A DISTRIBUTED PASSWORD AUTHENTICATED KEY EXCHANGE PROTOCOL USING A HYBRID APPROACH

A. A. Orunsolu [1], A. S. Sodiya [2], O. O. Folorunso [2], A. A. A. Agboola [3]

[1] **Moshood Abiola Polytechnic, South West, Nigeria, Department of Computer Science**
[2] **Department of Computer Science, Federal University of Agriculture, Abeokuta**
[3] **Departement of Mathematical Sciences, Federal University of Agriculture, Abeokuta**

Corresponding author: A. A. Orunsolu, orunsolu.abdul@mapoly.edu.ng

ABSTRACT: Recent Password Authenticated Key Exchange (PAKE) protocols, which are used to establish secured communication between two remote parties without requiring a public key infrastructure, are still quite not efficient. Some of the problems are high memory requirement and low response time of encryption / decryption algorithms. In this work, an Elliptic Curve-ELGAMAL Distributed Password Authentication (EEDPA) in prime field was designed in order to correct these problems. Efficient cryptographic algorithms are examined for the different phases of the design methodology. The evaluation results showed that EEDPA had 23% computational advantage over one of the best PAKE protocol known as Rivest Shamir Adleman (RSA) cryptosystem. The results also showed that the proposed approach offers improved perfect forward secrecy that protects past sessions and passwords against future compromise. This shows that the new approach provides an improved technique for carrying out key exchange authenticated protocol.

KEY WORDS: Password Authentication, EC-ELGAMAL, Dictionary Attack, Security, RSA

1. INTRODUCTION

The idea of key exchange is not a new one as the development of public key cryptosystems has afforded us with a number of crypto-primitives that allow two sides to exchange a session key. This session key is used by communicating parties for bootstrapping a low entropy secret into a secure high entropy cryptographic secret ([FR08]). A key exchange protocol is said to be password-based if the means of identifying the communicating entities is a simple password. Password based authentication is attractive for its simplicity, convenience, adaptability, mobility, and less hardware requirement ([LW08]). The ease of deployment and high level of usability also contributed for the wide use of password-based authentication for most financial transaction over the internet ([MO07]). Nevertheless, passwords because of their low entropy are subjected to dictionary attacks ([And01]) and must therefore be protected during transmission ([LCL15]).

One crucial issue in password-based authentication has been to design protocols that are secure against offline dictionary attacks ([C+05]). The dominant security protocol for handling password transmission has been through SSL (Secure Socket Layer) or TLS (Transport Layer Security) ([Sti06]). However, the use of SSL or TLS requires the deployment of a Public Key Infrastructure (PKI), which is sometimes expensive and overly complex to maintain. In addition, SSL/TLS causes slow response time of web server ([LWK00]) and are subject to man-in-the-middle attacks ([And01]) since public key certificates are rarely checked

In the light of these, there is need to perform authentication and key exchange solely on password without PKI. This research subject is called the Password-Authenticated Key Exchange (PAKE) ([BM03]). Bellovin and Meritt first proposed PAKE in 1992 in a seminar paper. Since then, it has become a well-researched issue in computer security and cryptography. The motivation for PAKE extends to its usefulness especially for highly mobile environment, such as personal networking ([JW01]), conference/meeting ([Per01]), emergency rescue and military operations ([OTV01]). In PAKE, RSA, ELGAMAL and Diffie-Hellman protocols are used in most recent works ([A+09], [MN03], [Zha04] etc). Unfortunately, the deployment of these schemes imposes significant performance penalty on the speed of encryption/decryption algorithms, response time and memory requirement. In addition, some schemes especially those based on RSA has been shown to be insecure ([Zha04]).

Therefore, the need for a more secure protocol with low computational and communication cost especially for a memory-limited environment like mobile platform motivate this research. This work is aimed at providing an alternative and yet more efficient hybrid approach for password-based key exchange protocol using Elliptic Curve ELGAMAL Cryptosystems.

The rest of the paper is organized as follows; Section 2 contains the review of related, Section 3 presents

the basic mathematics for the proposed approach. In the Section 4, the implementation and security analysis of the approach was presented and Section 5 presents the conclusion and future work.

2. RELATED WORKS

Since Kobliz and Miller independently proposed the Elliptic Curve cryptography in 1985, it has become a good competitor to the traditional cryptosystems like RSA. The primary motivation for ECC based approach is the fact that there are no sub-exponential algorithms to solve the underlying mathematics of the cryptosystems. The shorter key sizes needed to achieve efficient security also make considerable saving on the storage, time, power and bandwidth requirement of Elliptic curve cryptosystems. Various analogues of ECC exist for traditional cryptosystems like RSA, DH and ELGAMAL. The EC-ELGAMAL is the most consistent and reliable analogues because of the similarity in the underlying mathematics of the two approaches .i.e. discrete logarithm problem. Boyd et al. ([BMN01]) first investigated password authenticated key exchange (PAKE) protocols in low resource environments, such as smartcards or mobile devices using ECC. Recently, Li et al. ([LW08]) considered the idea of ECC-based verifier protocol to mitigate the amount of damage that can be caused by corruptions in the server. The ECC-verifier protocol was applied to three-party PAKE settings. The authors showed their protocol was secure against several attacks and provided perfect forward secrecy. The advantage of their approach is that it does not require the server's public key.

Jablon D. ([Jab96]) proposed SPEKE (Simple Password Encrypted Key Exchange) as the extension of EKE. Besides preventing password from dictionary attack, DH-EKE and SPEKE protocols achieve perfect forward secrecy, which is the disclosure of the password does not compromise the remaining session keys. Nevertheless, Zhang ([Zha04]) showed that none of these protocols provides any formal security proofs and in fact, many have been shown to be insecure. The use of long exponents contributed to the computational cost of this approach ([FR08])

The OKE (Open Key Exchange) protocol, which is based on RSA, was the first provable approach based on the work of Bellare et al. ([BPR00]) and was followed by SNAPI (Secure Network Authentication Password Information) ([MBP00]). In their paper, the authors of SNAPI first show that OKE protocols are insecure and then modify it to a more secure SNAPI protocol. In 2004, Zhang presented a new password authenticated key exchange protocol called PEKEP (Protected Encrypted Key Exchange Protocol). The SNAPI protocol requires the public exponent e to be larger than the RSA modulus n. In contrast to SNAPI, PEKEP allows the usage of both small and large prime numbers as RSA public exponents. Unfortunately, Feng et al., ([FR08]) show that an active attacker may test multiple passwords in one protocol execution with this approach.

Abdalla et al. ([A+09]) introduced the notion of distributed password-based public-key cryptography, where a virtual high-entropy private key is implicitly defined as a concatenation of low-entropy passwords held in separate locations. Focusing on the case of ELGAMAL encryption as an example, the authors started by formally defining ideal functionalities for distributed public-key generation and virtual private-key computation in the UC model. The adoption of zero knowledge proof, however, adds to the cost of implementation of this approach.

Mustafa et al. ([MN03]) proposed the use of ELGAMAL encryption algorithms as a secure way through which user authentication can be achieved in e-mail. Identity authentication was performed by a unique hash function. This hash algorithm was used while authorized users registered their passwords. This password is not directly saved into database. It is transferred to another form by a hashing function before being saved into database. Thus, dictionary attacks are very unlikely.

Canetti et al. ([C+05]) proposed a new security model in the universal composability (UC) framework, which makes no assumption on the distribution on passwords used by the protocol participants. The authors also proved the security consistency of ELGAMAL cryptosystem in such a framework.

Feng et al. ([FR08]) proposed a novel protocol called Password Authenticated Key Exchange by Juggling in which the public keys are re-arranged in a verified way. The authors showed that J-PAKE is lightweight and required short exponents. However, the use of zero knowledge proof added to the computational and communication cost of this approach.

In a more recent works, Lee et al. ([LCL15]) examined how to fix an offline guessing attack in a three party PAKE. The work was based on the research of Wu et al. ([W+12]) where the problem of the offline guessing attack was discussed. In a similar recent work, Abdalla et al. ([ABM15]) reported the security of the J-PAKE. J-PAKE is an efficient password authenticated key exchange protocol that is included in the OpenSSL library. The work used Decision Square Diffie-Hellman assumptions as well as non-interactive zero-knowledge proofs in the design of their approach.

This current paper is a step forward in the direction of a new Elliptic Curve Cryptosystem using ELGAMAL method. The hybrid approach combines ELGAMAL and Elliptic Curve Cryptosystems (ECC). Abdalla et al., ([A+09]) and Canetti et al., ([C+05]) show that

ELGAMAL cryptosystems is efficient in proving security consistency in PAKE protocols. The Elliptic curve component of the architecture facilitates the use of small key size that provides efficient security in resource-limited environment. The ELGAMAL components on the other hand provides non-regular pattern in the choice of private key for encryption. In addition, the ELGAMAL approach provides enhanced security through masking of encrypted messages. This creates additional burden for potential adversary. The Elliptic Curve ELGAMAL (EC-ELGAMAL) cryptosystem is based on infeasibility of solving elliptic curve discrete logarithm problem.

3. OVERVIEW OF THE DESIGN

Let $p > 3$ be a prime, $a, b \in F_q$ satisfy that the discriminant delta $= 4a^3+27b^2 \neq 0$, which defines the elliptic curve with singularity. The curve is of a simple form:

$y_2= x^3 + ax + b$ with $a, b \in F_q$ or F_{2m}.

We define the Elliptic Curve for the ELGAMAL method over the field of Fq because of the characteristic support for efficient software implementation and absence of binary field arithmetic, which is not compatible with most existing microprocessors ([BGM03])
The Elliptic Curve $E(F_q)$ over Fq consists of a set of points together with a point at infinity. These points form an abelian group $(E(F_q), +)$ with 0 as a group identity.
For some group $G \in Z_p$, suppose $a, b \in G$. Then solving for an integer x such that $ax = b$ is called the discrete logarithm problem which formed the basis of conventional ELGAMAL cryptosystems. The DLP in Zp is replaced by elliptic curve field, Fq, to form the Elliptic curve ELGAMAL cryptosystem and is considered intractable if prime q has at least 160 digits and $q - 1$ has at least one large prime factor. These criteria for q are safeguards against the known attack on EC-ELGAMAL.

3.1. Elliptic Curve-Elgamal Architecture for PAKE

In this scheme, an EC-ELGAMAL approach is adopted for a distributed password authenticated key exchange based on the difficulty of ECDLP. The EC-ELGAMAL is a very useful protocol for randomly generated curves and points because the order of the curve, the factors of that number or the order of the base point is not necessary. Given an elliptic curve E defined over a finite field F_q, $P \in E$ is point of order n and G is the generator point on the curve. A point $Q = kP$ where $k \in [1, n-1]$ defines the scalar multiplication which forms the basis of EC-based cryptographic approach. The secret key for password decryption is an integer $r \in F_q$ while the public key for password encryption is computed as $c = mG$. We define a deterministic mapping function dmap() that take distributed password, $p = a + b + c+\ldots= m$, to curve point $M \in Fq$ such that it obeys the additive homomorphic property of EC-ELGAMAL protocol:

$$dmap(a+b+c+...) = dmap(a) + dmap(b) + dmap(c)+\ldots$$

where M demonstrates how many times m associates with G .i.e. $M = mG$. The reverse mapping function rdmap() is the decryption function that extracts the password m from a given point mG.
One important operation for this mapping is the addition over elliptic curve that is only possible with the points on the curve.
If we define the opposite (encryption) point of $P = (x_1, y_1)$ to be $-P= (x_1, -y_1)$ and $Q= (x_2. y_2)$ with $Q \neq -P$, then $(P+Q) = (x_3, y_3)$ can be calculated as:

$x_3=\lambda_2-x_1-x_2$
$y_3= \lambda(x_1-x_3) - y_1$
$\lambda = (y_2-y_1) / (x_2-x_1)$ if $x_1 \neq x_2$ i.e. adding
$\lambda= (3x_1^2+A) / 2y_1$ if $x_2=x_1$ i.e. doubling

Since the preceding formulae has great impact on the performance optimization of the EC-ELGAMAL based approach, we choose the Double and Add algorithms for the above computation. The optimization of the basic Double and Add algorithm using addition-subtraction method is used for this implementation as described in algorithm 1. Addition-subtraction method has the advantage of reducing the complexity of scalar multiplication by reducing the required number of addition operations.

Algorithm 1: Double and Add Point Scalar Multiplication with subtraction
input : $P \in E(GF(q))$, $k = \Sigma_{i=0}^{nk-1}$ *ki2i*
output: $Q = [k]P \in E(GF(q))$
Initialise: Q=P;

```
for i ← nk − 2 to 0 do
        Q = 2Q //Point Doubling;
      if ki = 1then
    Q = Q + P //Point Addition;
   if ki = -1then
  Q = Q - P //Point Subtraction;
 end
end
end
```

3.2 The Proposed Approach

This subsection describes the execution of our proposed EC-ELGAMAL approach in achieving

mutual authentication, forward secrecy and key confirmation in order to establish a secure channel. The proposed protocol applies ECDLP to the PAKE protocol to enhance the safety level and to simply the computational and communication load. The process flow of user authentication is described in Figure 1.
Prior to commencement of the protocol, the two entities A and B must agree upon the password, Pw. Then, A and B share and divide the previously known password communicated in a secure way by the chopping function define below into x and y

$P = f(x, y) = b$

where f is a cipher algorithm that act on x, y which is equivalent to Boolean variable b equal 1 (true) if the flow is incorruptible.
User A select an elliptic curve Ep (a, b) defined on Zp and picks a random point e_1 over the elliptic curve of order n. In addition, A chooses a random integer r as his private key and computes the public key, C_1 as:

$C_1 = r * e_1$

The username of entity A and C_1 are sent to B. User B chooses his private key, d and computes his own public key using any selected points on the curve as:

$C_1b = d* e_2$

Upon receiving the request, B examines the sender's credentials and uses the public key of A to encrypt his own y portion of the password Pw as:

$Y^* = C_2 = y + d*C_1$

Thereafter, B sent the encrypted Y* and C_1b to A. User A decrypt Y* according to the computation below:

$y = C_2 – (r* C_1b)$

The proof of y as generated by user A is:

$y + r * e_2 - (d*r*e_1) = y + r*d*e1 – r*d*e_1 = y + 0 = y$

where y, C_1, C_2, e_1, e_2 are all points on the curve while 0 is the zero point which serves as the identity of the elliptic curve additive group operation.
If no attack has modified the value of Y*, it follows that Y=Y* as already known by A from B. User A repeat the same process encrypting his x portion of the password with the public key of B so that B confirms that X=X* as already known by B.
Consequently, A and B authenticated each other and generates a session key upon successful authentication for confidential exchanges of long messages.

The notion of reflection message is proposed in this analysis to thwart user corruption. The reflection message, rm, is introduced into authentication flow to tackle user corruption and compensate for forgetfulness on the parts of genuine users. The superscript n-1 on the reflection message denotes that it is related to the topic discussion of the most recent previous secret communication. It is a message whose disclosure can affect the parties in the communication severely. Thus, parties in natural sense guard such information from a third party. A doubting partner may require this message from the other party to prevent corruption

4. EVALUATION AND SECURITY ANALYSIS

The design was implemented using C# Cryptographic Extension. The CCE provides implementations for several algorithms, key generation and key agreement and Message Authentication Codes algorithms. We evaluate the protocol from the point of security robustness, communication overhead (bandwidth) and memory requirement/response time. The security robustness relates to key size and issues of password confidentiality, authentication and integrity

4.1. Security Analysis

A. Password Confidentiality means that it is computationally infeasible whether online or online for an adversary to gain any partial information on the content of EC-ELGAMAL message. In our protocol, if the adversary intercepts the password message and searches the message to obtain r. However, to find r, the attacker needs to solve the equation $C_1=r*e_1$ in which he must find the multiplier that creates C_1 starting from e1. This is the elliptic curve discrete algorithm. Equally, the adversary cannot know accurately guess the private key in one run (since the approach permit only one run of the private key), he cannot compute the session keys due to the difficulty of the elliptic curve discrete logarithm problem ([MVV97]). In addition, the security mask provides by C_1 cannot be partioned in decrypting the message because the adversary had to inverts i.e. C_1-1 = $(r*d*e_1)$-1 and multiplies with the result of C_2 to remove the mask. The secret knowledge of d increases the computation hardness of this attack.
B. Password integrity preserves the password from unauthorized modification, deletion and destruction. Suppose the adversary can know d, then he can use $P= C_2-(d*C_1)$ to find the point P related to the plaintext password message. Because $e_2=d*e_1$, this is the same type of problem. Adversary knows the value of e_1 and e_2; he needs to find the multiplier of d.

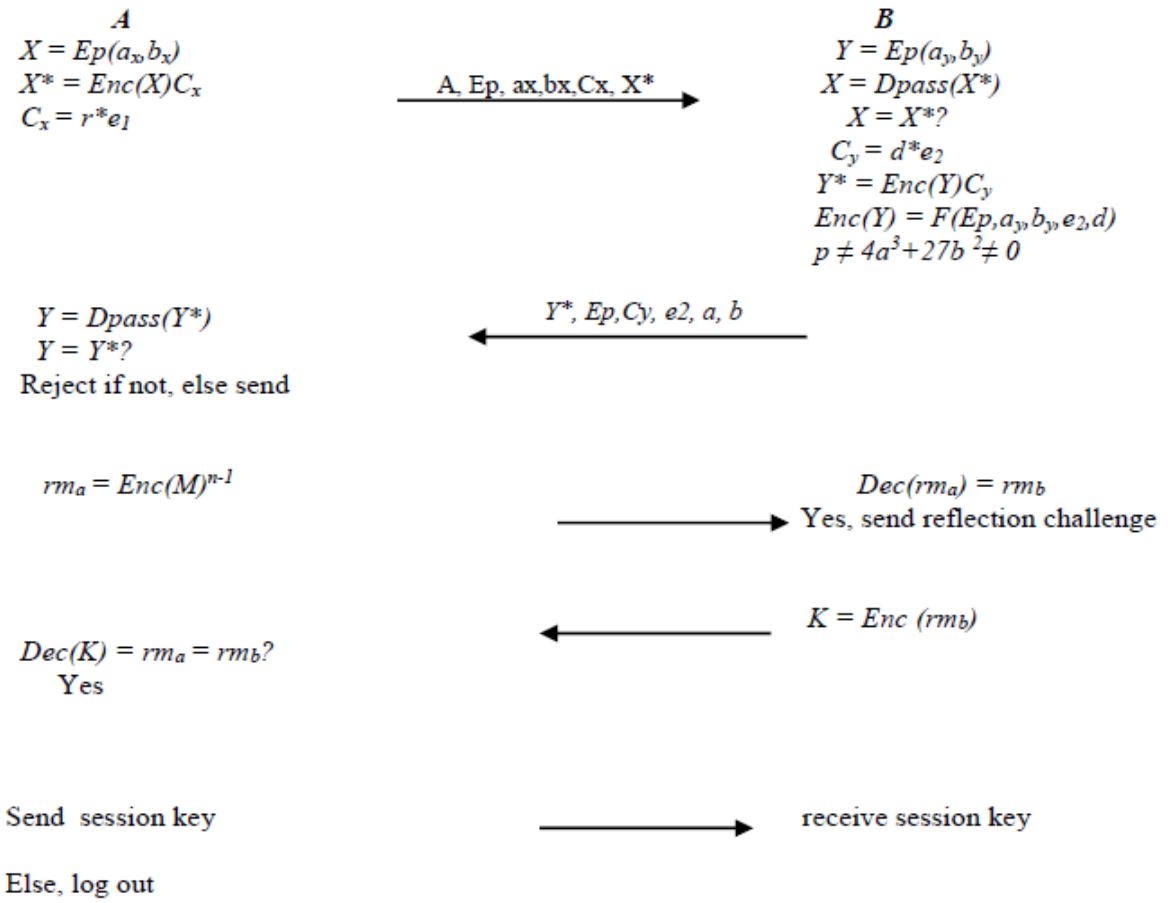

Figure 1: User Authentication Flow

4.2. Performance Evaluation

Computation cost and communication cost are the most important aspects of password authentication protocols, which affect the overall performance. They include number of steps (rounds), exponentiation, large blocks, symmetric encryption and decryption, hash functions and random numbers.

In this section, the EE-DPA is compared with the following protocols: RSA, Simple Key Agreement (SKA) protocols, Authentication Memorable Password (AMP) protocols, Simple Password Exponentiation Key Exchange (B-SPEKE) protocols that is based on RSA and DH and Secure Remote Password (SRP) protocols. The comparison is done in terms of number of steps, exponentiation, hash functions and random numbers.

It is clear from table 1 that the EE-DPA required 2 rounds and 3 random numbers while all the other protocols required more. The absence of XOR and exponentiation operations in the proposed protocol saves computational time and increase the rate of decryption/encryption. The implication of this is the saving in memory requirement and response time of encryption/decryption as compared with the well-known RSA. The EE-DPA has ratio 5:8 with the best known-RSA. This translated to 38.46% and 61.54% for EE-DPA and RSA respectively. The implication is that EE-DPA had 23.08% computational advantage over RSA. Figure 2 shows the graphical illustration of the data obtained from evaluation. The time in milliseconds for different key sizes of the proposed scheme and RSA were compared. The memory usage was a direct implication of small key sizes of the proposed technique when compared with RSA. The bandwidth requirements of communicated messages are shorter as hash function and signatures are not appended to them.

Table 2 shows the comparison in the key sizes need to achieve some level of security. A secure RSA needs at least 1024 bits, which is equivalent to 160 bits in EC-ELGAMAL approach. This is particularly important in constraint environment such as mobile applications and network management applications.

Table 1. Comparison of Performance

Protocol	Round	Exponentiation	Hash Function	Random number	Total
RSA	2	2	-	4	8
SKA	3	5	7	2	17
AMP	4	5	9	2	20
B-SPEKE	4	7	-	2	11
SRP	4	6	6	2	18
EC-ELGAMAL	2	-	-	3	5

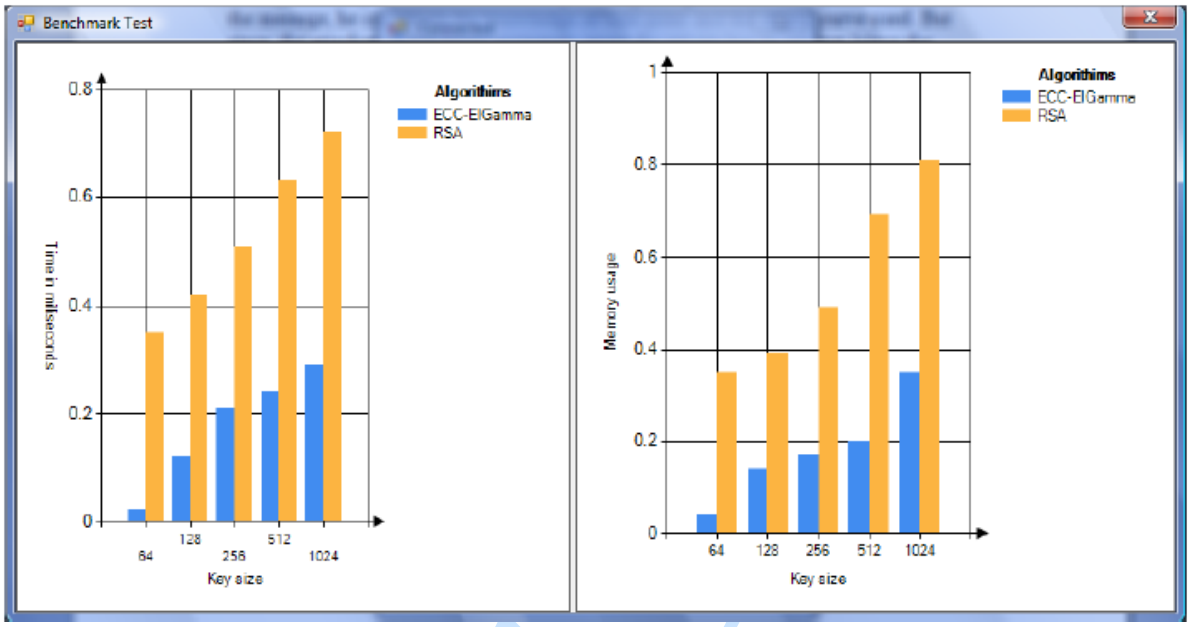

Figure 2: Performance Evaluation

Some of the advantages on this approach include:
1.The rate at which EC-ELGAMAL key sizes increase in order to obtain increased security is much slower than the conventional RSA or DL systems
2.The ECC-ELGAMAL approach uses an elliptic curve group in which encryption/decryption is more secure and faster than the conventional RSA or ELGAMAL.
3.Computation overhead, storage cost and bandwidths requirement are low compared to conventional RSA or ELGAMAL.
4.The public keys of EC-ELGAMAL can be left unchanged for a long period and there is not need to remember the secret key as a new one can be selected for every new message. This provides both secret sharing and authentication.

CONCLUSION AND FUTURE WORKS

In this paper, we discussed a framework for distributed password authenticated key exchange using a hybrid approach. This approach requires low memory, which can be easily extended to mobile applications where authentication is available only by numeric keypad.
We hope to extend PAKE approach to mobile agent technology for efficient gateway and network management especially at different levels of OSI models where challenge/acknowledge can prevent wiretappers intending to view sensitive data. We believe Mobile agent PAKE (MAPAKE) will provide a very interesting research domain for efficient mobile transactions.
Furthermore, new results in the area of quantum cryptography may eventually make all discrete logarithm problem approach obsolete. This is because quantum computers are capable of solving ECDLP in polynomial time. It is hope that the development of non-associative binary system would provide rescue for cryptographers. Is it possible to construct non-associative binary system over elliptic curve with a trapdoor of cross inverse property from Keedwell CIPQ? This is one of the research issues that will dominate future cryptography.

REFERENCES

[And01] **R. J. Anderson** - *Security Engineering: A Guide to Building Dependable Distributed Systems*, New York, Wiley, 2001.

[ABM15] **M. Abdalla, F. Benhamouda, P. MacKenzie** - *Security of the J-PAKE Password Authenticated Key Exchange Protocol*, IEEE Symbosium on Security and Privacy, 2015.

[A+09] **M. Abdalla, X. Boyen, C. Chevalier, D. Pointcheval** - *Distributed Public-Key Cryptography from Weak Secrets*, International Conference on Theory and Practice in Public Key Cryptography - PKC 2009, Irvine, CA, USA, Springer-Verlag, LNCS 5443, pages 139-159, 2009.

[Beh08] **A. Behrouz** - *Cryptography and Network Security*, McGrawHill, International Edition. 2008.

[BM03] **C. Boyd, A. Mathuria** - *Protocols for authentication and key establishment*, Springer-Verlag, 2003.

[BM93] **S. Bellovin, M. Merritt** - *Augmented Encrypted Key Exchange: a password-based protocol secure against dictionary attacks and password file compromise*, Proceedings of the first ACM Conference on Computer and Communications Security, pp. 244–250, 1993.

[BGM03] **I. Branovic, H. Giorgi, E. Martinelli** - *Memory Performance of Public-Key cryptography Methods in Mobile Environments*, ACM SIGARCH Workshop (MEDEA-03), pages 24–31, New Orleans, LA, USA, 2003.

[BMN01] **C. Boyd, P. Montague, K. Nguyen** - *Elliptic Curve Based Password Authenticated Key Exchange Protocols*, LNCS 2119, pp. 487–501, Springer-Verlag Berlin Heidelberg, 2001.

[BPR00] **M. Bellare, D. Pointcheval, P. Rogaway** - *Authenticated Key Exchange Secure Against Dictionary Attacks*, Springer, 2000.

[C+05] **R. Canetti, S. Halevi, J. Katz, Y. Lindell, P. D. MacKenzie** - *Universally composable password-based key exchange*, EUROCRYPT 2005, volume 3494 of LNCS, pages 404-421, Springer, 2005.

[FR08] **H. Feng, P. Ryan** - *Password Authenticated Key Exchange by Juggling*, 2008.

[F+04] **L. Fang, S. Meder, O. Chevassat, F. Siebenlist** - *Secure Password-Based Authenticated Key Exchange for Web Services*, ACM, Fairfax VA, USA, 2004.

[GMR06] **C. Gentry, P. MacKenzie, Z. Ramzan** - *A method for making password-based key exchange resilient to server compromise*, Crypto'06, LNCS 4117, pp. 142–159, 2006.

[Jab96] **D. Jablon** - *Strong password-only authenticated key exchange*, ACM Computer Communications Review, Vol. 26, No. 5, pp. 5–26, 1996.

[JW01] **M. Jakobsson, S. Wetzel** - *Security weaknesses in Bluetooth*, in Proceedings of the RSA Cryptology, LNCS 2020, Springer-Verlag, 2001.

[LW08] **W. M. Li, Q. Y. Wen** - *Efficient verifier-based password-authentication key exchange protocol via elliptic curves*, International Conference on Computer science and Software engineering, 2008.

[LCL15] **C. C. Lee, S. T. Chiu, C. T. Li** - *Improving Security of a Communication efficient Three party Password Authentication Key Exchange Protocol*, International Journal of Network Security. Vol.7, 2015.

[LWK00] **X. Lin, J. W. Wong, W. Kou** - *Performance analysis of secure web server based on SSL*, pp. 249-261, Berlin, Heidelberg: Springer, 2000.

[Mat06] **E. Mathew** - *Elliptic Curve Cryptography*, M.Sc Thesis, Herriot-Watt University, 2006.

[MN03] **D. Mustafa, S. Nusret** - *A Secure E-mail Application using the ELGAMAL Algorithm: MD message controller*, Journal of Electrical & Electronic Engineering, Istanbul University, Turkey, 2003.

[MO07] **M. Mannan, P. C. van Oorschot** - *Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer*, 2007.

[MBP00] **P. MacKenzie, V. Boyko, S. Patel** - *Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman*, 2000.

[MVV97] **A. Menezes, P. C. van Oorschot, S. A. Vanstone** - *Handbook of Applied Cryptography*, CRC press, 1997.

[OTV01] **K. Obraczka, G. Tsudik, K. Vismanath** - *Pushing the limits of multicast in ad hoc networks*, in International Conference on Distributed Computing System, 2001.

[Per01] **C. Perkins** - *Ad hoc networking*, Addition Wesley, 2001.

[Sti08] **D. Stinson** - *Cryptography: theory and practice*, Third Edition, Chapman & Hall/CRC, 2008.

[SJ08] **S. Sean, M. John** - *The Craft of System Security*, Orange Book, 2008.

[W+12] **S. Wu, Q. Pu, S. Wang, D. He** - *Cryptanalysis of a communication-efficient three party password authentication key exchange protocol*, Information Science Journal, 2012.

[Zha04] **M. Zhang** - *Analysis of the SPEKE password authenticated key exchange protocol*, IEEE Communication Letters, Vol 8, 2004.

Tibiscus