# Secure Identity-based Online/Offline Signature System

**Zinah S. Jabbar, Sattar J. Aboud**

***Abstract***: ***The article introduces an identity-based online/offline signature system for wireless sensor network (WSN). The authors claim that when the computation cost is low, the proposed system is more suitable for WSN. The authors also claim that their scheme provides multi-level use from offline information allowing the signer to reuse this before the calculated data within a limited time, unlike those used in the existing online/offline signature systems. The introduced system gave a promising outcome when used with a MICAz platform. MICAz platform is the mote 2.4HGz module wireless measurement system used for low-power WSN.***

***Keywords*: *identity-based signature, wireless sensor network, distributed sensors, Base Station.in alphabetical order, separated by commas.***

## I. INTRODUCTION

The WSN defined as a group of distributed sensors to see and gather the physical environment information and then regulate this information gathered to keep it at the center. The WSN determines the circumferential variables such as temperature, humidity, wind, and others. The WSN can be as an observer in a certain hazardous environment, such as nuclear energy stations. It is used in many parts of the world for observing some ecological conditions, without the need to update its own energy supply. The WSN is vulnerable to various attacks because of the wireless connection environment. When applying WSN, the validation of the sensor data must first be provided because it is of great importance. For example, sensors gather data concerning the radiation degree of nuclear energy and send this data to the Base Station (BS) to identify its capacity [1]. It must also check that the collected data is unchanged when it is sent for processing to avoid any risks related to regarding the employees. For example, in the medical service applications, the data regarding patient cases are sent from sensors to BS. However, because sensors typically contain limited resources such as storage and power, a WSN is a challenge to network security because it requires low power and an efficient encryption algorithm.

Identity-based encryption is modern encryption. It is a public key encryption type where the public key of the user is unique to the user's identity, such as his or her e-mail address. This means that the sender can access public keys to encrypt a message using the recipient's e-mail address as a key. The recipient receives the decryption key from the trusted reference that it creates. Identity-based encryption was introduced by Shamir in 1984 [2]. His signature system can provide an identity-based signature. The advantage of the Shamir system is eliminating the need to validate the certificate. However, a digital signature based on identity requires two basic elements: the message, and the signature. The program can then be implemented immediately. However, identity-based encryption remains an unresolved problem for more than a decade.

## II. RELATED WORKS

In 2001, Shamir-Tauman proposed an online/offline signature system [3], which is more efficient than other systems. But, it is not effective. However, another system was described in 2007 by Chen *et al*. They proved that their system was at risk in standard cryptography, but showed that their system was better than other systems [4]. In 2006, Xu *et al*. proposed the first online/offline signature system using identity [5]. Their system requires the signer to perform an offline phase if it wants to re-create the signature phase. In this system, the offline signature is used only once, and cannot be used again. However, if such a system is implemented in the wireless sensor network, the system becomes impractical as the offline phase is executed in BS. Inability shortcoming shows that the sensor requires that you return to the BS each time to get the next offline signature. In addition, validation of the Xu *et al*. system requires a binding process, so this method is an expensive method which results in an insufficient signature system to connect data transfer from a node to the next node in the WSN. However, in 2008, Li *et al*. reported that Xu *et al*. system was non-functional [6] because it did not achieve the goal of its construction and increased the cost of running the interaction. In a separate work, Li *et al*. proposed an online/offline identity-based signature system. This system allows the signer to reuse previously calculated data offline in polynomial time. However, Kar [7] proved that Li *et al*. system does not include any case in which the signer randomly chooses the string. Here, the system requires another system to detect malicious attacks.

However, in 2016, Gao, *et al*. [8] proposed an identity-based online/offline signature system using bilinear maps. They claimed that their system had been proved, by the tough Diffie-Hellman system, against impersonation under the adaptive chosen-plaintext attack. No one has yet shown that this system is safe. Also, Bo Sang in 2017 [9] introduced an identity-based system and a signature system of code-based assumptions against forgery inactive and concurrent attacks. In this article, the authors proposed a secure system by investigating which of the signatures was

**Revised Manuscript Received on October 05, 2019**
***** Correspondence Author
**Sattar J. Aboud**, Information Technology College, Imam Ja'afar Al-Sadiq University, Baghdad-Iraq, sattar_aboud@yahoo.com
**Zinah S. Jabbar**, Information Technology College, Imam Ja'afar Al-Sadiq University, Baghdad-Iraq, sattarzeina@gmail.com

forged, and the authors explained how to falsify the signature system later on. In 2019, Pani Nisha and Vahitha Thangam [10] proposed two data Transmission (SET) protocols for cluster based wireless sensor networks, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain; no one has yet shown that this system is secure.

The rest of this article is organized as follows. In Section 3, the proposed system is described. In Section 4, the security evidence is presented with an analysis of achievements. Implementing the proposed system is presented in Section 5. Finally, the conclusion is provided in Section 6.

## III. THE PROPOSED METHODOLOGY

The proposed methodology is based on the difficulty of discrete logarithm assumptions. Assume that the group $G$ of prime $ord(n)$ , and a primitive element $a$ with an integer $a^d$ of $G$ so that $d$ be chosen randomly of $Z_n^*$. Thus, it can declare that a problem of the discrete logarithm $(P,t)$ is carried in $G$ when there is no algorithm operating with $t$ time such that $t$ is able to decrypt a discrete logarithm at $G$ for probability $P$ . The proposed methodology comprises the following algorithms:

**Setup algorithm**: Assume that $G$ is the cyclic group whose order is a prime number $n$ that means $ord(n)$ . Then, the trusted authority should do the following:

1. Choose an integer generator $a \in G$ ;
2. Select an integer number $d \in Z_n^*$;
3. Compute $k := a^d \bmod n$ ;
4. Assume that $h_1 : \{0,1\} \to Z_n^*$ is a secure hash function;
5. Determine the public keys as $pk = (G, n, a, k, h_1)$ ;
6. Determine the master key as $mk = d$ ;

**Extract algorithm**: In this algorithm, the trusted authority needs to create the secret key to the user identity $id$ . So, it should do the following:

1. Choose an integer $l \in Z_n^*$ ;
2. Find $x := a^l \bmod n$ ;
3. Find $f := l + h_1(x, id)d \bmod n$ ;
4. Determine a secret key of the user by $(x, f)$ ;
5. The user secret key must satisfy the equation of

$$a^f = xk^{h_1(x,id)} \bmod n; \qquad (1)$$

**Offline-Sign algorithm**: in this algorithm, a signer should do the following:

1. Find $c_j := a^{2^i} \bmod n$ ; // *for* $j = 0,...,|n|-1$

**Online-Sign algorithm**: In this algorithm, a signer should do the following:

1. Choose an integer $r \in Z_n^*$;
2. Assume that $r[j]$ is the $j-th$ bit of $r$ ;
3. Select $\ell \subset \{1,...,|n|\}$ is a set of indices where $r[1] = 1$ ;
4. Find $g := \prod_{j \in \ell} c_{j=1}$ ;
5. Compute $h := h_1(g, x, m)$ ;
6. Find $i := r + h \cdot f \bmod n$ ;
7. Determine the signature as $(g, x, i)$ ;

**Verify algorithm**: In this algorithm, the signature $(g, x, i)$ for plaintext $m$ and user identity $id$ , is verified by the verifier. For verification, we should do the following:

1. Find $h := (h_1(g, x, m)$ ;
2. Ensure that if $a^i \equiv gx^h k^{hh_1(x,id)}$ ; (2)
3. Accept when it is congruent, and refuse if it is not;

**Correctness**: observe that $g = a^r$ . It has

$$gx^h k^{hh_1(R,id)} = a^g g^{rh} a^{dhh_1(x,id)}$$
$$= a^{r||h(l||h_1(x,id)d)}$$
$$= a^{r||hf} = a^i$$

**Remarks**

The identity-based signature system is denoted as $IBS$ . Where $IBS$ = (Setup, Extract, Sign, Verify) is secure under 'chosen-plaintext attack' when there is no polynomial-time and the attacker $A$ has the non-trivial advantage in the following scenarios between the attacker $A$ and the challenger $C$ .

**Firstly**, the challenger $C$ runs the Setup algorithm to create the system keys and passes them to the attacker $A$ .

**Secondly**, the attacker $A$ performs the following queries::

1. Once the attacker $A$ requests the private key $xk$ of an identity $id$ , a challenger $C$ runs the Extract algorithm to get the identity $id$ of the corresponding private key $xk_{id}$ and sends it to the attacker $A$ .
2. Once the attacker $A$ requests the offline signature on the identity $id$ , in order to get the corresponding private key $xk_{id}$ , the challenger $C$ runs the offline-Sign algorithm providing the private key $xk_{id}$ then gets the signature $s$ and sends it to the attacker $A$ .
3. Once the attacker $A$ requests the online signature on the plaintext $m$ to the identity $id$ , the challenger $C$ runs the online signature system then gets the signature $s$ and sends it to the attacker $A$ .

**Thirdly**, after the queries described above, the attacker $A$ issues the signature $(id', m', s')$ where $id'$ is the corresponding identity and is required on the key extract queries, $m'$ is the plaintext and has not been issued in online signature queries, and $s'$ is the signing for plaintext $m'$ when the signature $s'$ is valid. If the attacker $A$ succeeds in probability in the above attack scenario, it means that the attacker $A$ is forged $(P, t, e, s, q)$ when it obtains an advantage at least probability $P$ in the above attack scenario, runs in time at most $t$ , then performs at most $(e, s, q)$ extract, signature and random oracle queries. However, the identity-based online/offline signature system $(P, t, e, s, q)$ is secure

when there is no $(P,t,e,s,q)$ -forger.

## IV. THE PROPOSED ALGORITHM

The section covers the result of security analysis and the result of probability analysis.

### A. Result of Security Analysis

A presented system is $(P,t,e,s,q)$ secure by means of an un-forgeable identity-based system under 'chosen plaintext attack' in the random oracle model. Suppose that $(P',t')$, a discrete logarithm problem has in $G$, such that:

$$P' = (1-(q(e+s))/n)\cdot(1-(1/n))\cdot(1/q)\cdot P$$

$$t' = t + O(e+s)\wedge$$

So $(e,s,q)$ is the extraction random of oracle values, signatures and hashing queries. Assume that the below scenario occurs between the challenger is $C$ and the attacker is $A$. Also, assume that challenger $C$ builds an algorithm to find a discrete logarithm to the base $a$ of $\partial$ in the group $G$ and the group $G$ is provided, a primitive element $a$ of the group, a prime $ord(n)$, and an integer $w$ of $G$. The challenger $C$ is requested to solve $\partial \in Z_n$ where $a^{\partial} = w \bmod n$.

**Setup**: the challenger $C$ does the following:

1. Select the secure hash function $h_1 : \{0,1\}^* \in Z_n$; // act similar to the random oracle.
2. Find $k := w$;
3. Send a public key $pk = (G,n,a,k,h_1)$ to the attacker $A$;

**Extract Oracle**: the attacker $A$ does the following:

1. Accept a query of a random oracle to the identity $id$;

Then, the challenger $C$ does simulate the random oracle as follows:

1. Select randomly $u,b \in Z_n$;
2. Find $x := k^u a^b \bmod n$;
3. Find $f := b$;
4. Find $h_1(x,id) := -u$;
5. Issue $(x, f)$ as a secret key to the identity $id$
6. Keep the parameters $(x, f, h_1(x,id), id)$ in the table for uniformity;

**Sign-Oracle**: the attacker $A$ does the following:

1. Enquire about a signature oracle to the plaintext $m$ with the identity $id$;

Then, the challenger $C$ does the following:

1. Verify if $id$ is queried to an extract oracle $h_1$;
   a. Restore $(x, f, h_1(x,id))$ of the table;
   b. Utilize such parameters to sign a plaintext $m$, consistent with a signature algorithm illustrated in the system;
   c. Issue a signature $(g,x,i)$ for the plaintext $m$;
   d. Keep the parameters of $h_1(g,x,m)$ in hash table for uniformity;
2. But, if identity $id$ is not queried for a random oracle $h_1$;
   a. Perform the random oracle simulation;
   b. Utilize a related private key for signature plaintext $m$;

**Result Computation**: In this stage, the scenario between the attacker $A$ and the challenger $C$ is as follows:

1. An attacker $A$ issues the rigged signature $s_1' = (g', x', i_1')$ of plaintext $m'$ and identity $id'$;
2. The challenger $C$ returns the attacker $A$ to the step at which it queries $h_1(g', x', m')$ provided by the different output;
3. The attacker $A$ issues a new pair of signatures $s_2' = (g', x', i_2')$;
4. The challenger $C$ issues another pair of signatures to get $s_3' = (g', x', i_3')$;
5. Suppose that $y_1, y_2, y_3$ are the results from extraction of oracle queries $h_1(g', x', m')$ to the three rounds shown above;
6. Select $l, d, r \in Z_n$;
7. Find $a^l := x \bmod n$;
8. Find $a^d := k \bmod n$;
9. Find $a^r := g \bmod n$; // indicate discrete logarithms for $(x, k, g)$.
10. Compute $i_j' := r \| ly_j \| dy_j h_1(x', id) \bmod n$ using formula (2);//for $j := 1,2,...$
11. The challenger $C$ resolves the three linear formulas described above;

### B. Result of Probability Analysis

A random oracle simulation process is unsuccessful when an oracle task $h_1(x,id)$ produces the collision. This is highly probable at most $q/n$. So, a simulation wins $(e \| s)$ times where $h_1(x,id)$ can also be queried in the oracle signature when the identity $id$ is not queried in the oracle extraction in the probability at least $1-(q(e \| s))/n < (1-(q/n))^{e\|s}$. Because of randomization of the random oracle model, there is a query $h_1(g', x', m')$ with probability of at least $1-1/n$. Challenger $C$ solves these properly as a return point, by at least $1/q$ probability. So a winning probability is $(1-(q(e \| s)/n)(1-(1/n)(1/q)P$. Where, an algorithm computing cost is controlled through exponent that is done in the extraction and signature queries, which reaches $(t \| O(e \| s)\wedge)$.

### C. Result of Efficiency Analysis

By comparing the proposed signature system to other identity-based online/offline signature systems, such as the

Gao, *et al*, identity-based signature system [8], we find that these systems are not able to cover the multi-time form. The Bo Song signature system [9] does not give the multi-time form to online/offline signature. Suppose that $t(o)$ refers to the computing time of operation $o$, and by $|\beta|$ the bits of $\beta$. Suppose also that $\wedge$ indicates the exponent in $G$, $M$ the multiplication in $G$, $\tilde{m}$ the standard multiplication in $Z_n^*$ and $p$ the pairing operation. Table (1) displays a comparison of computing time result, $h$ denotes the hash operation, this needs however one $\wedge$ calculation, $s_a$ and $s_v$ signify the standard signature creation and verification. This needs one $\wedge$ calculation per operation. Also, $cert_v$ signifies the certificate verification; this also needs one $\wedge$ calculation. Also, table (1) displays a storage space in addition to signature length. For example, $|n|$ and $|G|$ need 160 bits. Where $|s|$ indicates the size of the standard signature, this needs 160 bits. Where, $|cert|$ denotes a size of the identity certificate, this needs also 320 bits. Table (1) shows the proposed system with a better performance in comparison to Gao, *et al* system. But, in comparison to a Bo Song system, there is around 40% boost when we focus on signature checking.

**Table- I: computing time, storage space, and signature length**

| Scheme | Gao, *et al* Scheme | Bo Song Scheme | Proposed Scheme |
|---|---|---|---|
| Offline (one-time) | $t(h) \| t(s_a)$ | $2\wedge \| \tilde{m}$ | 0 |
| Offline (multi-time) | – | $\|n\| \cdot 2\wedge$ | 0 |
| Online (one-time) | $\tilde{m}$ | $\tilde{m}$ | $\tilde{m}$ |
| Online (multi-time) | – | $O(\|n\|) \cdot 2M \| i$ | $O(\|n\|) \cdot M \| i$ |
| Verification | $t(h) \| t(s_v) \| t(cert_v)$ | $p \| 2\wedge \| M$ | $2\wedge \| M$ |
| Offline storage (one-time) | $2\|n\|+\|s\|+\|cert\|$ $\geq 640$ *bits* | $2\|G\|+2\|n\| \approx 5$ *bits* | $\|G\|+\|n\| \approx 32$ *bits* |
| Offline storage (Multi-time) | – | $2\|n\| \cdot \|G\| \approx 6.$ | $\|n\| \cdot \|G\|$ $\approx 3.2$*kbytes* |
| Size of Signature | $\|n\|+\|s\|+\|cert\|$ $\geq 640$ *bits* | $2\|G\|+\|n\| \approx 4$ *bits* | $\|G\|+\|n\| \approx 48$ *bits* |

## V. THE RESULT ANALYSIS

This section discusses the implementation of the WSN, which is as follows:

### A. Set up

The sensor node utilized in the application is *MICAz*, established via Crossbow Technology with a microcontroller of $8-bits$. Authors employed a laptop ( *HP* with $i7-4500U$ *CPU*@1.8*GHz* 2.40,8*GB* *RAM* ) as the BS. The language used is Python. To apply the system in sensor node, we used the public key encryption. A packet information presentation in the application is divided into two parts. The aim behind dividing a signature into two phases rather than one is that the $x$ portion of the signature will be the same to all signatures created of the sensor node; thus, it provides public connections through the transmission $x$ at the start of connections. The standard phase packet to one phase is 984 bits versus packet with two phases that are 664 bits and 320 bits of saved connections to every signature. In the Setup phase, every packet is 344 bits, namely 24 bits to the header, 320 bits to signature, 160 bits to $x.d^*$, 160 bits to $x.r^*$; the remainder is a zero fill. In the standard phase, the length of every packet is 664 bits, namely 24 bytes to the header, 480 bits to signature, 160 Bit to $g.d^*$, 160 bits to $g.r^*$, 160 bits to $i$, and 160 bits to net load.

### B. Result of Energy Measurement

A power $E$ is determined by $E = p \cdot t$ so that $p$ indicates energy where $t$ indicates time. A unit $E$ is Joule and $p = V \cdot I$ so $V$ indicates the voltage measured across the conductor in units of volts where $I$ represents the current through the conductor in units of amperes. Note that $p$ is Watt. Furthermore, note that under Ohm Law, $I = V / x$ such that $x$ is the impedance of the conductor in units of Ohm. Real power is spent if the operation on the codes in *MICAz* is not computed with dependence on inner resistance. However, no track is left for rating the resistance of logic gates. Thus, we gauge the power consumption of *MICAz* in one way or another. A circuit is run via two rechargeable batteries of Panasonic *AA* 2000 *NiMH*. The aim to add the $x_1$ resistor to the circuit rather than simply linking it to measure the current in a circuit chain since it needs to catch voltage differences in circuit and in the time of modifications all at once. Through such arrangement, it is capable to gauge the voltage flow to *MICAz* rather than directly through gauging a voltage reduction, $Vx_1$ in the in the $x_1$ resistor employing *HP* digital oscilloscope. Select the trivial value resistor to reduce extra impedance for a circuit. Once the voltage data is obtained, we gauge an entire low current via *MICAz*, *VM* and employing Fluke 87*V* digital Multi-meter coupled corresponding to *MICAz*. It is now capable of computing the total circuit energy. To obtain power consumption, it needs a measuring data. The authors set up *MICAz* to sign and check the signature regularly. The oscilloscope is capable of catching the calculation time because a current over $x_1$ and $Vx_1$ can be modified over *MICAz* through the calculation of the proposed online/offline identity-based signature system. The real energy consumption is presented in Table 2.

Table (2) shows the result of power consumption and time consumption of the proposed system if the $160-bits$ random message is signed and checked utilizing the online/offline identity-based signature system. Note that there are two issues for signature verification if a signature is checked through the BS and *MICAz* sensor node.

**Table- II: Power and time of the proposed system**

| Operation | Power | Time |
|---|---|---|
| Signature (offline BS) | zero | 0.289 |
| Signature (online *MICAz* ) | 11.29 | 0.672 |
| Verification (BS) | zero | 0.014 |
| Verification ( *MICAz* ) | 64.13 | 3.140 |

## VI. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. The authors proposed an effective online/offline identity-based signature system that is not needed some certificate accompanying with the signature to check. Also, this not needs the pairing process in signature creation and verification of the signature. Also, the offline signature will not need any private key. It is calculated in advance via the trusted authority. The offline data could be used again. That is an important benefit of the WNS, where offline data could be strongly encrypted in the sensor node when creation. This will remove the message among BS and sensor node to an offline signature that is measured as an expensive factor in the WSN. These predefined offline data are around 160 group items. It might be measured a long time to sign some messages. But, when a sensor needs for signature the hundreds messages, the 160 group items are trivial if compared with these messages. The proposed system is therefore appropriate to the great scale network.

## ACKNOWLEDGMENT

It is optional. The preferred spelling of the word “The Authors wish to extend their thanks to the University of Imam Ja’afar Al-Sadiq, at Baghdad-Iraq, Faculty of Information Technology for their help suggestions and their financial support.

## REFERENCES

1 Sattar J. Aboud, Secure online-offline Identity-Typed Signature Scheme, International Journal of Scientific Research and Management Studies (IJSRMS) Volume 1, Issue 9, 2015.
2 Shamir A., Identity-based cryptosystems and signature schemes, In Proc. CRYPTO ’84, volume 196 of Lecture Notes in Computer Science, pp. 47–53, Springer-Verlag, 1984.
3 Shamir A., Tauman Y., Improved online/offline signature schemes. In Proc. CRYPTO ’01, volume 2139 of Lecture Notes in Computer Science, pp. 355–367, Springer-Verlag, 2001.
4 Chen X., Zhang F., Susilo W., Mu Y., Efficient generic online/offline signatures without key exposure, In Proc. ACNS ’07, volume 4521 of Lecture Notes in Computer Science, pp. 18–30, Springer-Verlag, 2007.
5 Xu S., Mu Y., Susilo W., Online/offline signatures and multi-signatures for AVOD and DSR routing security. In Proc. ACISP ’06, volume 4058 of Lecture Notes in Computer Science, pp. 99–110, Springer-Verlag, 2006.
6 Li F., Shirase M., Takagi T., on the security of online/offline signatures and multi-signatures from acisp’06, In Proc. CANS ’08, volume 5339 of Lecture Notes in Computer Science, pp. 108–119, Springer-Verlag, 2008.
7 Kar J., Provably secure online/off-line identity-based signature scheme for wireless sensor network, International Journal of Network Security, vol. 16, no. 1, pp. 29–39, 2014.
8 Gao Y., Peng Zeng, Choo K., Song F., An improved online/offline identity-based signature scheme for WSNs, International Journal of Network Security, volume 18, No. 6, pp. 1143-1151, 2016,
9 Bo Song, Provably secure identity-based identification and signature schemes from code assumptions, PloS One, 12(8), 2017;
10 M. Pani Nisha & R.Vahitha Thangam, Secure and Efficient data Transmission in Cluster Based Wireless Sensor Network Using Set-Ibs and set-Iboos Protocol, *International Journal of Engineering Sciences & Research Technology*, March 2019.

## AUTHORS PROFILE

**Zinah S. Jabbar** is a lecturer in Information Technology College, University of Imam Ja’afar Al-Sadiq, Baghdad-Iraq. **Zinah** specializes in Databases, Information Security and Cryptography and she holds a first-class BSc in Computer Science, and MSc in Databases. **Zinah** currently is a Lecturer and conduct her research at the Information Technology College, University of Imam Ja’afar Al-Sadiq. **Zinah** has delivered a range of hand-on technical training on topics such as Database Security as part of a proactive approach to protect computer systems. She has many years of experience with the University of Imam Ja’afar Al-Sadiq. Also, she has leading IT training courses in Lab. Earlier in her career; she was a lecturer at the School of Computer Science and Technology, Al Rafidain University College. She has published numerous professional and peer-reviewed articles. Her research interests include Databases Security, Applied Cryptography Schemes and Security for Cyber-Physical Systems. Additionally, **Zinah** is interested in multidisciplinary projects to mitigate cyber-related challenges such as online anti-social behavior. By the end of 2019, **Zinah** has supervised 20 BSc final year projects to successful completion

**Sattar J. Aboud** is a full professor in Information Technology College, University of Imam Ja’afar Al-Sadiq, at Baghdad-Iraq. Sattar specializes in Information Security and Applied Cryptography and holds a first-class Postgraduate Diploma in Computing Science, and PhD in Computing Systems, both degrees from Glasgow University, UK. Sattar is a full professor and conduct his research at the Faculty of Information Technology; University of Imam Ja’afar Al-Sadiq, Baghdad-Iraq. Sattar has delivered a range of hand-on technical training on topics such as Encryption Schemes, Digital Signature Schemes, Authentication and Identification Protocols, Algorithms Analysis and Design, Information Security Management, Network Security, Cyber security including Ethical Hacking as part of a proactive approach to protect computer systems. He has more than 30 years of experience with Transnational Education as a Link-coordinator of franchised courses and a flying faculty team, supported MSc and PhD programs at many Universities, as well as delivering Executive Master's degrees in Cyber security through leading IT training providers in the UK such as QA Ltd. He has published more than 150 professional and peer-reviewed articles. His research interests include Asymmetric Encryption, Digital Signatures, User Authentication Methods, Cyber Security and Security for Cyber-Physical Systems. Additionally, Sattar is interested in multidisciplinary PhD and MSc projects to mitigate security-related challenges such as Authentication Protocols. By the end of 2018, Sattar has supervised and exam more than 150 PhD and MSc dissertations to successful completion. His interest in a broad range of collaborative activities has led to work with national and international researchers to publish in leading journals and to write proposals addressing funding calls, in total he has assisted in the generation of over $3m. Within his area of expertise, he has also worked with new businesses, to launch new products, and authored 6 chapters in books by the end of 2017. His quality work has attracted various awards, recent recognitions include a Best Conference Paper Award in 2016, nomination by University of Bedfordshire, and to a Student Led Teaching Award in 2003 by the University of Philadelphia. When Sattar has free time, he enjoys reading, walking, and travelling.