author:

Nedal Tahat,
Department of Mathematics, Faculty of Sciences,
The Hashemite University,
P.O. Box 150459, Zarqa 13115, Jordan.
Email: nedal@hu.edu.jo

1. INTRODUCTION

Digital signature with message recovery has become one of the most important aspects of data security. It is used to allow a message owner to send only a signature of his message. The verifiers use the received signature for verification first and then to recover the original message from the signature. In [1-3] Nyberg and Rueppel presented several signature schemes based on the discrete logarithm problem (DLP) to recover the encrypted messages from the received signatures. Later, Horster et al. [4] proposed an authenticated encryption scheme modified from Nyberg and Rueppel algorithms, where only the designated verifiers can retrieve and verify the messages from the signatures. Therefore, the scheme can be classified as a combination of the data encryption scheme and the digital signature scheme.

In order to recover the original message from the signature, the message cannot be hashed to reduce its size. However, if the message is large, it should be divided into a sequence blocks, and each block is encrypted and signed as a signature block individually. Consequently, each message block contains some data redundancy. The redundant data is employed to correctly link all the data blocks together. The main drawback of the above scheme is the high cost of communications. Hwang et al. [5] proposed an authenticated encryption scheme with message linkages based on Horster et al. scheme [4]. Since then, several improved authenticated encryption schemes have been proposed [6-8] to increase the performance.

Girault in [9] presents the concept of the self-certified public keys. A public key is obtained from the signature of the user's private key, with his/her identity signed by the system authority. The public key of each user does not need to be companied by a separate certificate. The proof of the public key can implicitly computed with the signature verification. Thus, the storage space and computations cost is reduced by using self-certified public keys. Clearly, the system authority does not know the user's private key, which is chosen by user privately.

Several digital signature schemes using self-certified public keys [10] have been proposed based on Girault's algorithm [9]. Various authenticated encryption schemes are presented to allow only the specified receiver to verify and to recover the original message. Obviously, all techniques depends on the fact that there is a trusted system authority (SA). In the real world, SA is not guaranteed to be totally reliable. Encinas et al. [11] showed that there is a major weakness in [10] and all related schemes [12-16] affecting both the authentication of the signer's public key and the security of the system.

Elliptic curves for cryptographic systems are introduced in [17, 18]. Elliptic curves provides a smaller key size with simpler calculations and the same level of security [19-21]. The coding and decoding can be carried out more efficiently in the elliptic curves point group, making it a very exciting feature

The above problems including the limited robustness against attacks and the high computation cost, motivated the authors to introduce a digital signature scheme with message recovery based on two hard problems. The clue is to use the elliptic curve over Z_n based on elliptic curve discrete logarithm problem (ECDLP) and quadratic residue problem (QRP). This idea is novel and never been used for digital signature approaches.

2. BACKGROUND

In this section, we describe some elementary tools on elliptic curves.

Definition: Let K be a field with characteristic > 3, then an elliptic curve can be expressed as:

$$y^2 = x^3 + ax + b \quad (1)$$

Where $a, b \in K$ and $4a^3 + 27b^2 \neq 0$. The set $E(K)$ consists of all point $(x, y), x, y \in K$ which satisfies the defining (1) together with a special point $\mathcal{O}$ called the point at infinity. Let G be a point on the elliptic curve defined in (1). If n is the smallest positive integer satisfies the equation $nG = \mathcal{O}$, then G is the base point of order n [17]-[23].

The new digital signature scheme based on both ECDLP and QRP is given as follows.

- ECDLP: Let G and C be two elliptic curve points on (1). Then find a positive integer k such that $kG = C$.
- QRP: Let p, q are two strong primes of large size and γ is an integer. Then, compute γ such that $\gamma \equiv \beta^2 (\text{mod } pq)$.

3. THE PROPOSED SCHEMES

In this section, we propose new elliptic curve digital signature schemes with message recovery based on two hard problems. We discuss in details two authenticated encryption schemes one of them is with message linkage. The proposed three schemes consist of the system initialization phase including the system parameters. There are three participants in the trusted SA, a signer U_a and a verifier U_b.

First, SA chooses the following system parameters:

- The field $K = F_p$ of order p , where p be a large prime number and $p - 1$ have two prime factors $\bar{p}$ and $\bar{q}$
- Two coefficients $a, b \in F_p$ that define the equation $y^2 = x^3 + ax + b (\text{mod } p)$ over F_p.
- $n = \bar{p}\bar{q}$, so that $n / (p - 1)$ is the root points of elliptic curve construct a circulating subgroup. G is a generating element for subgroup and its rank equals n.
- $h(.)$ is a secure hash function.
- (n, a, b, G, y) are published and(p, q) are all discarded.
- Each user U_i selects his private key $d_i \in Z_n^*$ and computes his public $y_i = d_i^2 G$ (mod n)

3.1. Digital signature scheme with message recovery

The proposed scheme is composed in two phases: the signature generation phase, and the message recovery phase.

3.1.1. Signature generation phase

Suppose that a signer $U_a$wants to sign a message M. The signature generation process is given by:

- Select a random integer $r \in [1, n - 1]$
- Compute

$$K = r^{-1} d_a\, G\ (mod\ n) = (\omega, \tau) \quad (2)$$

- Encrypt the message M to find a ciphertext

$$\delta = M\ H^{-1}(\omega)(\mathrm{mod}\ n) \quad (3)$$

- Calculate

$$\alpha = (d_a r^{-1} - d_a^2\ H(\delta))(mod\ n). \quad (4)$$

The pair (δ, α) is the signature of message M. Finally, the sender delivers (δ, α) to the receiver.

3.1.2. Message recovery phase

After receiving the digital signature (δ, α), any verifier can use U_a's public key y_a to recover the message M as follows.

- Computes

$$(\alpha G + H(\delta) y_a)(mod\ n) = K = (\omega, \tau) \quad (5)$$

- Decrypt the cipher text δ to find the plaintext M such that

$$M = \delta\ H(\ \omega)\ (mod\ n) \quad (6)$$

- Check that the format of message M.

It could be proven that the proposed scheme works correctly.

Theorem 1. The message $M$is recovered correctly from the digital signature(δ, α)through (6) *Proof***.** From (5), we have

$$\begin{aligned}(\alpha G + H(\delta) y_a)(mod\ n) &= (d_a r^{-1} - d_a^2\ H(\delta))G + H(\delta) y_a \\ &= d_a r^{-1} G + \left(- d_a^2\ H(\delta)\right) G + H(\delta)\ d_a^2\, G \\ &= d_a r^{-1} G (mod\ n) \\ &= K \\ &= (\omega, \tau)\end{aligned}$$

Then the message M is obtained by calculating

$$\delta\ H(\omega) = M\ H^{-1}(\omega) H(\omega)(mod\ n) = M$$

3.2. Authenticated encryption scheme

In this subsection, we present an authenticated encryption scheme that combine the data encryption and the digital signature scheme. In other words, the signer can generate a digital signature for message M and then deliver it to a designated verifier. Upon receiving the digital signature, only the designated verifier U_b can retrieve and verify the message M. Details of the signature generation phase and the message recovery phase are described as follows:

3.2.1. Encryption and signature generation phase

Assume that U_a wants to generate a signature for a message M and send it to U_b. The signature generating procedure is stated as follows:

- Select a random integer $r \in [1, n-1]$
- Compute

$$K = r^{-1} d_a (G + y_b)(mod\ n) = (\omega, \tau) \quad (7)$$

- Encrypt the message M to find a ciphertext δ

$$\delta = M\ H^{-1}(\omega)(\mathrm{mod}\ n) \quad (8)$$

- Calculates

$$\alpha = (d_a r^{-1} - d_a^2 \ H(\delta))(mod\ n) \tag{9}$$

Finally, U_a delivers the digital signature (δ, α) to U_b

3.2.2. Signature verification and message recovery phase

After receiving the digital signature (δ, α), U_b can recover the message M by using his/her private key d_b and the public values y_a as follows:

- Computes

$$\alpha(G + y_b) + H(\delta)(d_b^2 + 1)y_a(mod\ n) = K = (\omega, \tau) \tag{10}$$

- Decrypt the ciphertext δ to find the plaintext M such that

$$M = \delta\ H(\ \omega)\ (mod\ n) \tag{11}$$

- Checks that the format of message M is correct or not.

The following theorem is used to prove the correctness of this scheme.

Theorem 2. The designated verifier $U_b$can correctly verify the message M from the digital signature (δ, α) by (10) and (11) *Proof***.** From (10), we have

$$\begin{aligned}
&\alpha(G + y_b) + H(\delta)(d_b^2 + 1)y_a(mod\ n) \\
&= (d_a r^{-1} - d_a^2\ H(\delta))(G + y_b) \oplus H(\delta)(d_b^2 + 1)y_a \\
&= d_a r^{-1}(G + y_b) + \left(- d_a^2\ H(\delta)\right)G + (- d_a^2\ H(\delta) d_b^2)G + d_a^2\ H(\delta) d_b^2\ )G + d_a^2\ H(\delta)G \\
&= d_a r^{-1}(G + y_b)(mod\ n) \\
&= K \\
&= (\omega, \tau)
\end{aligned}$$

According to (11), the message M can be derived by calculating

$$\delta\ H(\omega) = M\ H^{-1}(\omega)H(\omega)(mod\ n) = M$$

This theorem is thus proven.

3.3. Authenticated encryption scheme with message linkage

The basic authenticated encryption scheme is only applied to smaller messages. A large message has to be divided into smaller blocks first and then each block is signed and encrypted individually. In this scheme, if the smaller blocks have been reordered, modified, deleted, or replicated during the transmission then the signature is modified as well. The details procedure is as the follows:

3.3.1. Signature and encryption generation phase

Without loss of generality, assume that U_a desires to create a message M that is to be sent toU_b. The message is composed of the sequence of $\{M_1, M_2, \ldots, M_t\}$, where $M_i \in Z_n$ for $i = 1,2, \ldots, t$. U_a fulfills the following steps to generate the signatures blocks for the message M.

- Make $c_\circ = 0$ and select a random integer $r \in [1, n-1]$ and computes

$$K = r^{-1} d_a(G + y_b)(mod\ n) = (\omega, \tau) \tag{12}$$

- Computes

$$c_i = M_i H^{-1}(c_{i-1} \oplus \omega)(mod\ n) \tag{13}$$

for $i = 1,2, \ldots, t$, where $\oplus$ *denotes the* bit wise exclusive or operator.

- Calculates

$$\begin{aligned}
&\delta = H(c_1 \parallel c_2 \parallel \cdots \parallel c_t) \\
&\alpha = (d_a r^{-1} - d_a^2\ H(\delta))(mod\ n)
\end{aligned} \tag{14}$$

Where " $\parallel$ " denotes the concatenation operator.

U_a deliver the signature blocks $(\delta, \alpha, c_1, c_2, \dots, c_t)$ to U_b via a public channel. Note that c_i is used as a linking parameter between the $i^{th}$and $(i+1)^{th}$ blocks.

3.3.2. Message recovery phase

After receiving the signature blocks $(\delta, \alpha, c_1, c_2, \dots, c_t), U_b$ can retrieve the message blocks $\{M_1, M_2, \dots, M_t\}$ by the following steps.

- Calculate $\acute{\delta} = H(c_1 \parallel c_2 \parallel \cdots \parallel c_t)$ and confirm that $\acute{\delta} = \delta$ is true.
- Compute

$$\alpha(G + y_b) + H(\delta)(d_b^2 + 1)y_a(mod\ n) = K = (\omega, \tau) \quad (15)$$

Recover the message blocks $\{M_1, M_2, \dots, M_t\}$ as follows

$$M_i = c_i H(c_{i-1} \oplus \omega)(\text{mod}\ n) \quad (16)$$

for $i = 1,2, \dots, t$and $c_\circ = 0$

The proposed scheme could be proven that it works correctly by the following theorem.

Theorem 3. In the message recovery phase, the designated verifier $U_b$can recover the message blocks $\{M_1, M_2, \dots, M_t\}$ by using Eqs. (15) and (16). ***Proof*.** From (15) we have

$$\begin{aligned} &\alpha(G + y_b) + H(\delta)(d_b^2 + 1)y_a(\text{mod}\ n) \\ &= (d_a r^{-1} - d_a^2\ H(\delta))(G + y_b) + H(\delta)(d_b^2 + 1)y_a \\ &= d_a r^{-1}(G + y_b) + \left(-\ d_a^2\ H(\delta)\right)G + (-\ d_a^2\ H(\delta)d_b^2)G + d_a^2\ H(\delta)d_b^2\ )G +\ d_a^2\ H(\delta)G \\ &= d_a r^{-1}(G + y_b)(\text{mod}\ n) \\ &= K \\ &= (\omega, \tau) \end{aligned}$$

According to Eq. (16), the message M_i can be derived by calculating

$$c_i H(c_{i-1} \oplus\ \omega)(mod\ n) = M_i H^{-1}(c_{i-1} \oplus \omega)H(c_{i-1} \oplus \omega) = M_i$$

Therefore, U_b can get the message M. This theorem is thus proven.

4. SECURITY ANALYSIS

In this section, the robustness of the proposed scheme is tested. The difficulties associated with the unauthorized attackers are based on the solution of the ECDLP and quadratic residue problem QRP. The security caused from ECDLP and QRP is sufficient under reasonable computational complexity. Some possible attacks by which an adversary (Adv) may try to take down the new elliptic curve digital signatures with message recovery will be analyzed as follows:

Attack 1. An Adv attempts to derive the user's private key d_i from all public information available. An Adv can derive d_i from $y_i \equiv d_i^2 G(mod\ n)$. It is obvious that to find d_i the Adv has to solve both the ECDLP and QRP. An Adv wants to get the signer's private key d_a from the signer's signature δ and α in the message recovery scheme, he/she should first obtain δ , α and r, Adv need to solve the ECDLP to obtain $d_a r^{-1}$ and then obtain $d_a^2\ (mod\ n)$ by computing $d_a^2 \equiv (\alpha - d_a r^{-1})H(\delta)^{-1}(mod\ n)$. The Adv needs to know the secret random r in addition to solve the hard ECDLP. If the Adv know the random number r he must solve the difficult QRP and then obtain d_a from $d_a^2\ (mod\ n)$. This is because finding d_a is computationally equivalent to factoring the composite number n . Similarly the second scheme and third scheme the Adv still facing the same difficulties.

Attack 2. An Adv impersonates the signer's signature without knowing the signer's private key. In the first proposed scheme, Adv can know the signature δ, α, the signer's public key y_a and the message M. If he tries to invent signer's signature, he needs to select a random number $\acute{r}$ and a message $\acute{M}$. However, he cannot generate $\acute{\omega}$ by computing $K = K^{\acute{}} = \acute{r}^{-1} d_a G(mod\ n) = (\acute{\omega}\ , \acute{\tau}\ )$ because the Adv does not know the signer's private key d_a.

Attack 3. In the authenticated encryption scheme, an Adv attempts to decrypt the message M from the digital signature (δ, α) without U_b's private key d_b. The Adv does not know d_b, he/she cannot obtain ω to recover $M = \delta H(\ \omega)\ (mod\ n)$ by calculating $\alpha(G + y_b) + H(\delta)(d_b^2 + 1)y_a(mod\ n) = (\omega, \tau)$. The Adv attempts to find $\alpha(G + y_b) + H(\delta)(d_b^2 + 1) = d_a r^{-1}(G + y_b)(mod\ n)$ from $\alpha = (d_a r^{-1} - d_a^2\ H(\delta))$ and then calculates $M = \delta H(\ \omega)$. Thus, he/she needs to know the private key d_a by solving ECDLP and QRP.

In the authenticated encryption scheme with message linkage, he cannot get α, δ and $c_1, c_2, \dots c_t$. If he wants to decrypt the i^{th} cipher text block, he must know the verifier's private key d_b and then computes the value ω from $r^{-1} d_a(G + y_b) = (\omega, \tau)$. The Adv will fail to get the content of the message blocks.

Attack 4. An Adv recorders, modifies, deletes or replicates the message blocks. He/she should also modify the signature α by computing the equations $\delta = H(c_1 \parallel c_2 \parallel \cdots \parallel c_t)$ and $\alpha \equiv (d_a r^{-1} - d_a^2\ H(\delta))(mod\ n)$. If he cannot execute the modification, reorder, deletion or replication of the message blocks, he/she will not pass the verification equation $\acute{\delta} \stackrel{?}{=} \delta$.

Attack 5. Suppose the difficulty of computing ECDLP has been broken.
If an Adv breaks the ECDLP and get access to α, δ, M, and the signer's public key y_a, he can derive the $d_a r^{-1}$ from the equation $K \equiv r^{-1} d_a\, G\ (mod\ n)$. If he wants to get the signer's private key d_a from $\alpha \equiv (d_a r^{-1} - d_a^2\ H(\delta))(mod\ n)$ he must break the difficulty of QRP simultaneously. It is extremely hard to get the signer's private key d_a by computing $d_a^2 \equiv (\alpha - d_a r^{-1})H(\delta)^{-1}(mod\ n)$, where finding d_a is computationally equivalent to factoring the composite number.

Attack 6. Suppose the difficulty of computing QRP has been broken. Therefore, an Adv can undertake $\alpha \equiv (d_a r^{-1} - d_a^2\ H(\delta))(mod\ n)$ which is related the factoring assumption. Although an Adv can solve the difficulty of QRP, he cannot still get the signer's private key d_a from the equation. Because the equations contains two unknown variables r and d_a.

Attack 7. An Adv, without U_a's private key d_a, attempts to forge the digital signature to impersonate U_a. Suppose an Adv wants to forge a valid signature for a given message $\acute{M}$ that can pass the verification equation. If the Adv determines α first, he will have to solve $H(\delta)$ to obtain the value of δ. However, this process is as difficult as breaking the one-way hash function. On the other hand, if the Adv fixes the integer δ first, he/she has to obtain the value of α by solving ECDLP.

5. PERFOMANCE EVALUATION

In this section, we evaluate the performance of the proposed schemes. The following notations are used to analyze the computational complexity:
- T_{exp} is the time complexity for executing the modular exponentiation;
- T_{mul} is the time for executing the modular multiplication;
- T_{ec-add} is the time complexity for executing the addition of two elliptic curve points;
- T_{ec-mul} is the time complexity for executing the multiplication on elliptic curve points;
- T_{sqr} is the time complexity for executing the modular square;
- T_h is the time for executing the one-way hash function.

To describe the efficiency performance in terms of T_{mul}, we convert various operations units to the time complexity for executing the modular multiplication [8].

$$T_{exp} \approx 240\ T_{mul};\ T_{ec-mul} \approx 29 T_{mul};\ T_{ec-add} \approx 0.12 T_{mul}$$

First scheme, in the signature generation phase, the signer needs $(T_{ec-mul} + 4T_{mul} + T_{sqr} + 2T_h) \approx 33T_{mul} + T_{sqr} + 2T_h$ to perform the process of this phase. In the message recovery and verification phase, the verifier should perform $(2\ T_{ec-mul} + T_{ec-add} + T_{mul} + 2T_h) \approx (59.12 T_{mul} + 2T_h)$ to complete the processes the message recovery.

Second scheme, in the authenticated encryption scheme, the signer requires $\left(T_{ec-mul} + T_{ec-add} + 4T_{mul} + T_{sqr} + 2T_h\right) \approx \left(33.12 T_{mul} + T_{sqr} + 2T_h\right)$ to generate the signature. The time required by the designated verifier to recover the message is $(2T_{ec-mul} + 2T_{ec-add} + 2T_{mul} + T_{sqr} + 2T_h) \approx (60.24\ T_{mul} + T_{sqr} + 2T_h)$.

Third scheme, if there are t blocks. The authenticated encryption scheme with message linkage requires $(T_{ec-mul} + T_{ec-add} + T_{sqr} + (t + 4)T_{mul} + (t + 2)T_h) \approx ((t + 33.12)\ T_{mul} + T_{sqr} + (t + 2)T_h)$to generate the message blocks, while verifying and retrieving the message blocks requires $(2T_{ec-mul} + 2T_{ec-add} + T_{sqr} + (t + 1)T_{mul} + (t + 2)T_h) \approx ((t + 59.24)T_{mul} + T_{sqr} + (t + 2)T_h)$.

The efficiency performance reveals that the modular multiplication operation dominates our proposed schemes in terms of time complexity. Note that, in our proposed algorithms no modular exponentiation operation is used giving our schemes a clear advantage over other schemes.

6. CONCLUSION

In this paper, we proposed new elliptic curve digital signature schemes with message recovery based on ECDLP and QRP. Multiple levels of security are used to amplify the difficulty of breaking the proposed system. It requires breaking ECDLP, QRP and a one-way hash function. The main attractive features of the Elliptic curve cryptography are simplicity and easiness of achieving encoding. The proposed schemes require minimal operation for signing and verifying the signature. The effectiveness and the security of the proposed schemes are evaluated by conducting several attacks. The results clearly showed the robustness of the proposed schemes.

REFERENCES

[1] K. Nyberg, R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," *Proceedings of the 1st ACM Conference On Computer and Communications Security*, Fairfax, VA, 1993.

[2] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on discrete logarithm problem," *Advances in Cryptology – EUROCRYPT'94*, Springer, Berlin, 1994, pp. 175–190.

[3] K. Nyberg, R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Designs Codes Cryptograph*y, vol.7, no. 1-2, pp. 61-81, 1996.

[4] P. Horster, M. Michels, H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, pp. 1212-1213, 1994.

[5] S. J. Hwang, C. C. Chang, W. P. Yang, "Authenticated encryption schemes with message linkage," *Information Processing Letters*, vol. 58, no. 4, pp. 189-194, 1996.

[6] S. Araki, S. Uehara, K. Imamura, "The limited verifier signature and its application," *IEIDE Transaction on Fundamentals*, vol. 82, no. 1, pp. 63-68, 1999.

[7] W. B. Lee, C. C. Chang, "Authenticated encryption schemes with linkage between message blocks," *Information Processing Letters*, vol. 63, no. 5, pp. 247-250, 1997.

[8] Y. M. Tseng, J. K. Jan, "An efficient authenticated encryption scheme with message linkages and low communication costs," *Journal of Information Science and Engineering*, vol. 18, no. 1, pp. 41-46, 2002.

[9] M. Girault, "Self-certified public keys," *Advances in Cryptology – EUROCRYPT_91*, Springer, Berlin, 1991, pp. 491–497.

[10] Y. M. Tseng, J. K. Jan and H. Y. Chien, "Digital signature with message recovery using self-certified public keys and its variants," *Applied Mathematics and Computation*, vol. 136, no. 2-3, pp. 203-214, 2003.

[11] L. H. Encines, A. M. D. Rey and J. M. Masque, "A weakness in authenticated encryption scheme based on Tseng et al.'s schemes," *International Journal of Network Security*, vol. 7, no. 2, pp. 185–187, Sep 2008.

[12] Y. F. Chang, C. C. Chang and H. F. Huang, "Digital signature with message recovery using self- certified public keys without trustworthy system authority," *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 211-227, 2005.

[13] S. J. Hwang, "Improvement of Tseng et al's authenticated encryption scheme," *Applied Mathematics and Computation*, vol. 165, no. 1, pp. 1-4, 2005.

[14] Z. Shao, "Improvement of digital signature with message recovery using self-certified public keys and its variants," *Applied Mathematics and Computation*, vol. 159, no. 2, pp. 391-399, 2004.

[15] Q. Xie, and X. Y. Yu, "Cryptanalysis of Tseng, *et al.*'s authenticated encryption schemes," *Applied Mathematics and Computation*, vol. 158, no. 1, pp. 1-5, 2004.

[16] J. Zhang, W. Zou, D. Chen, and Y. Wang, "On the security of a digital signature with message recovery using self-certified public key," *Informatica*, vol. 29, pp. 343-346, 2005.

[17] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 77, pp. 203-209, 1987.

[18] V. Miller, "Use of elliptic curve in cryptography," *Advances in Cryptology-Proceeding of CRYPTO' 85 Lecture Notes in Computer Sciences*, 218, Springer-Verlage, 1986, pp. 417-426.

[19] A. Menezes and N. Koblitz, *Elliptic curve public key cryptosystem*, Kluwer Academic Publishers, 1993.

[20] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, Cambridge University Press, 1999.

[21] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[22] D. Johnson, D. A. Menezesand S. Vanstone, "The elliptic curve digital signature algorithm," *International Journal of Information Security*, vol. 1, no. 1, pp. 36-63, 2001.

[23] N. Koblitz, A. Menezes and S. Vanstone, "The state of elliptic curve cryptography," *Designs Code Cryptography*, vol. 19, no. 2-3, pp. 173-193, 2000.

BIOGRAPHIES OF AUTHORS

Nedal Tahat, He received the B.Sc. degree in mathematics from Yarmouk University, Jordan, in 1994, the M.Sc. degree in Pure Mathematics from Al al-Bayt University,Jordan, in 1998, and the Ph.D. degree in Applied Number Theory (Cryptography) from National University of Malaysia (UKM) in 2010. He is an Associate Professor at Department Mathematics, Hashemite University. His main research interests are cryptology and number theory. He has published more than 35 papers, authored/coauthored, and more than 15 refereed journal and conference papers.

Rania Shaqboua, She received the B.Sc. degree in mathematics from Yarmouk University, Jordan, in 1999, the M.Sc. degree in Pure Mathematics from University of Jordan, IN 2005. She is an Assistant Lecturer at Department Mathematics, Hashemite University.

Alaa Abdallah is currently an Associate Professor in the Department of Computer Science at the Hashemite University (HU), Jordan. He received his PhD in Computer Science from Concordia University in 2008, where he worked on routing algorithms for mobile ad hoc networks. He received his BS from Yarmouk University, Jordan, and MS from the University of Jordan in 2000 and 2004, respectively. Prior to joining HU, he was a network researcher at consulting private company in Montreal (20082011). His current research interests include routing protocols for ad hoc networks, parallel and distributed systems, and multimedia security.

Mohammad Bsoul is an Associate Professor in the Computer Science Department of Hashemite University. He received his BSc in Computer Science from Jordan University of Science and Technology, Jordan, his Master from University ofWestern Sydney, Australia, and his PhD from Loughborough University, UK. His research interests include wireless sensor networks, grid computing, distributed systems, and performance evaluation.

Wasfi Shatanawi, PhD, is a professor of Mathematics in the Department of Mathematics at Prince Sultan University. Shatanawi completed his PhD study from Carleton University/Canada in 2001. He published more than 120 papers in high standard journals. Shatanawi is one of the most influential scientific minds in the world. Professor Shatanawi is highly cited researchers for four consecutive years 2015, 2016, 2017 and 2018 according to Clarivate Analytic (previously Thomson Reuters). Shatanawi is an editor in many reputable journals.