An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model

Mohammed Hassouna[1], Nashwa Mohamed[2], Bazara Barry[2] and Eihab Bashier[2, 3]

[1] Faculty of Computer Studies, National Ribat University,

P.O.Box 55, Khartoum, Sudan

[2] Faculty of Mathematical Sciences, University of Khartoum,

P.O.Box 321, Khartoum, Sudan

[3] Faculty of Sciences and Arts, University of Albaha,

P.O.Box 1988, Baljurashi, Albaha, Saudi Arabia

Abstract

Most of the existing mailing systems provide limited authentication mechanisms, including web trust model, password authentication or identity based cryptography. Few existing mailing systems found in the literature provide strong authentication based on public key infrastructure (PKI). However, PKI based-systems generally suffer from certificate management and scalability problems.

This paper proposes a mailing system that is based on certificeteless cryptography. In the proposed mailing system the message payload is encrypted by a per-mail symmetric key generated from a secret value, the public and private keys of the sender and the receiver at each side. The proposed mailing system is secure against standard security model and provides many security properties.

Keywords: *Authentication, Certificateless cryptography, Mailing systems, Security model.*

1. Introduction

Electronic mail or e-mail is a method by which a digital message is delivered from a sender to one or more recipients. The history of electronic mail started at the Massachusetts Institute of Technology (MIT) in 1965 under the name MailBox, with the aim of sending files from one computer to another. A major breakthrough was witnessed in the year 1971 with the appearance of a real email system, when Ray Tomilson who worked for the department of defence (DoD) sent his first ARPANET email message to himself [11].

Some early email systems required that the sender and the recipient both be online at the same time, in accordance with instant messaging. The modern email systems operate across the Internet or other computer networks to enable the users to send and access email messages using standard protocols. These protocols include the Simple Mail Transfer Protocol (SMTP), the Internet Mail Access Protocol (IMAP) and the Post Office Protocol (POP). The Simple Mail Transfer Protocol (SMTP) and its extensions are used to ensure reliability and efficiency of message transport. Internet Mail Access Protocol (IMAP) and Post Office Protocol (POP) are used to enable the recipients to access their email messages at the mail servers. Services introduced by mail servers include accept, forward, deliver and store messages, and neither the senders nor the recipients are required to be online simultaneously in such setting.

The users of any email system need a software interface to interact with the mail server to allow them to read, compose, send, and store email messages, and that software interface is called mail client and can be desktop application like MS Outlook, Mozilla Thunderbird or web-based application (also known as webmail) like Gmail, Hotmail and Roundcube.

Nowadays, emails have become official communication with the ability to attach sensitive documents to them. Therefore, the four basic security services, namely, authentication, confidentiality, integrity and non-repudiation are indeed necessary requirements that have to

be satisfied for email systems. Cryptographic protocols and solutions are used to insure these security services. However, such solutions suffer from limitations that hinder wide acceptance and adoption.

For example, systems that use symmetric and asymmetric cryptography may suffer from key management problems. Moreover, identity-based encryption, which has been proposed to address the key management problem, suffers from the key escrow problem which violates the non-repudiation service that should be offered by secure systems.

This paper proposes the use of certificateless cryptography as alternative technology for email security to eliminate the key management problem in Public Key Cryptography (PKI) based mailing systems and the key escrow problem in identity based mailing systems.

The proposed secure mailing system makes use of the certificateless public key cryptography scheme proposed by Al-Riyami and Paterson [1] in 2003. In the proposed scheme, the sender downloads the public key of the receiver from a public directory, then he/she generates a random positive integer *t* and uses it to compute a per-mail symmetric key and encrypts the message by this secret key. Then, he/she encrypts *t* using the receiver's public key, attaches the encrypted *t* to the encrypted message, signs the message and sends it to the receiver. On the other side, the receiver verifies the signature, decrypts the encrypted *t* using his/her private key, downloads the public key of the sender from the public directory, computes the per mail key and decrypts the encrypted email.

The rest of this paper is organized as follows. Section 2 provides backgrounds and basic concepts of email systems and their protocols. Existing systems to secure email messages and introduction of ceritificateless cryptography are provided as well. Section 3 describes the proposed secure mail system based on certificate-less cryptography and its security features. Finally, in Section 4 conclusions and remarks are given.

2. Literature Review

In this section, an explanation on how electronic mailing systems work is provided. The explanation is largely based on parts from [14].

2.1 Email System: Components and Protocols

At the most basic level, the two primary message sections are the header and the body. The header section contains the vital information about the message including origination date, sender, recipient(s), delivery path, subject, and format information. The body of the message contains the actual content of the message.

The process starts with message composition. The most basic mail clients typically ask the user to provide the following: subject line, message content, and intended recipients. When these fields are completed and the user sends the message, the message is transformed into a specific standard format specified by Request for Comments document (RFC) 2822 [13] on Internet Message Format.

Once the message is translated into an RFC 2822 compliant message, it can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. After initiating communication, the mail client provides the sender's identity to the server. Next, using the mail server commands, the client tells the server who the intended recipients are. Although the message contains a list of intended recipients, the mail server does not examine the message for this information. Only after the complete recipient list is sent to the server does the client supply the message. From this point, message delivery is under control of the mail server.

Once the mail server is processing the message, several events occur, namely, recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client. At this point, one of two events could occur. If the sender's and recipient's mailboxes are located on the same mail server, the message is delivered using a local delivery agent (LDA). If the sender's and recipient's mailboxes are located on different mail servers, the send process is repeated from one MTA to another until the message reaches the recipient's mailbox, when the LDA has control of the message, a number of possible events may occur. Depending on the configuration, the LDA could deliver the message or process the message based on a

predefined message filter before delivery. Once the message is delivered, it is placed in the recipient's mailbox where it is stored until the recipient performs some action on it (e.g., read, delete) using the MUA. Figure 1 illustrates the flow of the message through the various mail components discussed previously

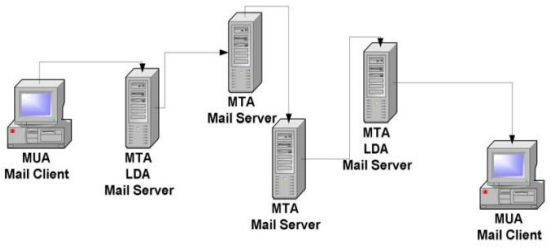

Fig. 1 The flow of the message through the various mail components. Source [14]

The essential transport protocols are Simple Mail Transport Protocol (SMTP) and its extension ESMTP which are explained in RFC 821 [12] and RFC 2821 [7] respectively. These protocols are basically responsible for transferring the email from one MUA to MTA or from MTA to MTA. SMTP was developed to ensure a more reliable and efficient way to transport messages. As the number of email users grew, additional functionality was sought in mail clients and SMTP servers. For SMTP servers to support this additional functionality, extensions were added to SMTP to produce ESMTP protocol.

Once a message is delivered by the LDA, users need to access the mail server to retrieve the message. Mail clients (MUAs) are used to access the mail server and retrieve email messages. Several methods exist for users to access their mail- boxes, the simplest being direct access. Post Office Protocol Version 3 (POP3) and Internet Message Access Protocol Version 4 (IMAP4), which are explained in RFCs 2449 [5], 3501 [2], 4466 [9], and 6237 [8], are two standard protocols that are used to directly access the user's mailbox.

Web-based mail applications, also known as Webmail applications, are increasingly being used as a means of email service delivery, because Web browsers that enable access to the client are available on nearly every Internet-enabled device. A user simply runs a Web browser and connects to a Web site that hosts the Web-based mail application. Webmail applications incorporate much of the mail-handling functionality of traditional mail clients and communicate with their associated mail servers using the same mailbox access protocols (SMTP, POP, and IMAP). The mailbox access protocols are used between the Web servers and mail servers only, and are not carried between the Web servers and Web browsers.

2.2 Existing Schemes to Secure Email Systems

Nowadays, emails have become official communication technology and sensitive documents can be attached to them. Therefore, it is necessary to provide the four basic security services, namely, authentication, confidentiality, integrity and non-repudiation by email systems to insure security and privacy. Most of the existing mailing systems enable users to access their emails with usernames and passwords, which is called password authentication method (i. e., something you know mechanism).

One possibility to securely transfer an email message is to cryptographically protect it in a way that is useful only for the intended recipients. A common software package that offers such cryptographic protection is the Pretty Good Privacy (PGP) [4] which provides confidentiality, authentication, email compatibility, compression and segmentation of email messages. PGP uses a symmetric algorithm for encryption and an asymmetric algorithm for key exchange. Public keys are posted in a public directory, and the overhead of key management is left for users. The hushmail is an example of a web-based email system which offers PGP email encryption.

Another approach which was developed by an industry working group is Secure Multipurpose Internet Mail Extensions (S/MIME), which was designed to add security to email messages that make use of the MIME message formats. MIME is an extension to the RFC 822 [3] framework that is intended to address some of the problems and limitations of the use of SMTP for electronic mail.

S/MIME works in a manner similar to PGP but it uses Public Key Infrastructure (PKI) for key management. However, both PGP and S/MIME suffer from the key management problem. To secure the path between the user's web-browser and web-server, some web-mail systems such as Gmail and Yahoo use SSL/TLS protocols and a PKI system to manage the servers certificates.

To address the key management problem some email cryptography systems that are based on Identity-based Encryption (IBE) have been proposed in the literature. Examples of such systems are Voltage email security system developed by Voltage Security Inc., the FortiMail

developed by Fortinet company and the MessageGuard. In identity based email systems email encryption is an easy process in which user's email addresses represent users public keys and the private keys are generated for users by centric trusted third party known as Private Key Generator (PKG). Then, private keys are transmitted to users on a secure channel after authentication process.

It is known that Identity-based Encryption (IBE) schemes suffer from the key escrow problem which refers to the PKG having the private keys of all system users. Such a scheme allows the PKG to decrypt any message in the system in violation of non-repudiation service that should be offered by secure systems.

Comparisons between many secure mail technologies including the X.509/PKI, PGP, IBE and ZMAIL were carried out in [6].

As shown previously, the main challenges of almost all the existing technologies to secure the e-mail system are the key authentication and management problems. Therefore, a robust model for key authentication and management that enhances the scalability and security of the mail system is needed.

This paper proposes the use of certificateless cryptography as alternative technology for email security to eliminate the key management problem in PKI-based mailing systems and the key escrow problem in identity based mailing systems.

2.3 Certificateless Public Key Cryptography (CL-PKC)

In 2003 Al-Riyami and Paterson [1] introduced the concept of Certificateless Public Key Cryptography (CL-PKC) to overcome the key escrow limitation of the identity-based cryptography. In CL-PKC a trusted third party called Key Generation Center (KGC) supplies a user with partial private key. The user then combines the partial private key with a secret value that is unknown to the KGC to obtain his/her full private key. This way the KGC does not know users private keys. Then, the user combines the same secret value with the KGC's public parameters to compute his/her public key.

Compared to identity based public key cryptography (ID-PKC), the trust assumptions made about the trusted third party in CL-PKC are much reduced. In ID-PKC, users must trust the private key generator (PKG) not to abuse its knowledge of private keys in performing passive attacks, whereas in CL-PKC, users need only trust the KGC not to actively propagate false public keys [1].

In CL-PKC users can generate more than one pair of private and public keys for the same partial private key. To guarantee that KGC does not replace user's public keys, Al-Riyami and Paterson [1] introduced a binding technique to bind a user's public key with his/her private key. In their binding scheme, the user first fixes his/her secret value and generates his/her public key and supplies the KGC with the public key. Then the KGC redefines the identity of the user to be the user's identity concatenated with his/her public key. By this binding scheme the KGC replacement of a public key of a user in the system is equivalent to certificate forgery by a CA in a traditional PKI.

3. Proposed Scheme

In this section, the proposed secure mail system that is based on certificateless cryptography is introduced. In the proposed mailing system, the CL-PKC that is proposed by Al-Riyami and Paterson [1] is used. Therefore, proper elaboration on Al-Riyami and Paterson scheme[1] is provided alongside the introduction of the proposed system and its security analysis.

3.1 Al-Riyami and Paterson Scheme

In this section, a general description of the algorithms Setup, Set-Secret-Value, Partial-Private-Key-Extract, Set-Private-Key and Set-Public-Key as introduced by Alriyami and Paterson [1] is provided.

Let k be a security parameter given to the Setup algorithm and IG be a Bilinear Diffie-Hellman Problem (BDH) parameter generator with input k.

1) Setup (performed by the KGC): this algorithm runs as follows:

a) Run Ω on input k to generate output $< G_1, G_2, e>$ where G_1 and G_2 are groups of some order q and

$$e : G_1 \times G_1 \rightarrow G_2$$

is a pairing.

b) Choose an arbitrary generator $P \epsilon G_1$.

c) Select a master-key s uniformly at random from Z^*_q and set $P_0 = sP$.

d) Choose cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow G_1^*$ and $H_2 : G_2 \rightarrow \{0,1\}^n$ where n is the bit-length of plaintexts taken from some message space $M=\{0,1\}^n$ with a corresponding ciphertext space $C = G_1 \times \{0,1\}^n$.

Then, the KGC publishes the system parameters

$$params = < G_1, G_2, e, n, P, P_0, H_1, H_2 >,$$

while the secret master-key s is saved securely by the KGC.

2) Set-Secret-Value (performed by the user):

This algorithm takes as inputs *params* and entity m's idntifier ID_m. Entity m selects $x_m \in Z^*_q$ at random and outputs x_m as m's secret value. Then, it computes $X_m = x_m P$ and sends X_m to the KGC.

3) Partial-Private-Key-Extract (performed by the KGC):

This algorithm takes as input an identifier $ID_m \in \{0,1\}^*$ and X_m, and carries out the following steps to construct the partial private key for client m with identifier ID_m.

a) Compute $Q_m = H_1(ID_m || X_m)$.

b) Output the partial private key $D_m = sQ_m \in G1$.

Entity m when armed with its partial private key D_m, it can verify the correctness of the partial private key D_m by checking $e(D_m, P) = e(Q_m, P_0)$.

4) Set-Private-Key (performed by the user):

This algorithm takes as inputs *params*, entity m's partial private key D_m and m's secret value $x_m \in Z^*_q$. Entity m transforms partial private key D_m to private key S_m by computing

$$S_m = x_m D_m = x_m s Q_m \in G_1.$$

5) Set-Public-Key (performed by the user):

This algorithm takes as inputs *params* and entity m's secrete value $x_m \in Z^*_q$ and constructs m's public key as $P_m = <X_m, Y_m >$, where $X_m = x_m P$ and $Y_m = x_m P_0 = x_m sP$.

3.2 Proposed Certificateless Mail System

In this section, the proposed certificateless mailing system algorithm is described. Fig 2 illustrates the proposed scheme.

Assume that client A wants to send secure mail message to the client B. Also, assume that the client A has a private key $S_A = x_A D_A$, and a public key $P_A = < X_A , Y_A >$ whereas client B has a private key $S_B = x_B D_B$, and a public key $P_B = < X_B , Y_B >$. Public keys of all clients are available in a public directory. The proposed certificateless email system works as follows:

1. Client A does the following:

(a) downloads the public key of client B from the public directory that could be maintained by The Lightweight Directory Access Protocol (LDAP), then checks that

$$\hat{e}(X_B, P_0) = \hat{e}(Y_B, P)$$

to authenticate the public key of client B.

(b) generates a random number $t \in Z^*$ and encrypts it using the public key of client B as $t^* = EP_B(t)$.

(c) computes $K_{AB} = tx_A X_B$, and then computes the per- mail symmetric key

$$K = H_2(Q_A || Q_B || KAB).$$

(d) encrypts the mail M using the symmetric key K as $M^* = E_K(M)$.

(e) adds the encrypted value t^* at the beginning of the encrypted mail M^* (i.e $M^* = M || t^*$).

(f) signs the encrypted mail M^* to produce the signature S using the client A's private key.

(g) adds the header and the signature to the encrypted mail, and then client's A mail client sends the encrypted mail to the mail server using SMTP.

2. Client B does the following:

(a) copies the encrypted mail from the mail server to client B mail client using the IMAP/POP3 protocols.

(b) downloads the public key of the client A from the public directory, then checks that

$\hat{e}(X_A , P_0) = \hat{e}(Y_A, P)$ to authenticate the public key of client A.

(c) verifies the signature.

(d) decrypts t^* using client A's public key

$$t = D_{PA}(t^*).$$

(e) computes $K_{BA} = tx_B X_A$, and then computes the per-mail symmetric key

$$K_B = H_2(Q_B||Q_A||K_{BA}).$$

(f) decrypts the encrypted mail M^* using the symmetric key K as

$$M = D_K(M^*).$$

*Note that $K_A = K_B$ since:

$$K_A = H_2(Q_A \| Q_B \| K_{AB}) = H_2(Q_A \| Q_B \| tx_A X_B)$$
$$= H_2(Q_B \| Q_A \| tx_A x_B P) = H_2(Q_B \| Q_A \| tx_B X_A)$$
$$= H_2(Q_B \| Q_A \| K_{BA}) = K_B$$

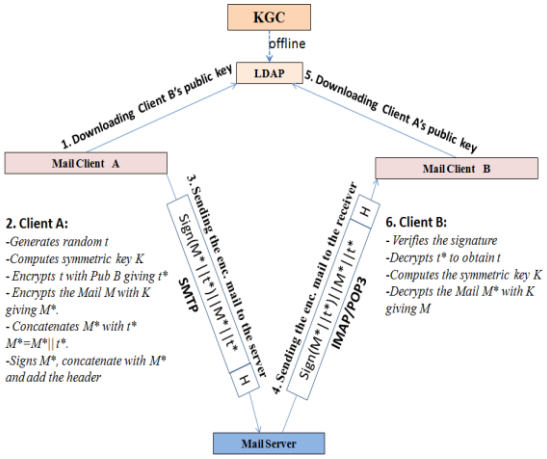

Fig. 2 The proposed scheme and its components

3. Security analysis

Since the proposed CTAKA protocol is based on the Elliptic Curve Discrete Logarithm (ECDLP) and Collision Resistant hash function standard cryptographic primitives, it is secure against standard security model. In this section, the cryptographic primitives and assumptions that the proposed protocol is based on are mentioned in addition to the security properties it provides. In the following, general definitions of negligible function and other related concepts are introduced.

Definition: We say that a real-valued function $\epsilon(k)$ is negligible in k, if for all $c > 0$, there exists $k_c > 0$, such that $k > k_c$ implies $\epsilon(k) < k_c$. A function that is not negligible is known as non-negligible.

Definition: Collision Resistant Hash Function Asumption A hash function $H \rightarrow H(k)$ is collision resistant if for all probabilistic polynomial time (PPT) algorithms A the advantage $Adv_A^{CR}(k) = Pr[H(x) = H(y) \wedge x \neq y \mid (x, y) \rightarrow A(1^k, H) \wedge H \rightarrow H(k)]$ is negligible as a function of the security parameter k.

Definition: Elliptic Curve Discrete Logarithm Problem (ECDLP) Assumption.

Given two points $P, Q \in E(F_q)$ on an elliptic curve, ECDLP determines the integer a, satisfying $Q = aP$, where P has order n, provided that such $k < n$ exists. So the advantage of any PPT algorithm A to find a given P, Q is negligible as function of security parameter k or $Adv_A^{ECDLP} = Pr[\text{find } a \text{ such that } Q = aP] \leq \epsilon$.

The proposed scheme also provides the following security properties.

1. End-to-End Authentication: the shared per-session secret key is generated using the client's secret values and the other client's public key and public parameters, and since the proposed mailing system uses the CLPKC with the binding technique, both clients can authenticate each other using pairing operation.

2. Key agreement without interaction: the most probable attack during a run of a key agreement protocol is the man-in-the-middle attack. The proposed mailing system enables both the sender and receiver to compute the shared secret key using their own secret values, the other party's public key and a randomly generated number which is encrypted by the receiver's private key without any interaction between the two parties. Therefore, the proposed protocol is secure against the man-in-the-middle attack.

3. Confidentiality: the mail payload is encrypted by a symmetric cryptosystem, which guarantees the confidentiality of the email.

4. Integrity and Non-repudiation: since the sender signs the message using his/her private key, the

integrity of the message can be verified, and the sender cannot deny sending the email.

5. Known key security: each session key is unique, because both the two communicating parties use the random number t which is generated by the sender and encrypted by the public key of the receiver in each protocol run. Thus the knowledge of previous session keys, if it exists, does not help an adversary to derive information about other session keys.

6. Known session-specific temporary information security: If the attacker or even the KGC has access to the ephemeral keys of a given protocol run(i. e., secret value t), they are unable to determine the corresponding session key sine there is no mathematical relation between the secret value t and the per-mail symmetric key (i. e., x_A/x_B still is missing).

7. Unknown key-share resilience: Since Q_A and Q_B are included in the hash function , the two parties know who they share the key with.

8. Key-compromise impersonation resilience: An adversary who has compromised the long-term private key of entity A is unable to compute the session key because Q_A , Q_B , D_A , x_A are also required in computing the session key. Thus, the adversary has no ability to impersonate entity B to establish a session key with entity A.

4. Conclusions

This paper proposed an end-to-end secure mailing system based on certificate-less public key cryptography. The sender obtains the public key of the receiver from a public directory at the KGC side. Then, the sender generates a random number, uses it together with his/her full private key and the public key of the receiver to generate a per mail secret symmetric key. Then the sender encrypts the mail payload with the symmetric key, encrypts the random number with the public key of the receiver, and concatenates the encrypted random number with the encrypted mail payload and signs them using the sender's private key, and sends the signed email to the receiver. On the other hand, the receiver verifies the signature, uses his/her private key to decrypt the random number, and uses it together with his/her full private key and the sender's public key to compute the secret symmetric key, by which the receiver decrypts the email.

Both the two communicating parties are able to compute the same secret symmetric key without message exchange. This makes it impossible to carry out a man-in-the-middle attack to obtain information about the encryption/decryption key, and hence, the mail contents. Moreover, the proposed mailing system provides authentication, confidentiality, integrity, non-repudiation, known key security, unknown key share resilience and Key-compromise impersonation resilience.

Also, the proposed mailing system is based on standard cryptographic primitives, which makes it secure against standard security model.

Acknowledgments

The authors of this paper are pleased to acknowledge the full funding of the University of Khartoum(http://www.uofk.edu), The National Ribat University(http://www.ribat.edu.sd) and the Nile Center for Technology Research (NCTR) (http://www.nctr.sd) to the research led to this paper.

References

[1] S. Al-Riyami and K. Paterson. Certificateless public key cryptography. In C. Laih, editor, Asiacrypt 2003, Lecture Notes in Computer Science, pages 452–473, 2003.
[2] M. Crispin. Internet message access protocol - version 4rev1, 2003. http://tools.ietf.org/html/rfc3501.txt.
[3] D. H. Crocker. Standard for the format of arpa internet text messages, 1982.
http://www.ietf.org/rfc/rfc0822.txt.
[4] M. Elkins, D. D. Torto, R. Levien, and T. Roessler. Mime security with openpgp, 2001.
http://www.ietf.org/rfc/rfc3156.txt.
[5] R. Gellens, C. Newman, and L. Lundblade. Pop3 extension mechanism, 1998. http://www.ietf.org/rfc/rfc2449.txt.
[6] E. Gerck. Secure Email Technologies X.509/PKI, PGP, IBE and ZMAIL: A us- ability and security comparison, pages 171–196. ICFAI University Press, 2007.
[7] J. Klensin. Simple mail transfer protocol, 2001. http://www.ietf.org/rfc/rfc2821.txt.
[8] B. Leiba and A. Melnikov. Imap4 multimailbox search extension, 2011. http://tools.ietf.org/html/rfc4466.
[9] A. Melnikov and C. Daboo. Collected extensions to imap4 abnf, 2006. http://tools.ietf.org/html/rfc4466.
[10] C. Partridge. The technical developmentof internet email. IEEE Annalsof the History of Computing, 30(2):3–29, 2008.
[11] J. B. Postel. Simple mail transfer protocol, 1982. http://www.rfc-editor.org/info/rfc821.
[12] P. Resnick. Internet message format, 2001. http://www.ietf.org/rfc/rfc2822.txt.
[13] M. Tracy, W. Jansen, K. Scarfone, and J. Butterfield. Guidelines on electronic mail security. Technical report, National Institute of Standards and Technology, 2007.

Mohammed Hassouna received his BS.c (honors degree) in mathematics and computer sciences from Faculty of Mathematical and Computer Science, University of Gezira, Sudan in 2007, and his MS.c in Industrial and Computation Mathematic from the Faculty of Mathematical Science, University of Khartoum, Sudan in 2009. Currently, he is registered as a PhD student at the Department of Computer Science – Faculty of Mathematical Science – University of Khartoum. Mohammed is a lecturer and IT Manager at the Faculty of Computer Studies, National Ribat University, Sudan. He is also working as researcher in a Cryptography unit at the Mathematical Sciences and Information Technology Research Unit at University of Khartoum since 2008, his basic research interest is Cryptography and he published a journal and a conference paper in that field.

Nashwa Mohamed received her B.Sc (honors degree) in mathematics and computer sciences in 2001, her M.Sc in Induastrial and Computational Mathematics in 2004 and her Phd in Mathematics in 2012 from University of Khartoum, Sudan. She is currently working as an assistant professor at the University of Khartoum and the head of the department of Pure Mathematics at the same institute. Also she is working as researcher in a Cryptography unit at the Mathematical Sciences and Information Technology Research Unit at University of Khartoum.

Bazara Barry received his Computer Science B.Sc. and M.Sc. degrees in 2001 and 2004 respectively from University of Khartoum, Sudan and his PhD in Electrical Engineering from University of Cape Town, South Africa in 2009. He is currently an assistant professor at University of Khartoum and the head of the department of Computer Science at the same institute. Bazara has served as TPC chair, co-chair, and member at local and international workshops/conferences in computing and engineering, and a reviewer for international journals in information security. In 2011, he received the best paper in session award at IMCIC in Orlando, Florida, USA and the Honor Award in Zayed University competition in IT. He headed the Mathematical Sciences and Information Technology Research Unit at University of Khartoum which carried out research projects for the university and its partners. He has over 10 years of experience in IT industry leading and directing projects, and is a certified Project Management Professional (PMP)®. Bazara is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Project Management Institute (PMI).

Eihab Bashier graduated from the University of Khartoum in 1999 with a joint degree in mathematics and computer sciences. In the years 2002 and 2004 he did his Master and postgraduate diploma in industrial and computational mathematics and mathematical sciences from the University of Khartoum and the African Institute for Mathematical Sciences (South Africa), respectively. In 2009 he obtained his PhD (numerical analysis) from the University of the Western Cape, South Africa. Then he joined the University of Khartoum as an assistant professor in applied mathematics. He also led the cryptography research groups in both the University of Khartoum and the Nile centre for technology research from 2009 to 2012. Currently, he is working as an assistant professor at Albaha University, Saudi Arabia..