DOI: 10.15415/jtmge.2015.61004

On Security Analysis of Recent Password Authentication and Key Agreement Schemes Based on Elliptic Curve Cryptography

Prabhdeep Kaur
Guru Nanak Dev University, Regional Campus, Jalandhar, India.

Sheetal Kalra
Guru Nanak Dev University, Regional Campus, Jalandhar, India.

Abstract

Secure and efficient mutual authentication and key agreement schemes form the basis for any robust network communication system. Elliptic Curve Cryptography (ECC) has emerged as one of the most successful Public Key Cryptosystem that efficiently meets all the security challenges. Comparison of ECC with other Public Key Cryptosystems (RSA, Rabin, ElGamal) shows that it provides equal level of security for a far smaller bit size, thereby substantially reducing the processing overhead. This makes it suitable for constrained environments like wireless networks and mobile devices as well as for security sensitive applications like electronic banking, financial transactions and smart grids. With the successful implementation of ECC in security applications (e-passports, e-IDs, embedded systems), it is getting widely commercialized. ECC is simple and faster and is therefore emerging as an attractive alternative for providing security in lightweight device, which contributes to its popularity in the present scenario. In this paper, we have analyzed some of the recent password based authentication and key agreement schemes using ECC for various environments. Furthermore, we have carried out security, functionality and performance comparisons of these schemes and found that they are unable to satisfy their claimed security goals.

Keywords: *Elliptic curve cryptography, Smart Card, Remote user authentication, ECDLP, User anonymity.*

INTRODUCTION

With the rapid growth of internet and wireless communication network, users can easily use the services of remote server anytime and anywhere. The popularity of such services has exposed the information over network to various security threats and the need of practically secure user authentication and key agreement systems has become vital for these networks. Various schemes based on password, biometric, smart card, dynamic-id or a combination of these have been proposed for remote user authentication. Of these, password based authentication schemes have gained more popularity due to their simplicity, scalability, efficiency and convenience. The concept of authentication based on password was introduced by Lamport [1] in 1981. He proposed a password authentication scheme based on hash function that mutually authenticates client and the server. Although it

Journal of Technology
Management for
Growing Economies
Vol. 6, No. 1
April 2015
pp. 39-52

was resistant to eavesdropping and impersonation attack but was vulnerable to replay attacks, offline password guessing attacks and password related problems. A number of improved password authentication and key agreement schemes have been proposed since then. For the purpose of confidentiality and authentication, public key cryptosystems have advantage over symmetric key cryptosystems as they eliminate the problem of key distribution and digital signatures. Neal Koblitz [33] and Victor S. Miller [32] independently proposed security protocols using elliptic curves in 1985. ECC based protocols gained popularity in early 2000 and are the strongest public-key cryptographic systems known today. Compared with RSA, Rabin and Elgamal cryptographic systems, ECC has remarkable strength and efficiency advantages in terms of bandwidth, key sizes and computational overheads. ECC is therefore the most sought after clean and sustainable technology which is widely being implemented in next generation wireless networks, Internet of Things (IoT), embedded systems, smart grids, mobile ad-hoc networks, radio frequency identification and so on. Thus ECC when used in password authentication and update schemes provide high security at a reasonable computational cost.

This paper is organized as follows: In Section II, survey of recent ECC based password authentication and update schemes for smart cards has been done. In Section III, mathematical background of ECC has been given. Security and efficiency analysis of existing schemes is done in Section IV. Section V gives the performance analysis of the existing schemes. Various applications of ECC are presented in Section VI. In Section VII, we outline various issues and propose future directions. Finally in Section VIII, we conclude the paper.

SURVEY OF RECENT ECC BASED PASSSWORD AUTHENTICATION AND UPDATE SCHEMES FOR SMART CARDS

Although a number of password, biometric [30-31], dynamic-id [27-29] based authentication and update schemes have been proposed for smart cards [6][9][12][14][16][23-26][31], mobile devices [15][17-23], smart grids, etc; it is practically impossible to conduct a survey of all such schemes.

Table 1: Survey of recent password authentication schemes based on ECC

Year	Author	Related Research Scholarship
2011	Islam and Biswas [2]	In this paper, they studied the flaws of Lin and Hwang scheme [3] and found that it is susceptible to insider attack, stolen verifier attack, impersonation attack, many logged-in users attack, known session specific temporary information attack and proposed a secure password authentication and update scheme based on ECC. Their scheme also generates a common ECC based secret key that is used for symmetric encryption.

Year	Author	Related Research Scholarship
2011	D. He [4]	In this paper, he analyzed the security of Islam and Biswas scheme [2] and found that it is vulnerable to three kinds of attacks in different scenarios: (1) Stolen-verifier attack (2) Offline password guessing attack (3) Privileged Insider attack
2011	Wang, Juang and Lei [5]	In this paper, they studied Wang et al. [6] scheme and found that it is vulnerable to smart card loss problem and known key attack. They further proposed a key agreement scheme based on the elliptic curve discrete logarithm problem.
2012	He, Wu and Chen [7]	In this paper, they performed a cryptanalysis of Islam and Biswas scheme [2] and found that their scheme is vulnerable to offline password guessing attack and stolen-verifier attack.
2012	Wang et al. [8]	In this paper, they analyzed Islam and Biswas scheme [2] and showed it has following weaknesses: (1) It is susceptible to offline password guessing attack, stolen verifier attack and denial of service (DoS) attack; (2) It also fails to preserve user anonymity.
2012	C.T.Li [9]	In this paper, he analyzed Islam and Biswas scheme [2] and found that it is prone to offline password guessing attack, stolen-verifier and insider attacks. He further proposed a smart card based ECC scheme that also provides user anonymity.
2014	Wang [10]	In this paper, she demonstrated that in addition to previously found security flaws [4][8][9] in Islam and Biswas scheme [2] like offline password guessing attack, stolen verifier attack, privilege insider attack, and denial of service attack, their scheme cannot resist password compromise impersonation attack. She further proposed an anonymous remote authentication scheme using smart card without using bilinear paring computation. She claimed that her scheme not only inherits the advantages in Islam and Biswas' scheme, but also provides more features, including preserving user anonymity, supporting offline password change, revocation, re-registration with the same identifier and system update.
2014	Qiao and Tu [11]	In this paper, they proposed a security enhanced scheme that eliminates the weaknesses of Islam and Biswas scheme [2] as pointed out by He et al. [7]. They claimed that their scheme performs better than Islam and Biswas's scheme and is more suitable for practical applications.

Year	Author	Related Research Scholarship
2014	Ramesh and Bhaskaran [12]	In this paper, they analyzed Li’s scheme [9] and demonstrated that Li’s scheme is prone to insiders attack, password guessing attack, stolen verifier attack and does not provide user anonymity. It is also inefficient in error password login. They also found that when the public key of the server is compromised, the adversary can obtain all the previous session keys between user and the server. They further proposed an improved scheme that inherits the merits of Li’s scheme with the removal of modular computations involved in bilinear pairing operations.

Thus in this paper, we have considered only ECC based password authentication and update schemes for smart cards. Literature survey of various recent password authentication and key agreement schemes based on ECC and the works related to their improvement has been studied in Table I.

MATHEMATICAL BACKGROUND OF ECC

The robustness of any cryptographic security protocol depends on the hardness in solving the underlying mathematical problem. The security of ECC based protocols depend on the difficulty of solving Elliptic Curve Discrete Logarithm Problem (ECDLP), Elliptic Curve Computational Diffie–Hellman Problem (ECCDHP) and Elliptic Curve Decisional Diffie–Hellman Problem (ECDDHP).

Theory of elliptic curve

The equation of a non-singular elliptic curve $E_p(a,b)$ over a finite field Z_p can be written as:

$$y^2 \ mod \ p \equiv x^3+ax+b(modp)$$

where a and b are two integer elements and p is a large prime number. Furthermore, for the above equation to be non-singular, the condition must be satisfied. G is a base point in $E_p(a,b)$ with a prime order n and O is the point of elliptic curve at infinity, where G multiplies n is equal to O ($n.G=O$). A cyclic group $E = \{(x, y) \ \ E_p(a, b)\} \ \ \{O\}$ is formed by any point $P(x, y) \ \ E_p(a, b), x, y$ Z_p, where O represents additive identity element of the group. The point multiplication is evaluated by iterative addition as,

$$x.P = \overbrace{P + P + \ldots\ldots + P}^{x \ times}$$

Mathematical problems

The security of ECC based protocols depend on hardness in solving the following problems:

Problem 1. Elliptic Curve Discrete Logarithm Problem (ECDLP): Given the equation $P = kG$ where $P, G \in E_p(a,b)$ and $k < p$, it is relatively easy to compute P when the values of k and G are known, but it is hard to evaluate k given the values of P and G. Although ECDLP is computationally hard to solve, various exponential algorithms for attacks on ECDLP are known. Such attacks, also known as generic attacks use algorithms like the Pohlig- Hellman [35], Pollard- Rho [36] and parallelized version [37] of the Pollard rho algorithm for attacks on ECDLP. However, if the elliptic curve parameters are cautiously selected, then all the known attacks on ECDLP are believed to be infeasible given the state of today's scientific technology.

Problem 2. Elliptic Curve Computational Diffie–Hellman Problem (ECCDHP): Given G and two point xG, yG, computation of xyG is hard, where $x, y \in Z_p^*$ and are randomly chosen and are smaller than n. Like ECDLP, the solution to ECCDHP is also computationally hard. The proof of intractability of the ECCDHP was given by Boneh and Lipton [38] who proved that if the ECDLP cannot be solved in subexponential time, then neither can ECCDHP. Shoup's [39] result further provide more evidence of hardness of ECCDHP.

Problem 3. Elliptic Curve Decisional Diffie–Hellman Problem (ECDDHP): Given G and three point xG, yG, zG, it is hard to decide whether $zG = xyG$ or not, where $x, y, z \in Z_p^*$ and are chosen randomly and are smaller than n. Like ECCDHP, the solution to ECDDHP is also computationally hard. The evidence of hardness of ECDDHP has been given by Shoup [39].

Elliptic Curve Point Operation

The security of elliptic curve cryptosystem is also based on the efficient execution of arithmetic operations in the underlying field. In point multiplication operation, a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equations to obtain another point R on the same elliptic curve i.e. kP=R. Point multiplication is performed by two basic elliptic curve operations.

- *Point addition*, where two points P and Q on the elliptic curve are added to obtain another point R which also lie on the same elliptic curve i.e., R = P + Q.
- *Point doubling*, where the same point P on the elliptic curve is added to itself to obtain another point R on the curve i.e. R = 2P.

An instance of point multiplication operation is as shown. Here let P is a point on elliptic curve and k is a scalar. P is multiplied with k to obtain another point R on the curve i.e. R = kP.

If k = 11 then kP = 11.P = 2(2(2P) + P) + P.

Thus point multiplication operation involves repeated point addition and point doubling operations to find the result.

Also, a point on an elliptic curve if repeatedly added to itself will eventually reach O, the point at infinity. The number of times a point can be repeatedly added to itself until it reaches infinity is called the order of the point.

SECURITY AND EFFICIENCY ANALYSIS

An ideal password authentication and key agreement scheme is expected to satisfy some prerequisite security and functionality features. In this section, we list out these desired attributes. We further compare some of the existing ECC based authentication schemes to analyze their claimed security and functionality goals.

Security Analysis

The security comparison of existing schemes is presented in Table II. The security attributes are discussed as below.

Offline Password Guessing Attack

The offline password guessing attack is a serious problem in any password based remote user authentication scheme. In this type of attack, the adversary eavesdrops various communication messages between remote server (S) and client (A) via insecure channel and tries to guess the client's identity ID_A and password PW_A from the exchanged messages. Most of the ECC schemes rely on the hard problem of Elliptic Curve Discrete Logarithm Problem (ECDLP) which is impossible to compromise using any polynomial time algorithm. Unfortunately, the adversary can guess the correct password by using the authentication information stored in the user's insecure device or by illegally accessing the secure information stored in the remote server. Also, the client chooses low entropy passwords which can be easily resolved by ECDLP in a polynomial time algorithm, thus exposing the system to offline password guessing attack.

Stolen Verifier Attack

The stolen verifier attack occur when the adversary steals the password verifier U_A or other security sensitive information from the server's database and launch an offline guessing attack on it to acquire the client's legitimate password PW_A. The adversary may then impersonate as a legitimate client to access the remote server.

Insider Attack

In insider attack, a client A may register with a number of servers $S_1, S_2, ..., S_n$

using the same identity ID_A and password PW_A for his/her convenience. If the privileged insider U_1 of server S_1 has knowledge of A's password PW_A and identity ID_A, then U_1 may try to access other servers $S_2, S_3, \ldots, S_n$ by using the same password PW_A and identity ID_A, thereby compromising the security of the system.

Impersonation Attack

In impersonation attack, the adversary makes an attempt to imitate as a legal client A by forging the authentication information of the user. He may eavesdrop the information transmitted between the client A and server S and thus can launch an offline guessing attack on it to acquire the client's legitimate password PW_A. Once the adversary obtains the correct password of client A, he can login to the remote server using PW_A and ID_A.

Server Spoofing Attack

Server spoofing attack is also known as server impersonation attack. In this type of attack, the adversary sets up a fake server by manipulating the sensitive data of the legitimate user. The client thus transmits security sensitive information to this fake server without being aware of its authenticity.

Many Logged-in Users Attack

In this attack, it is assumed that the password (PW_A) and the identity of A (ID_A) are leaked to many adversaries who can in turn login the remote server whenever they want. This is a serious issue as a number of adversaries can cause a security breach using valid password PW_A and the identity of ID_A thus disrupting the whole system.

Password Disclosure Attack

In password disclosure, the client's password is disclosed by intrusion in the verification table from the server or by using the authentication information stored in the user's insecure device.

Table 2: Security Comparison of the Existing Schemes

Security Characteristics	**Song et al. [16] (2010)**	**Islam [2] (2011)**	**C.T.Li [9] (2012)**	**S.Ramesh [12] (2014)**
Offline password guessing attack	No	Yes	Yes	Yes
Stolen verifier attack	No	Yes	Yes	Yes
Insider attack	Yes	Yes	Yes	Yes

Security Characteristics	Song et al. [16] (2010)	Islam [2] (2011)	C.T.Li [9] (2012)	S.Ramesh [12] (2014)
Impersonation attack	Yes	Yes	No	Yes
Server spoofing attack	Yes	Yes	Yes	Yes
Many logged-in users attack	No	No	No	Yes
Password disclosure attack	No	No	No	No

Table 3: Functionality Comparison of the Existing Schemes

Functionality comparisons	Song et al. [16] (2010)	Islam [2] (2011)	C.T.Li [9] (2012)	S.Ramesh [12] (2014)
Mutual authentication	Yes	No	No	No
Freely choosing and updating password	Yes	Yes	Yes	Yes
Session key agreement	Yes	Yes	No	Yes
Prevention of clock synchronization	No	Yes	Yes	Yes
User anonymity	No	No	No	No
Perfect forward secrecy	No	No	No	No
Bilinear pairing	No	Yes	Yes	No

Functionality Analysis

The functionality comparison of existing schemes is presented in Table III. The functionality attributes are discussed as below.

Mutual Authentication

Mutual authentication is the mechanism in which both the client and server authenticate each other using response-challenge technique and are assured of each others' legal identity before the initiation of communication over insecure channel. After mutual authentication, the security sensitive information is exchanged between the server and the client.

Freely Choosing and Updating Password

In ideal authentication scheme, the client can easily choose his/her password PW_A without any support from the remote server. Also the legal client can modify his/her password anytime using the password change phase.

Session Key Agreement

In session key agreement, after successful mutual authentication a common and secure session key *SK* is established between the legal server and client in each session. With this *SK*, the confidential messages between the client and the remote server can exchange safely.

Prevention of Clock Synchronization

The clock synchronization problem arises due to the use of time stamps used in login systems to prevent replay attacks. Random numbers can be used instead of time stamps to prevent replay attack and thus can prevent clock synchronization problem.

User Anonymity

During the communication between client and remote server over an insecure network, the adversary or third parties may know the identity of the client by intercepting the messages exchanged between them. Thus providing user anonymity is very important.

Perfect Forward Secrecy

In perfect forward secrecy, the security of previous sessions established between the legal client and remote server using common session key is not affected even if the security of private keys of client and server is compromised.

Bilinear Pairing

Bilinear pairings derived from the Weil pairings or Tate pairings on elliptic curves are used in cryptography to construct identity and password based cryptographic schemes. It has been found that the cost of the bilinear parings is approximately 20 times more than that of the scalar multiplication over elliptic curve group [34]. Thus using an alternative approach over bilinear pairing improves the performance of the system to a great extent.

PERFORMANCE ANALYSIS

In this section, in order to evaluate the performance of the recent existing schemes, we compare the computation cost of these schemes in each phase. Table IV gives a brief review of the performance by computing the time consumed by various operations in each phase. Here T_S denote the symmetric key encryption, T_H denote the hash operation, T_E denotes the modulus exponentiation operation, T_{EM} denotes the elliptic curve multiplication, T_A denotes the elliptic curve addition and subtraction, T_X denotes the XOR operation and T_P denotes bilinear pairing operation

We analyze that Islam-Biswas's scheme [2] and C.T.Li's scheme [9] make use of bilinear pairings. It has been found that the cost of the bilinear parings is approximately 20 times more than that of the scalar multiplication over elliptic curve group [34] i.e. $T_P \gg T_{EM}$. Also Song [16] uses exponential operation and the time taken to perform an exponential operation is approximately 8 times than the time taken to perform one elliptic point multiplication [40] i.e. $T_E \gg T_{EM}$. Furthermore, Islam and Biswas [2], Li [9] and Ramesh and Bhaskaran [12] makes use of elliptic curve addition/multiplication which is quite slow than XOR operation which increases their overall computation cost. Thus we can analyze that the existing schemes are quite inefficient in terms of their overall performance.

Table 4:Computation Cost Comparison of the Existing Schemes

Computation cost	**Song et al. [16] (2010)**	**Islam [2] (2011)**	**C.T.Li [9] (2012)**	**S.Ramesh [12] (2014)**
Registration Phase	$T_E + 2T_H$	T_{EM}	$2T_{EM}$	$T_{EM} + 3T_H + 4T_X$
Login & Authentication Phase	$2T_S + 5T_H + T_E$	$2T_S + 4T_H + 6T_{EM} + 2T_P + 2T_A$	$2T_S + 4T_H + 11T_{EM} + 2T_P + 2T_A$	$2T_S + 5T_H + 6T_{EM} + 6T_X + 2T_A$
Session key generation Phase	$2T_H$	$2T_S + 4T_H + 8T_{EM} + 2T_P + 2T_A$	$2T_S + 4T_H + 13T_{EM} + 2T_P + 2T_A$	$2T_S + 5T_H + 8T_{EM} + 6T_X + 2T_A$
Password change Phase	$3T_H + T_E$	$2T_S + 4T_H + 8T_{EM} + 2T_P + 4T_A$	$2T_S + 4T_H + 11T_{EM} + 2T_P + 4T_A$	$2T_S + 5T_H + 6T_{EM} + 6T_X + 4T_A$

APPLICATIONS OF ECC

ECC is successfully being used in vast majority of existing applications. In resource constrained environments, elliptic curves are emerging as an attractive alternative over the first generation public key systems like Diffie and Hellman. Also, the elliptic curves are suitable in applications where

- Computing power is limited (intelligent cards, wireless devices, PC boards, PDAs, etc.)
- Processing overheads should be less (wireless sensor networks)
- Memory size on integrated circuit is limited (embedded systems)
- a great speed of computing is necessary (Big Data, e-commerce)
- Digital bandwidth is limited

This makes it suitable for constrained environments like wireless networks, mobile devices as well as security sensitive applications like electronic banking, financial transactions and smart grids. ECC significantly reduces the high processing burden on applications conducting large number of secure transactions thus making it widely acceptable for e-commerce and e-ID documents. ECC delivers faster, more secure processing for e-passports and other government issued e-ID. ECC provides high performance and security at a reasonable cost. Furthermore, it successfully prevents most of the security attacks with a very small key size as compared to other public key cryptosystems like RSA. Today, manufacturers have incorporated ECC into their solutions because the technology is designed for small devices like smart meters, smart cards, etc. Due to this commercialization, ECC based technology is finding applicability in wired and wireless networks, mobile ad-hoc networks, Internet of Things (IoT), radio frequency identification, Wireless Body Area Networks (WBAN), smart grids, big data, ubiquitous computing and so on.

ISSUES AND FUTURE DIRECTION

Issues

Despite the wide acceptance of elliptic curves because of their unlimited merits, they have been criticized by researchers on various grounds which limit their use and implementation.

1 Various features of ECC have been patented by corporate and business organizations all over the world. For instance, Certicom Inc. which is a Canadian company holds over 130 patents related to public key cryptography and elliptic curves, thus restricting its usage.

2 Various attacks against curve over prime fields as well as over binary fields are possible if the elliptic curve is not chosen carefully. Such curves which are also known as supersingular or anomalous curves have been identified and strictly prohibited in various projects developing standard specifications for public key cryptography like IEEE P1363, ANSI X9.62 and ANSI X9.63. Many such anomalous curves still remain unidentified.

3 Pollard's Rho method provides a simple yet powerful way to solve discrete logarithm problems on elliptic curves defined over finite fields. The algorithm is easy to implement, requires minimal storage and works for curves defined over any finite field with any type of representation. Thus strengthening the security of system from pollard's attack is a major issue.

4 The security of ECC based authentication schemes is further crippled due to weak passwords. Passwords can be easily compromised by launching offline password guessing, impersonation and stolen verifier attacks. In

such a scenario, proposal of password less authentication schemes can remarkably contribute towards improving the security of these systems.

B. Future scope

Despite of the above issues, ECC based applications are getting commercialized. For instance, Certicom has planned to enter the market by selling elliptic curve cryptography based software toolkits. National Security Agency (NSA) which is an American organization utilizes the mathematics of elliptic curves over finite fields for providing internet security. Other countries like U.K and Canada have also adopted ECC based systems to ensure the security of their systems. The popularity and successful implementation of ECC can be estimated from the fact that the US Department of Defense plans at replacing almost 1.3 million existing equipments over the coming decade. New generation of cryptographic equipments that are based on the mathematics of elliptic curves for key management and digital signatures are successfully being used in defense sector in many countries. Thus we can foresee the bright future of ECC in the coming years.

CONCLUSIONS

Elliptic Curve Cryptography provides higher security and efficiency than other public key cryptosystems (RSA, Rabin and Elgamal). In implementations, the savings of processing overhead leads to higher processing speeds, lower power consumption and code size reductions. The applications seeking practically efficient, clean and sustainable solutions to network security threats have seriously considered elliptic curve cryptosystems as an attractive alternative over the other systems. Unfortunately, we observe that no single scheme till date satisfies all the security and functionality requirements. Thus robust and improved elliptic curve cryptography based authentication scheme need to be developed that not only provide all the security and functionality features but also reduce the computation costs.

REFERENCES

Lamport, L. (1981) "*Password Authentication With Insecure Communication*," *Commun. ACM*, Vol. 24:11, pp. 770–772.

Islam, S.H., Biswas, G.P. (2013) "*Design of Improved Password Authentication and Update Scheme Based on Elliptic Curve Cryptography*," Math. Comput. Model., Vol. 57:. 11–12, pp. 2703–2717.

Lin, C.L., Hwang T. (2003) "*A Password Authentication Scheme with Secure Password Updating*," Computer and Security, Vol. 22:1, pp. 68-72. http://dx.doi.org/10.1016/S0167-4048(03)00114-7.

D. He, (2011) "*Comments on A Password Authentication and Update Scheme Based on Elliptic Curve Cryptography*," Cryptology EPrint Archive Report 2011/411.

Wang, R.C., Juang, W.S., Lei, C.L. (2011) "*Robust Authentication and Key Agreement Scheme Preserving yhe Privacy of Secret Key*," Computer Communications, Vol. 34:3, pp. 274–280. http://dx.doi.org/10.1016/j.comcom.2010.04.005.

X.M. Wang, W.F. Zhang, J.S. Zhang, M.K. Khan. (2007) "*Cryptanalysis and Improvement on Two*

Efficient Remote User Authentication Scheme Using Smart Cards," Computer Standards and Interfaces, Vol. 29:5, pp. 507–512, 2007. http://dx.doi.org/10.1016/j.csi.2006.11.005.

Debiao He, Shuhua Wu, Jianhua Chen (2012) "*Note on 'Design ff Improved Password Authentication and Update Scheme Based on Elliptic Curve Cryptography*'", Mathematical and Computer Modelling, Vol. 55: 3–4, pp. 1661-1664. http://dx.doi.org/10.1016/j.mcm.2011.10.079.

D. Wang, C. G. Ma, L. Shi, and Y. H. Wang (2012) "*On ihe Security of An Improved Password Authentication Scheme Based on Ecc*," in Information Computing and Applications, vol. 7473 of Lecture Notes in Computer Science, pp. 181–188.

C.T. Li (2012) "*A New Password Authentication and User Anonymity Scheme Based on Elliptic Curve Cryptography and Smart Card*," IET Information Security, Vol. 7, No. 1, pp. 3-10.

Lili Wang (2014) "*Analysis and Enhancement of a Password Authentication and Update Scheme Based on Elliptic Curve Cryptography*," Journal of Applied Mathematics, Volume 2014 (2014), Article ID 247836, 11 pages. http://dx.doi.org/10.1155/2014/247836.

P. Qiao, H. Tu (2014) "*A Security Enhanced Password Authentication and Update Scheme Based on Elliptic Curve Cryptography*," International Journal of Electronic Security and Digital Forensics, vol. 6 Issue 2, pp. 130-139. http://dx.doi.org/10.1504/IJESDF.2014.063109.

S. Ramesh, Dr.V.Murali Bhaskaran (2014) "*An Improved Remote User Authentication Scheme with Elliptic Curve Cryptography and Smart Card without using Bilinear Pairings*," International Journal of Engineering and Technology (IJET) Vol. 5, No. 6 Dec 2013-Jan 2014.

I.-E. Liao, C.-C. Lee, and M.-S. Hwang (2006) "A *Password Authentication Scheme Over Insecure Networks," Journal Of Computer And System Sciences*, Vol. 72, No. 4, pp. 727–740. http://dx.doi.org/10.1016/j.jcss.2005.10.001.

Chun-Ta Li and Cheng-Chi Lee (2011) "A Robust Remote User Authentication Scheme Using Smart Card," *Information Technology and Control*, Vol. 40, No. 3, pp. 236–245.

Toan-Thinh Truong, Tran, M.-T, Anh-Duc Duong (2012) "*Improvement of More Efficient and Secure Id-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC*," 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA). pp. 698-703.

R. Song (2010) "*Advanced Smart Card Based Password Authentication Protocol"*, Computer Standards & Interfaces, Elsevier Vol. 32, No. 4, pp. 321-325. http://dx.doi.org/10.1016/j.csi.2010.03.008.

SK Hafizul Islam, G.P.Biswas (2011) "*A More Efficient and Secure Id-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptography*", Journal of Systems and Software, Vol. 84, No. 11, pp. 1892-1898.

T.-H. Chen, Y.-C. Chen, W.-K. Shih (2010) "*An Advanced ECC Id-Based Remote Mutual Authentication Scheme for Mobile Devices*," 7th International Conference on Ubiquitous, Autonomic and Trusted Computing, pp. 116–120. http://dx.doi.org/10.1109/UIC-ATC.2010.18.

H. Debiao, C.Jianhua, and H.Jin (2012) "*An Id Based Client Authentication with Key Agreement Protocol for Mobile Client Server Environment on ECC with Provable Security*," Information Fusion, Elsevier, Vol. 13:3, pp. 223-230. http://dx.doi.org/10.1016/j.inffus.2011.01.001.

H. Debiao, C. Yitao, C.Jianhua (2013) "*An Id-Based Three-Party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography for Mobile-Commerce Environments*," Arabian Journal for Science and Engineering, Vol. 38:8, pp. 2055-2061.

J. Yang, C. Chang (2009) "*An Id-Based Remote Mutual Authentication with Key Agreement Protocol for Mobile Devices on Elliptic Curve Cryptosystem*," *Computers and Security*, Vol. 28, pp. 138–143.

E. Yoon, K. Yoo (2009) "*Robust Id-Based Remote Mutual Authentication with Key Agreement Protocol for Mobile Devices on ECC*," in: 2009 *International Conference on Computational Science and Engineering,* Vancouver, Canada, pp. 633–640.

Sheetal Kalra, Sandeep K.Sood (2010) "Advanced Password Based Authentication Scheme for Wireless Sensor Networks," *Journal of Information Security and Applications*, Elsevier, In press. http://dx.doi.org/10.1016/j.jisa.2014.10.008.

Z.H. Shen (2008) “*A New Modified Remote User Authentication Scheme Using Smartcards*,” Applied Mathematics, Vol. 23:3, pp. 371–376.

H. L. Yeh, T. H. Chen and W.K. Shih (2013) “*Robust Smart Card Secured Authentication Scheme on Sip Using Elliptic Curve Cryptography*,” *Computer Standards & Interfaces*, Elsevier, In press. http://dx.doi.org/10.1016/j.csi.2013.08.010.

Y.L. Jia, A.M. Jhou, M.X. Gao (2008) “A New Mutual Authentication Scheme Based on Nonce and Smartcards,” *Computer Communications*, Vol. 31:10, pp. 2205–2209. http://dx.doi.org/10.1016/10.1016/j.comcom.2008.02.002.

T.Y. Chen, M.S. Hwang, C.C. Lee, J.K. Jan (2009) “*Cryptanalysis of A Secure Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environment*,” Fourth International Conference on Innovative Computing, Information and Control (ICICIC), Kaohsiung, Taiwan, China, pp. 725–728.

Khan, M.K., Kim, S.K. and Alghathbar, K. (2011) “*Cryptanalysis and Security Enhancement of a More Efficient & Secure Dynamic ID-Based Remote User Authentication Scheme*,” Computer Communications, Vol. 34, pp. 305-309. http://dx.doi.org/10.1016/j.comcom.2010.02.011.

Z. Gao, Y. Tu (2008) “*An Improvement of Dynamic Id-Based Remote User Authentication Scheme with Smart Cards*,” Proceedings of the 7th World Congress on Intelligent Control and Automation, Vol. 8, June 25–27, Chongqing, China, pp. 4562–4567.

Yoon E., Yoo K (2011) “*Robust Biometric-Based Three-Party Authenticated Key Establishment Protocols*,” Int. J. Comput. Math., Vol. 88:5, pp. 1144–1157. http://dx.doi.org/10.1080/00207160.2010.496851.

D. He, D. Wang (2014) “*Robust Biometric-Based Authentication Scheme for Multiserver Environment*,” IEEE Systems Journal, Vol. PP:99, pp 1-8.

Miller, V.S. (1986) “*Use of Elliptic Curves in Cryptography*”, In: Advances in cryptology. Proceedings of CRYPTO’85, 417–26.

Koblitz N (1987) “*Elliptic Curve Cryptosystem*. Math. Comput, 48, pp.203–209.

H. Debiao, J.Chen, and R. Zhang (2011) “*An Efficient Identity Based Blind Signature Scheme Without Using Bilinear Parings*,” Computers and Electrical Engineering, Elsevier Vol. 37:4, pp. 444-450. http://dx.doi.org/10.1016/j.compeleceng.2011.05.009.

S. Pohlig, M. Hellman (1978) “*An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance*,” IEEE Transactions on Information Theory, Vol. 24, pp. 106–110. http://dx.doi.org/10.1109/TIT.1978.1055817.

J. M. Pollard (1978) “*Monte Carlo Methods for Index Computation* (mod p),” Mathematics of Computation, Vol. 32:143, pp. 918–924. http://dx.doi.org/10.2307/2006496.

P. C. van Oorschot, M. J. Wiener (1999) “Parallel Collision Search With Cryptanalytic Applications,” *Journal of Cryptology*, Vol. 12:1, pp. 1–28.

D. Boneh, R. Lipton (1996) “*Algorithms for Black-Box Fields and their Applications to Cryptography*,” Advances in Cryptology—CRYPTO ’96, LNCS, Springer-Verlag, Vol. 1109, pp. 283–297.

V. Shoup (1997) “*Lower Bounds for Discrete Logarithms and Related Problems*,” Advances in Cryptology–Eurocrypt ’97, LNCS, SpringerVerlag, Vol. 1233, pp. 256-266.

Juang, W.S. et al. (2008) “*Robust and Efficient Password Authentication Key Agreement Using Smart Cards*,” IEEE Transactions on Industrial Electronics, vol. 55:6, pp. 2551-2556. http://dx.doi.org/10.1109/TIE.2008.921677.

Hankerson, D., Menezes, A Vanstone., S. (2004) “*Guide to Elliptic Curve Cryptography*. Springer, New York.