Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/140308

Authenticated Encryption Scheme Based on ECDLP and DLP

Mohammad S. Hijazi[1], *Nedal Tahat*[2,*], *Ashraf A. Tahat*[3], *Raft Abdelrahim*[1] *and Eddie S. Ismail*[4]

[1] Department of Mathematics, College of Arts and Sciences Tabarjal, Jouf University, KSA
[2] Department of Mathematics, Faculty of Sciences, The Hashemite University, Zarqa 13133, Jordan
[3] Department of Communications Engineering, Princess Sumaya University for Technology, Jordan
[4] School of Mathematical Science, Faculty of Science and Technology, University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Received: 17 Dec. 2019, Revised: 19 Feb . 2020, Accepted: 27 Feb. 2020
Published online: 1 May 2020

Abstract: This paper presents a new authenticated encryption scheme (AES) based on elliptic curve discrete logarithm problem (ECDLP) and discrete logarithm problem (DLP). Assume that we have one signer, and a set of $U = (u_1, u_2, ..., u_l)$, which represents the verifiers group of L members. A single signer can encrypt and sign the message only if k $(1 \leq k \leq l)$ or more verifiers agree to recover the message m on behalf of the whole verifier group U. In addition, we need a system authority with the task of generating the parameter, while a trusted clerk selected by the signer is needed to verify the signature's validity. This scheme aims to overcome the modular exponentiation problem utilizing elliptic curve cryptography (ECC). To attain the desired benefit of enhanced performance and improved security, the presented technique is established based on the elliptic curve cryptosystem and discrete logarithm problems. Moreover, it resists strong attacks and operates efficiently. Compared to similar functional techniques, it requires a lower number of exponential and module operations.

Keywords: Authenticated Encryption, elliptic curve,discrete logarithm problem , cryptosystem

1 Introduction

A remarkable number of the existing Authenticated Encryption Schemes (AESs)share the feature that they rely on a single number theoretic cryptographic assumption. In [1], the authors suggested a signature that is associated with a discrete logarithm problem message recover. The authors of [2] presented an authenticated encryption technique relying on a modified message recovery method of that suggested in [1]. The scheme lacked security in application due to the fact that it endured "known ciphertext-plaintext attack". An improved scheme was proposed in [3]. In [4],the proposed scheme mitigated the disadvantages of the technique that was proposed in reference [3]. The authors of [6] proposed a new application in AES. Reference[7] presented an AES relying on ECDLP. Despite the fact that the basic AESs can reduce transmission cost effectively, those schemes still involve some drawbacks. The message to be transmitted has to be broken into several message segments. Subsequently, the signer sign and encrypt every segment and communicate it to a recipient. Hence, this will raise costs in terms of computations and transmission. However the authors of [5] suggested an AES incorporating message interconnection. The author of [8] revealed that the scheme of [5] raised an impediment, where the message segments must be sent in the right following the other. Although the authors of [9] presented a computationally efficient AES with lower cost of communications, its security was breached by [10] and [11].

In 1998 [13], the AES proposed was based on understanding that only a single verifier might use it . Accordingly, they advocated a (t,n) threshold signature with AES to broaden the verification capability applied to a single signer and an array of verifiers. In [12], the authors expanded the scheme of [13] to put forth a (t,n) threshold AES, which was applied to a party of signers and a party of verifiers. However, the authors of [14] indicated that the scheme of [12] was insecure.

* Corresponding author e-mail: nedal@hu.edu.jo

© 2020 NSP
Natural Sciences Publishing Cor.

The ECC employs efficient operation and surpasses those of alternative cryptosystems, such as the RSA and the DSA security approaches, because ECC method employs a smaller key size and reduced processing complexity [17,18]. Thus,the techniques that rely on ECDLP and DLP out performs those established on the DLP solely reduction in exponentiation computations. Considering these benefits, we present a novel Authenticated Encryption Scheme established on the ECDLP and DLP problems. The security involved in the proposed approach is greatly enhanced because an adversary's ability to simultaneously unravel two hard problems is virtually improbable.
The remainder of this paper is organized as follows: we propose a new AES in Section Two. In Section Three,the security properties of the proposed scheme are discussed. Performance is addressed in section Four.In Section Five,covers a numerical illustration of the presented authenticated cryptosystem technique. Section Six dedicated to discussion and conclusion.

2 The Proposed Scheme

Our scheme comprises a three-stage procedure: it starts with parameter formation stage, then the signature and encryption generation stage, and concludes with the stage of message recovery. They are described in the following subsections.

2.1 Parameter Formation Stage

Domain parameters are selected by the system authority [16] and comprise the following:

1.A pair of large prime numbers p and q that represent the field sizes.
2.The subsequent elliptic curve equation is defined by the pair of coefficients $a_1, a_2 \in \mathbb{F}_p$

$$y^2 = x^3 + a_1 x + a_2 (\bmod p) \text{ of elliptic curve } E \text{ over } \mathbb{F}_p.$$

thereupon $p > 3$ and $4a_1^3 + 27a_2^2 \neq 0 \, (\bmod p)$.
3.An order q generator point $G = (x_G, y_G)$.
4.Two secret polynomials $f(x) = c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \ldots + c_1 + c_0 (\bmod q)$ and $p(x) = d_{k-1}x^{k-1} + d_{k-2}x^{k-2} + \ldots + d_1 + d_0 (\bmod q)$ in which $c_j, d_j \in [1, q-1]$ for $j = 1, 2, \ldots k-1$.
5.A private and a public keys, $Y = aG$ and a, receptively, for the signer. In addition to group private and public keys, c_0 and $Y_u = c_0 G$, respectively, key for U.
6.An individual private and public keys, $f(x_i)$ and $Y_i = f(x_i)G$, respectively, for every verifier u_i belonging to U such that $i = 1, 2, \ldots, l$, along with x_i as the public state linked to each verifier u_i.
7.The clerk's pair of private and public keys, d_0 and $y = g^{d_0} (\bmod q)$, respectively.
8.The parameters of the system, p, q, E, G, Y, y, Y_i for $(i = 1, 2, \ldots, l)$ and Y_u are published by the system authority.

2.2 Signature and Encryption Formation Stage

If it is assumed that the signer commences with signing a message m, the first step will be that the signer creates her/his signature for the message m, in the ensuing manner:

1.An integer $b \in [1, q-1]$ is chosen randomly, then calculate $\bar{B} = bG = (\bar{x}, \bar{y})$.
2.Compute $Z = (a + b\bar{x})(\bmod q) Y_u = (x_Z, y_Z)$, thereupon Z is considered to be, for each of signer and the group of verifiers U, the common session key.
3.Compute $B = \bar{x}\bar{B} = (x_B, y_B)$.
4.Calculate $c = (m x_B + x_Z)(\bmod q)$.
5.The digital signature is produced as: $s = (b\bar{x} - ca)(\bmod q)$, then, the clerk, $(\bar{x}, c, s)$ is communicated.
After reception of the digital signature on the message m, the validity of the signature is confirmed by the clerk as:

$$\bar{x}\bar{B} = sG + cY$$

To confirm the the validity of the digital signature, the preceding equation must be fulfilled. Subsequently, the following tasks are performed by the clerk:
6.Compute $\bar{R} = s y^{d_0} (\bmod q)$.
7.The signature of the message m, $(c, \bar{R})$, is sent to the verifier group U.
8.Compute $p(i)$ for $i = 1, 2, \ldots, k$. Next, send it to the corresponding verifier.

2.3 Message Recovery Stage

Assuming that after the signature $(c, \bar{R})$ has been received, the message m could be recovered by any k verifiers from the verifier group U. Next, the following steps are carried out to retrieve the message m by each participant verifier $u_i (i = 1, 2, ..k)$:

1.Computes $L_i = y^{-w_i}$, where $w_i = p(i) \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{0 - x_j}{x_i - x_j} (\bmod q)$.
2.Send L_i through a secure channel to the other participating verifiers.
3.Compute $\prod_{i=1}^{k} L_i = \prod_{i=1}^{k} y^{-w_i} = y^{-\sum_{i=1}^{k} w_i} = y^{-p(0)} = y^{-d_0}$.
4.Calculate $s = \bar{R} y^{-d_0} = s (\bmod q)$.
5.Compute $A = sG + cY = (x_A, y_A)$.

© 2020 NSP
Natural Sciences Publishing Cor.

6.Compute $z_i = f(x_i)\prod_{\substack{j=1\\j\neq i}}^{k}(\frac{0-x_j}{x_i-x_j})(Y+A) = (x_{z_i}, y_{z_i})$

7.Utilizing a secure channel, send z_i to the designated participant.

8.The key for common session is found using $\bar{Z} = \sum_{i=1}^{k} Z_i = (x_{\bar{Z}}, y_{\bar{Z}})$.

9.Calculate $m = (c - x_{\bar{Z}})x_A^{-1} \bmod q$.

3 Security Analysis

We demonstrate that this new technique is heuristically secure when investigated under the most common attacks of interest within the domain of cryptosystems. These attacks were mentioned previously. The new cryptosystem is analyzed, we thereupon describe how the Adversary (Adv) may attempt to breach the new scheme. As a start, correctness of the scheme is inspected. Subsequently, we assess security performance through illustrating that its ability to resist all defined cryptosystem attacks. Proving the following theorems, we aim to confirm our new scheme's validity.

Theorem 2.1 If the group signature $(c, \bar{R})$ is created in the signature formation stage,the message m could be retrieved by the verifier in the message recovery stage.

*Proof.*Note that

$$\begin{aligned} A &= sG + cY = (x_A, y_A) = (\bar{x}b - ca)G + caG \\ &= \bar{x}bG \\ &= \bar{x}\bar{B} \\ &= B = (x_B, y_B) \end{aligned}$$

Also we have:

$$\begin{aligned} \bar{Z} &= \sum_{i=1}^{k} Z_i \\ &= \sum_{i=1}^{k} f(x_i)\prod_{\substack{j=1\\j\neq i}}^{k}(\frac{0-x_j}{x_i-x_j})(Y+A) \\ &= f(0)(aG+A) \\ &= ac_0G + c_0B \\ &= aY_u + c_0\bar{x}\bar{B} \\ &= aY_u + c_0\bar{x}bG \\ &= aY_u + b\bar{x}Y_u \\ &= (a+b\bar{x})Y_u \\ &= Z \end{aligned}$$

Then,

$$\begin{aligned} (c - x_{\bar{Z}})x_A^{-1} \bmod q &= (mx_B + x_Z - x_{\bar{z}})x_A^{-1} \\ &= (mx_B + x_Z)x_A^{-1} \\ &= (mx_A)x_A^{-1} \\ &= m \mod q \end{aligned}$$

In the following section we discuss some possible attacks against the proposed scheme and reveal that it is secure under the protection of the ECDLP and DLP assumption.

Attack 1. Adv desire to derive the private keys a and c_0 from the public keys $Y = aG$ and $Y_u = c_0G$, or s/he derives the personal private keys $f(x_i)$ from the personal public keys $Y_i = f(x_i)G$. Hence s/he will be confronted with the challenge of figuring out the ECDLP. Such problem is considered to be impossible to unravel via practical methods of computations. Accordingly, this type of attack is futile. In addition, if the Adv attempts to derive the private key d_0 from the public key $y = g^{d_0} \bmod q$ for the signer, s/he is required to untangle the DLP, which is evidently impractical.

Attack 2. If it is assumed the number of $(k-1)$ from verifiers $(u_1, u_2, \ldots, u_{(k-1)})$, which desire to fabricate the signature $(c, \bar{R})$ for a message m in order to cause the kth verifier u_k to have confidence that the signer has created the aforesaid signature. First, these $k-1$ conspirators pick, in a random fashion, three numbers $(c, \bar{R})$ for developing the false$A$. This is impossible since the attacker needs the number $p(k)$ to compute y^{-d_0}, and to then extract$s$. Nevertheless, s/he is incapable of doing that due to the fact that $p(x)$ is a secret polynomial, while the clerk is a trusted person selected by the signer.If s/he attempts to computey^{-d_0}, s/he will encounter the DLP.

Attack 3. Consider that that Adv is capable of unravelling the ECDLP. Under this scenario, the adversary knows the private keys $a, c_0, f(x_i), i = 1, \ldots, k$. Unfortunately, he cannot extract s because he is unable to find y^{-d_0} because of the predicament of DLP. Thus, he is incapable of defining m.

Attack 4. Suppose that the attacker is capable of unravelling the DLP. Under this scenario, the attacker knows d_0, then s/he can compute y^{-d_0} and extract s, so s/he can compute A. However, s/he is unable to compute z_i since s/he requires the private keys $f(x_k), i = 1, 2, \ldots, k$ of the corresponding verifiers group $u_i (i = 1, 2, \ldots, k)$ suggesting that the attacker will fail because of ECDLP.

4 Performance Evaluation

In this section, we examine performance, in terms of two key indicators, of our scheme, namely complexity of needed computations and communication costs. The subsequent notations are devised for the purpose of analyzing the scheme's performance:

–The number of secret keys, and number of public keys, of the scheme are SK and PK, respectively.

–T_{mul} denotes an executing a modular multiplication time complexity.

© 2020 NSP
Natural Sciences Publishing Cor.

Table 1: Time complexity performance estimation and comparison

Item of comparison	Scheme by Chen		The Proposal	
	Time complexity	Complexity in T_{mul}	Time Complexity	Complexity in T_{mul}
Parameter formation stage	$(n+l+2)T_{ec-mul}$	$(29n+29l+58)T_{mul}$	$(2+l)T_{ec-mul}+T_{exp}$	$(298+29l)T_{mul}$
Signature formation stage	$(t+5)T_{ec-mul}+(2t-1)T_{ec-add}+(6t-1)T_{mul}+(3t-3)T_{inv}$	$(35.24t-143.88)T_{mul}+(3t-3)T_{inv}$	$6T_{ec-mul}+T_{ec-add}+5T_{mul}+2T_{exp}$	$659.12T_{mul}$
Message retrieval stage	$3T_{ec-mul}+(k+2)T_{ec-add}+(2k+1)T_{mul}+kT_{inv}$	$(2.12k+59.24)T_{mul}+kT_{inv}$	$3T_{ec-mul}+(k+2)T_{ec-add}+(2k+2k^2+1)T_{mul}+kT_{exp}+T_{inv}$	$(89.24+242.12k+2k^2)T_{mul}+T_{inv}$

–T_{exp} is a measure for performing a modular exponentiation computation time complexity.
–T_{inv} presents an evaluation measure for a modular inverse computation time complexity.
–T_{ec-add} denotes an executing the addition of two elliptic curve points time complexity.
–T_{ec-mul} denotes an executing the multiplication on elliptic curve time complexity.
–$|x|$ stands for the bit length of x.

In order to recapitulate the performance of cryptosystems intrems of efficiency, we adapt the subsequent conversion provided in [15,19]. It works by converting a number of operations units to alternate units of execution of the modular multiplication.

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

In addition, we depicted and investigated the efficiency performance of the newly developed cryptosystems. The efficiency performance is heavily dependent on the parameters used; mainly on the modulus n. To depict the performance of each scheme, we utilize the following criteria:

–The number of keys,
–The complexity in computations and
–The incurred costs of communication.

Table (1) summarizes the efficiency performance comparing that of reference [10] and that of our scheme. Our scheme needs $(298+29l)T_{mul}$ in terms of time complexity within the parameter formation stage, $659.12T_{mul}$ in terms of time complexity within the signature formation stage, and $(89.24+242.12k+2k^2)T_{mul}$ in terms of time complexity within the message recovery stage, when assuming that T_{inv} is negligible.

5 Numerical simulation of the AES

For purpose of validation, we illustrate an example to show the basic principle of our developed scheme. Practitioners are not recommended to choose keys or parameters computed in this example in practice since inappropriate parameters would make this scheme vulnerable to attacks.

Assume that $p = 1091$, $q = 1051$, and consider the elliptic curve equation $E : y^2 = x^3 - 3x + 69 \pmod{1091}$. The point $G = (299,62)$ is a base point with order $q = 1051$ and $g = 20 \in \mathbb{Z}_q^*$. We select two secret polynomials, $f(x) = 71x^2 + 103x + 119 \pmod{1051}$ and $p(x) = 37x^2 + 61x + 83 \pmod{1051}$. Then, we select a private key $a = 113$ for the signer, $c_0 = 119$ as a private key for the group of verifier U and $d_0 = 83$ a private key for the clerk. Calculate the public key, as follows:

–$Y = aG = 113G = (643,1012)$
–$Y_u = c_0G = 119G = (972,360)$
–$y = 20^{83} = 1032 \pmod{1051}$

We will apply our example on 3 members verifier group. Choose $x_1 = 203, x_2 = 164$ and $x_3 = 373$ and compute $Y_1 = (691,674)$, $Y_2 = (491,895)$ and $(491,196)$.

In signature generation phase, the signer generates his or her signature for a chosen message $m = 733$, as follows:

© 2020 NSP
Natural Sciences Publishing Cor.

1.Select random integer $b = 523 \in [1, 1050]$ and compute $\bar{B} = (927, 259) = (\bar{x}, \bar{y})$.
2.Compute $Z = (1064, 754) = (x_z, y_z)$.
3.Compute $B = (116, 321) = (x_B, y_B)$.
4.Calculate $c = (mx_B + x_z)(\text{mod } q) = 961$.
5.Generate the digital signature $s = (b\bar{x} - ca)(\text{mod } q) = 1021$ and send it to the clerk.
After the digital signature on the message m is received, the clerk verifies the validity of the signature as follows:

$$\bar{x}\bar{B} = 927(523G) = (116, 321)$$
$$sG + cY = 1021G + 961(113)G = (116, 321)$$

If the equation is satisfied, validity of the digital signature is established. Then, the clerk does the following:
6.Compute $\bar{R} = sy^{d_0} = 236(\text{mod } q)$.
7.Send the signature $(961, 236)$ for the message $m = 733$ to the verifier group U.
8.Compute $p(1) = 181$, $p(2) = 353$ and $p(3) = 599$ and send it to the corresponding verifier.

After receiving the signature $(c, \bar{R}) = (961, 236)$ any $k = 3$ verfieirs can recover the message m by executing the following steps.

1.Compute $L_1 = 618$, $L_2 = 7760$ and $L_3 = 729$.
2.Send L_1, L_2, L_3 to other participant verifier via a secure channel.
3.Compute $\prod_{i=1}^{k} L_i = 116$.
4.Calculate $s = \bar{R}y^{-d_0} = 1021(\text{mod } q)$.
5.Compute $A = sG + cY = (116, 321) = (x_A, y_A)$.
6.Compute $z_1 = 355G = (x_{z_1}, y_{z_1})$, $z_2 = 158G = (x_{z_2}, y_{z_2})$ and $z_3 = 427G = (x_{z_3}, y_{z_3})$
7.Send z_1, z_2 and z_3 to the other participant via a secure channel.
8.Compute the common session key $\bar{Z} = (1064, 754) = (x_{\bar{Z}}, y_{\bar{Z}})$.
9.Calculate $m = (c - x_{\bar{Z}})x_A^{-1} \text{mod } q = (961 - 1064)(116^{-1}) = 733$.

6 Discussion and Conclusion

A remarkable number of the existing AESs in the literature share the feature that they rely on a single number theoretic cryptographic hard problem. Despite the fact that these schemes emerge to be secure today, if an Adv succeeds in solving this problem in the immanent future, s/he will be able to recover all secret information inclusive of secret keys and read any message in the genuine form. Accordingly, we proposed in this paper a new AES relying on ECDLP and DLP. This newly developed technique excels the schemes established on a single hard problem. In other words, it longer and higher level of security. By virtue of the fact that in order to compromise the scheme the attacker must simultaneously solve two problems, and that poses an impossibility. Moreover, we demonstrated that this new technique is heuristically secure when investigated under the most common attacks of interest within the domain of cryptosystems, namely the direct attack, the DLP attack, and the ECDLP attack. That was performed by assessing the security performance by means of proofs and illustrations to confirm our new scheme's validity. In terms of efficiency performance, we found that the new authenticated encryption schemes needs $(298 + 29l)T_{mul}$ in the parameter formation stage, $659.12T_{mul}$ time complexity in the signature formation stage, whereas the message recovery stage necessitates $(89.24 + 242.12k + 2k^2)T_{mul} + T_{inv}$ time complexity.

References

[1] K. Nyberg and R. A. Rueppel, A new signature scheme based on the dsa giving message recovery,In ACM Computer and Communications Security, **1**, 158-61(1993)
[2] P. Horster and M. Michels and H. Authenticated encryption schemes with low communication costs,IEEE Electronics Letters, **30**, 1212–1213(1994)
[3] W. B. Lee and C. C. Chan, Authenticated encryption scheme without using a one way function, IEEE Electronics Letter, **31**, 1656-1657(1995).
[4] T. S. Wu and C. L. Hsu, Convertible authenticated encryption scheme, The journal of Systems and Software, **93**, 281-282(2002).
[5] N. Lee and T. Hwang, Modified Harn signature scheme based on factoring and discrete logarithms, IEE Proceeding of Computers Digital Techniques, **143**, 196-198(1996).
[6] C. Ma and K. Che, Publicly verifiable authenticated encryption, IEEE Electronics Letters, **39**, 281-282(2003).
[7] S. F. Tzeng and M. S. Hwang, Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem, Computer Standards and Interface,**26**, 61-71(2004).
[8] W. B. Lee and C. C. Chang, Authenticated encryption schemes with linkage between message blocks ,Information Processing Letter, **63**, 247-250(1996).
[9] Y. M. Tseng and J. K. Jan and H. Y. Chien, Authenticated encryption schemes with message linkages for message flows.International Journal of Computers, textbf29, 101-109,(2003).
[10] B. H. Chen, Improvement of authenticated encryption schemes with message linkages for message flows, Computers and Electrical Engineering, **30**, 465-469(2004).
[11] Z. Zhang and S. Araki and G. Xiao, Improvement of Tseng et al.'s authenticated encryption schemes with message linkages, Computers and Electrical Engineering, **162**, 1475-1483(2005).
[12] C. T. Wang and C. C. Chang and C. H. Lin, Generalization of threshold signature and authenticated encryption for group communications, Cryptologia, **E83-A**, 1228-1237 (2000).
[13] C. L. Hsu and T. C. Wu, Authenticated encryption scheme with (t, n) shared verification, **145**, 117-120(1998).
[14] C. L. Hsu and T. S. Wu, and T. C. Wu,Improvements of generalization of threshold signature and authenticated

© 2020 NSP
Natural Sciences Publishing Cor.

encryption for group communications, Information Processing Lettes, **81**, 41-45(2002).
[15] N. Koblizt and A. Menezes and S. Vanstone, The state of elliptic curve cryptography, Design, Code Cryptography, **19**,173-193(2000).
[16] T.-S. Chen et al., A practical authenticated encryption scheme based on the elliptic curve cryptosystem, Computer Standards and Interfaces, **26**, 461-469 (2004).
[17] N. Tahat, R Shaqboua, E. E. Abdallah, M. Bsoul and W. Shatanawi, A new digital signature scheme with message recovery using hybrid problems, International Journal of Electrical and Computer Engineering, **9**, 3576-3583(2019).
[18] N. Tahat, Convertible multi-authenticated encryption scheme with verification based on elliptic curve discrete logarithm problem, Int. J. Computer Applications in Technology, **54**, 229-235(2016).
[19] N. Tahat and M. S. Hijazi, A New Digital Signature Scheme Based on Chaotic Maps and Quadratic Residue Problems, Applied Mathematics and Information Sciences, **13**, 115-120 (2019).

Mohammad Saleh Hijazi is an assistant professor and head of the mathematics department in the college of arts and sciences in Jouf University since 2014 until present. He got his phd in mathematics from University Kebengsaan Malasya (UKM) in 2013. The PhD dissertation is about cryptography, design new cryptosystem and digital signature schemes based on multiple hard problems based on number theory and algebra. He also holds a M.Sc degree in Mathematics from Yarmouk University -Jordan, 2004 and B.Sc in Mathematics Yarmouk University-Jordan Very 2000.

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 of 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.

Ashraf A. Tahat is an Associate Professor in the Department of Communications Engineering at Princess Sumaya University for Technology (PSUT) and the Vice-Chairman of IEEE Jordan Section. Dr. Tahat earned his B.Sc. and M.Sc. degrees in Electrical Engineering from the Illinois Institute of Technology (IllinoisTech), Chicago, USA, where he also received a Ph.D. in 2002, with a focus on communications and signal processing. Dr. Tahat joined PSUT in 2005 and served as the Head of the department of Communications Eng. from 2010 to 2012. He was also a Visiting Professor with McGill University, Montreal, Canada, in the Department of ECE, conducting research on modern communications systems (2012-2013). From 2002 to 2003, he was an Adjunct Professor at IllinoisTech, Chicago, USA.

Raft Abdelrahim is an assistant professor in mathematics department in the college of arts and sciences in Jouf University since 2016 until present. He got his phd in mathematics from University Utara (UUM) in 2016. The PhD dissertation is about Numerical solution of Ordinary Differential Equations on number Numerical Analysis. He also holds a M.Sc degree in Mathematics from Jordan University of Science and Technology, 2009 and B.Sc in Mathematics Al al-bayt University-Jordan Very 2005

Eddie Shahril Ismail received his BSc and MSc in Mathematics from the Universiti Kebangsaan Malaysia (UKM) in 1998 and 1999 respectively, and completed his PhD in Cryptography from the Universiti Sains Malaysia (USM) in 2004. He is an Associate Professor at the School of Mathematical Sciences, UKM. His main research interests are cryptology and number theory. He has authored and co-authored more than 30 articles in international journals, conference proceedings and books. He has published his works which deal with the design of new cryptographic algorithms and protocols. He is a life member of the Malaysian Mathematical Sciences Society.

© 2020 NSP
Natural Sciences Publishing Cor.