# A Survey of Two-Party Password Authentication Key Exchange

Namita Raghuwanshi, Prof. Amit Saxena
Truba Institute of Engg. & Technology,
Bhopal, India

**Abstract**— Security in computers is information protection from unauthorized or accidental disclosure while the information is in transmission and while information is in storage. Authentication protocols provide two entities to ensure that the counterparty is the intended one whom he attempts to communicate with over an insecure network. These protocols can be considered from three dimensions: type, efficiency and security. Password Authenticated Key Exchange (PAKE) protocols facilitate two entities to consent on an ordinary session key based on a pre-shared human memorable password. The most important security goal of these protocols is providing security against password guessing attacks. Recently, In 2010 R. Song [1] proposed advanced smart card based password authentication protocol with such non-tamper resistant smart card based on symmetric key cryptosystem as well as modular exponentiation. R. Song et al method is defenseless to the offline password attack, forward secrecy, insider attack and denial of service attack are cryptanalysis by W B Horng [2]. Here in this paper we will survey on different protocols implemented based on two password authentication and a brief review is given based on different techniques.

Index Terms— Authentication, key exchange, PAKE, private key, security, attacks, encryption.

.

## 1 INTRODUCTION

As long as secure communication over insecure open networks has been a great concern for researchers. For the duration of modern years, cryptographic approaches have been concerned to remove these problems. Among these approaches, Password Authenticated Key Exchange (PAKE) protocols have been played a vital role in providing secure communications. PAKE protocols consent a client and a server to authenticate each other and engender a strong common session key through a pre-shared human memorable password over an insecure channel.

Two-party password-based authenticated key exchange (two-PAKE) protocol is quite valuable for client-server architectures. However, in large-scale client-client communication environments where a user wants to communicate with numerous other users, Two-PAKE protocol is very problematic in key management that the number of passwords that the user would need to remember.

Security in computers is information defense from unconstitutional or unintentional exposé while the information is in transmission and while information is in storage.

Authentication protocols make available two entities to make sure that the counterparty is the intended one whom he attempts to communicate with over an anxious network. These protocols can be considered from three dimensions: type, efficiency and security.

In general, there are two types of authentication protocols, the password-based and the public-key based. In a password based protocol, a user registers his account along with password to a remote server. Afterward, he can admittance the remote server if he can prove his information of the password. The server usually maintains a password or verification table but this will make the system easily subjected to a stolen-verifier attack. To deal with this problem, recent studies suggest an approach without any password or verification table in the server. Furthermore, to enhance password protection, modern studies also introduce a tamper-resistant smart card in the user end. In a public key-based system, a user should register himself to a trust party, named KGC (Key Generation Center) to obtain his public key and equivalent private key. Then, they can be recognized by a network entity through his public key. To simplify the key management, an identity-based public-key cryptosystem is usually adopted, in which KGC issues user ¡s ID as public key and computes corresponding private key for a user.

Considering computational efficiency in an authentication protocol, researchers employs low computational techniques encryptions rather than much expensive computation like asymmetric key encryptions (i.e., RSA, ECC, ElGamal, and bilinear pairings). As considering communication effectiveness, it usually to reduce the number of passes (rounds) of a protocol since the round efficiency is more significant than the computation efficiency. The most important dimension of an authentication protocol is its protection, and it should guarantee secure communications for any two legal entities over an insecure network. Attackers easily eavesdrop, modify or intercept the communication messages on the open network. Hence, an authentication protocol should withstand various attacks, such as password guessing attack, replay attack, impersonation attack, insider attack, and man-in-the-middle attack. In all types of attacks, off-line password guessing attacks are the most liberal ones for an attacker. Undetectable on-line password guessing attacks are less critical than offline attacks. But, a secure 3PEKE protocol should normally resist both types of un-detectable attacks. In this paper we try to handle both offline and online attack.

Most password-based user authentication systems place total trust on the authentication server where passwords or easily derived password verification data are stored in a central database. These systems could be easily compromised by offline dictionary attacks initiated at the server side. Conciliation of the authentication server by either outsiders or insiders subjects all user passwords to exposure and may have serious problems. To overcome these problems in the single server system many of the systems has been proposed such as multi server systems, public key cryptography and password systems, threshold password authentication systems, two server password authentication systems.

**Two Servers Password Authentication**

Two server authentication mechanisms are considered to be secure for authenticating a user in Internet based environment. As the number of services provided online is day by day increasing, users intending to use various online services are also increasing. With each service requiring the user to register separately, the overhead of remembering many user (Identity) ID /password pairs has lead to the problem of memorable. In this paper, proposed a two-server password authenticated key agreement mechanism using password where the user needs to recognize his secret key. The practical two-server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries.

**Quantum Channel for Two Server Password Authentication**

In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanism to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious quantum bits. This work study provides a pattern of integrating the classical key verification with the quantum mechanism employed in distributing the session key and provide efficient password sharing between the two servers to make the password authentication more robust.

The quantum based two server password authentication process flow diagram presented and explains our structure of two server password scheme deployed using the quantum key model to efficiently store user password in the internet applications. The service server (SS) is the end at which user interacts for the password authentication process. The service server communicates with the control server (CS) for the split portion of the password stored, to authenticate the exact user password. Quantum state verification enhances the security of communication between SS and CS. The key operation at the control server undergoes verification for quantum state authenticity. The encoded block sent from SS gets decoded to separate the quantum state and data portions for exact user password authentication.

Password based user authentication systems are low cost and easy to use. A user only needs to memorize a short password and can be authenticated anywhere, anytime, regardless of the types of access devices he/she employs. Password based authentication system

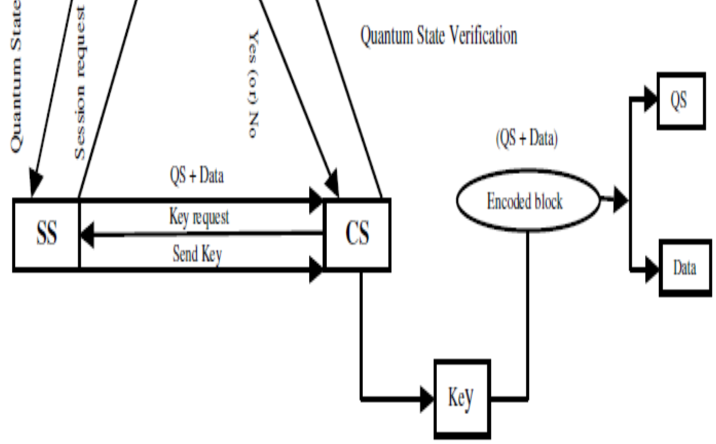

Figure 1: Process Flow Diagram for Quantum Based Two Server Passwords Authentication (SS-service server, CS-control server)

The best example of this two factor authentication system is our current ATM system, in which the ATM card is one factor and the PIN number is another factor. So if the ATM card is lost means, the authentication functionality will be disabled. As far as biometrics is concerned, the security is very effective and efficient in this system but the only concerns are the cost of hardware and software complexity.

The server is compromised by means of an offline dictionary attack. In recent years, much attention has focused on designing password based authenticated key exchange protocols which can resist any kind of intruder's attack. To solve this problem, a new kind of authentication structure called the multiple server authentications was proposed. In such schemes, the capability of verifying a password is split between two or more servers, and more than a certain threshold number of servers need to collude to recover the password. Till now, few multiple server schemes were proposed. In these multiple server authentication settings, the two-server authentication protocol is the simplest and the most acceptable to users.

**ONE TIME PRIVATE KEY**

Although there are various techniques implemented that are needed for the secure transmission of data from the sender to the receiver. During the transmission of data from the sender to the receiver security plays an important role because the chances of attacks in the network are more. Hence to overcome these limitations there are security techniques implemented for the secure transmission of data. Authentication is also one of the technique through which the data can be send securely.

One such concept of providing a strong authentication is using key generation using one time private key. As we know that key is important part for the authentication of the data where the sender and receiver uses his own key for the authentication, but if these keys can't be made strong then such techniques is not a secure one [10]. In the concept of key generation using OTPK during the generation of key by the sender or receiver or by any third party a key is generated for the authentication or for the encryption of the data or for the decryption a key is used and as soon as the sender and the receiver get's authenticated and data is send securely the key gets destroyed.

## 2 BACKGROUND

Providing secure communication over insecure open networks has been a great concern for researchers. During recent years, cryptographic approaches have been applied to remove these problems. Among these approaches, Password Authenticated Key Exchange (PAKE) protocols have been played an essential role in providing secure communications. PAKE protocols permit a client and a server to authenticate each other and generate a strong common session key through a pre-shared human memorable password over an insecure channel.

Password-Authenticated Key Exchange (PAKE) enables two communication entities to authenticate each other and establish a session key via easily memorable passwords. The first PAKE protocol was introduced by Bellovin and Merritt in 1992 known as Encrypted Key Exchange (EKE).

Two-party password-based authenticated key exchange (two-PAKE) protocol is quite useful for client-server architectures. However, in large-scale client-client communication environments where a user wants to communicate with many other users, Two-PAKE protocol is very inconvenient in key management that the number of passwords that the user would need to remember. Gong, Lomas, Needham, and Saltzer proposed a three-party password-based key transfer protocol using server's public key. Later, Steiner, Tsudik and Waider proposed a three-party PAKE (three-PAKE) protocol between two clients without server's public key. Wang and Mo also proposed an improved method to withstand this attack.

Security in computers is information protection from unauthorized or accidental disclosure while the information is in transmission and while information is in storage. Authentication protocols provide two entities to ensure that the counterparty is the intended one whom he attempts to communicate with over an insecure network. These protocols can be considered from three dimensions: type, efficiency and security.

In general, there are two types of authentication protocols, the password-based and the public-key based. In a password based protocol, a user registers his account and password to a remote server. Later, he can access the remote server if he can prove his knowledge of the password. The server usually maintains a password or verification table but this will make the system easily subjected to a stolen-verifier attack. To address this problem, recent studies suggest an approach without any password or verification table in the server. Moreover, to enhance password protection, recent studies also introduce a tamper-resistant smart card in the user end. In a public key-based system, a user should register himself to a trust party, named KGC (Key Generation Center) to obtain his public key and corresponding private key. Then, they can be recognized by a network entity through his public key. To simplify the key management, an identity-based public-key cryptosystem is usually adopted, in which KGC issues user ¡s ID as public key and computes corresponding private key for a user.

Password-based authenticated key exchange (PAKE) protocols enable two users to generate a common, cryptographically-strong key based on an initial, low-entropy, shared secret (i.e., a password). The difficulty in this setting is to prevent off-line dictionary attacks where an adversary exhaustively enumerates potential passwords on its own, attempting to match the correct password to observed protocol executions. Roughly, a PAKE protocol is secure if off-line attacks are of no use and the best attack is an on-line dictionary attack where an adversary must actively try to impersonate an honest party using each possible password. On-line attacks of this sort are inherent in the model of password-based authentication; more importantly, they can be detected by the server as failed login attempts and defended against. Protocols for authenticated key exchange enable two parties to generate a shared, cryptographically strong key while communicating over an insecure network under the complete control of an adversary. Such protocols are among the most widely used and fundamental cryptographic primitives; indeed, agreement on a shared key is necessary before higher-level tasks such as encryption and message authentication become possible. Password-based authenticated key exchange (PAKE) protocols enable two users to generate a common, cryptographically-strong key based on an initial, low-entropy, shared secret (i.e., a password). The difficulty in this setting is to prevent off-line dictionary attacks where an adversary exhaustively enumerates potential passwords on its own, attempting to match the correct password to observed protocol executions.

Roughly, a PAKE protocol is secure if off-line attacks are of no use and the best attack is an on-line dictionary attack where an adversary must actively try to impersonate an honest party using each possible password. On-line attacks of this sort are inherent in the model of password-based authentication; more importantly, they can be detected by the server as failed login attempts and defended against.

A random password generator is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using simple sources of randomness such as dice or coins, or they can be generated using a computer. While there are many examples of "random" password generator programs available on the Internet, generating randomness can be tricky and many programs do not generate random characters in a way that ensures strong security.

A common recommendation is to use open source security tools where possible, since they allow independent checks on the quality of the methods used. Note that simply generating a password at random does not ensure the password is a strong password, because it is possible, although highly unlikely, to generate an easily guessed or cracked password. A password generator can be part of a password manager. When a password policy enforces complex rules, it can be easier to use a password generator based on that set of rules than to manually create passwords. In situations where the attacker can obtain an encrypted version of the password, such testing can be performed rapidly enough so that a few million trial passwords can be checked in a matter of seconds.

The function rand presents another problem. All pseudorandom number generators have an internal memory or state**.** The size of that state determines the maximum number of different values it can produce; an n-bit state can produce at most 2n different values. On many systems rand has a 31 or 32 bit state, which is already a significant security limitation. Some computer operating systems provide much stronger random number generators.

Most password-based user authentication systems place total trust on the authentication server where passwords or easily derived password verification data are stored in a central database. These systems could be easily compromised by offline dictionary attacks initiated at the server side. Compromise of the authentication server by either outsiders or insiders subjects all user passwords to exposure and may have serious problems. To overcome these problems in the single server system many of the systems has been proposed such as multiserver systems, public key cryptography and password systems, threshold passowrd authentication systems, two server password authentication systems.

The proposed work continues the line of research on the two-server paradigm extend the model by imposing different levels of trust upon the two servers, and adopt a very different method at the technical level in the protocol design. As a result, they propose a practical two server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries. A hash function is a well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array (associative array). The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes. Hash functions are mostly used to speed up table lookup or data comparison tasks such as finding items in a database, detecting duplicated or similar records in a large file, and finding similar stretches in Distributed Network Application.

A hash function may map two or more keys to the same hash value. In many applications, it is desirable to minimize the occurrence of key collisions, which means that the hash function must map the keys to the hash values as evenly as possible. Therefore, each slot of a hash table is associated with (implicitly or explicitly) a set of records, rather than a single record. The hash function must be as insensitive as possible to data capture or transmission errors, and to "trivial" changes such as timing and volume changes, compression, etc.

These pseudo random and hash function password systems could be easily compromised by offline dictionary attacks initiated at the server side. Compromise of the authentication server by either outsiders or insiders, subjected to all user passwords exposed and may have serious problems. To overcome these problems in the single server system many schemes were proposed such as multi server systems, public key cryptography and password systems, threshold password authentication systems, two server password authentication systems.

## 3 RELATED WORK

In 2012 a simple and intuitive model for expressing the semantics of privacy-friendly authentication and accountability technologies such as anonymous credentials systems and verifiable encryption. It allows for expressing the precise relations as well as the authentication and accountability properties between parties. The concepts cover in the model comprises pseudonyms, attribute-based authentication, as well as conditional release of information. As a result, the model can express the relevant primitives for privacy-preserving authentication and accountability at the same time [3].

Many standards exist for authentication, ranging from simple static passwords stored on a single machine to complicated distributed systems. Organizations concerned about protecting their digital assets from sophisticated cyber attacks have begun relying on two-factor authentication as a defense against unauthorized access [4].

These protocols were proven secure in the random oracle model. Katz, Ostrovsky, and Yung (KOY) [5] demonstrated the first efficient PAKE protocol with a proof of security in the standard model.

It also achieves mutual authentication in three rounds. In their work [6], Groce and Katz mentioned their framework will significantly improve efficiency when basing the protocol on lattice assumptions. Katz and Vaikuntanathan [7] first instantiated the KOY/GL PAKE protocol under lattice assumptions. The most technically complex characteristic of their work is the construction of a lattice-based CCA-secure encryption scheme with an associated approximate smooth projective hash system. In order to plug into the JG/GK's structure, we use an approximate lattice-based SPH and an error correcting code (ECC) to do the job of an exact lattice-based SPH.

In 2012 by Wang, Y.G. [8] observed that the previous papers in this area present attacks on protocols in previous papers and propose new protocols without proper security justification (or even a security model to fully identify the practical threats), which contributes to the main cause of the above failure. Consequently, Wang offered three kinds of security models, specifically Type I, II and III, and further planned four concrete schemes, only two of which, i.e. PSCAb and PSCAV, are claimed to be secure under the harshest model, i.e. Type III security model. The type III model will be reviewed later in Section 2. However, PSCAb requires Weil or Tate pairing operations to defend against offline guessing attack and may not be suitable for systems where pairing operations are considered to be too expensive or infeasible to implement. Moreover, PSCAb suffers from the well-known key escrow problem and lacks some desirable features such as local password update, reparability and user anonymity. As for PSCAV, in Appendix B, we will demonstrate that it still cannot achieve the claimed security goals and is vulnerable to an offline password guessing attack and other attacks under the Type III security model [8].

In 2011 a password based authentication using Elliptic Curve Cryptography (ECC) for smart card. Since the secret key of the AS is a long-term key, it requires further security. When the secret key of the AS is compromised, the entire operation of the AS will be disrupted. It is necessary to replace or alter the long term secret key [9].

Password-authenticated secret sharing (PASS) methods, first commenced by Bagherzandi et al. at CCS 2011, permit users to allocate data among several servers so that the data can be recovered using a single human-memorizable password, but no single server (or even no collusion of servers up to a certain size) can mount an off-line dictionary attack on the password or learn anything about the data. Further in 2012 present a concrete 2PASS protocol and prove that it meets our definition. Given the strong safety measures guarantees, our protocol is amazingly proficient: in its most efficient instantiation under the DDH assumption in the random oracle model [10].

In 2011 the TW-KEAP is an efficient protocol for sharing a session key to protect communication in an insecure network. It is based on the concept of the Diffie-Hellman key exchange protocol which allows the key exchange without session key appearing in the message. The TW KEAP could support lawful interception because the corresponding server is involved in the key exchange procedure to derive the session key [11].

In 2011, Maryam Saeed has recommended a new two party validation protocol without the server's public key in which the limitations of PAKE1 and PAKE2 protocols has been overcome and new authentication protocols has been implemented which can provide several security attributes while it has a remarkable computational efficiency and lower number of rounds [12].

In [12], it is proved that the Hitchcock et al.'s protocol is exposed to momentary key compromise masquerade, Key Compromise Impersonation (KCI) attacks and off-line dictionary while it does not provide the mutual authentication and forward secrecy attributes. It is also shown that SPAKEI and SPAKE2 protocols are vulnerable to password compromise impersonation and Denial-of-Service (DoS) attacks while they do not provide the mutual authentication property. To remove the above disadvantages, an efficient secure two-party P AKE protocol is designed to provide several securities attributes while the efficiency is also improved.

In 2010 Songs projected extremely recently a password-based authentication and key establishment protocol using smart cards which attempts to solve some weaknesses [1] found in a previous scheme suggested by Xu, Zhu, and Feng [13].

In 2009, Lee et al. showed that Juang et al.'s design is not protected against stolen-verifier attack. Furthermore, Juang's method does not convince the user anonymity. To solve this problem, Kyungkug Kim proposed an improved anonymous authentication and key exchange proposal. Then, we demonstrate that the offered scheme is safe and sound against various well-known attacks [14].

## 4 SECURITY ANALYSIS

The security analysis is discussed with respect to the security features which the proposed protocol should satisfy. It is desirable for a two-party P AKE protocol to possess the following security attributes [15]:

a. **Forward secrecy:** If the user's password or the server's private key is divulged, the secrecy of previously established session keys should not be revealed.

b. **Known session key security:** Disclosure of one session key should not reveal other session keys.

c. **Resilience to Denning-Sacco attack:** Disclosure of session key should not enable an attacker to calculate or guess the password.

d. **Resilience to password compromise impersonation attack:** Password compromise of any user A should not enable an attacker to share any session key with A by impersonating himself/herself as any other entity.

e. **Resilience to Unknown Key Share (UKS) attack:** User A should not be coerced into sharing a key with an attacker while he thinks that his key is shared with another user B.

f. **Resilience to off-line dictionary attack:** If an attacker could guess a password, he should not be able to check his guess offline.

g. **Resilience to undetectable on-line dictionary attack:** If the attacker could guess a password in an on-line transaction, he should not be able to check the correctness of his guess by using responses from the server and the server is also able to detect an honest request from a malicious request.

h. **Resilience to replay attack:** An attacker or originator, who captured the exchanged data, should not be able to reuse it maliciously.

i. **Resilience to ephemeral key compromise impersonation attack:** Disclosure of the ephemeral key of any user A should not enable adversary to share session key with A by impersonating any other participant.

j. **Resilience to Key Compromise Impersonation (KCI) attack:** Disclosure of the user A's private key should not enable the attacker to masquerade as other participants to A.

k. **Resilience to malicious server attack:** If an attacker runs on a malicious server and tempts people to register with that server, he/she must not be capable to acquire the passwords of users and impersonate himself/herself as users in login to another server.

l. **Resilience to man-in-the-middle attack:** The attacker captures and changes the transferred messages between the user and server while two participants are unaware of being attacked by the attacker.

## 5 CONCLUSION

Here in this paper we will provide the literature survey on the basis of different PAKE techniques and the different ways of providing authentication to the user. We will only provide the survey of the work that had been done so far. In the next step we provide the simulation of the proposed work in the PAKE technique and analyze on the basis of different parameters.
This is just an overall survey of what we have studied so far regarding different authentication techniques. In the next paper we implement an efficient algorithm for password authentication using one time private key which provides more security features as compared to the other existing techniques of authentication.

## REFERENCES

[1] Juan E. Tapiador, Julio C. Hernandez-Castro, "Cryptanalysis of Song's advanced smart card based password authentication protocol", 2010.
Online available: http://arxiv.org/pdf/1111.2744.pdf

[2] W B Horng and Cheng p Lee, 2010 "Security weaknesses of song's advanced smart card based Password authentication Protocol", IEEE International Conference on Informatics and Computing (PIC), pp. 477-480, 2010 .

[3] Patrik Bichsel, Jan Camenisch, "A Calculus for Privacy friendly Authentication", Proceedings of the 17th ACM symposium on Access Control Models and Technologies, pp. 157-166, 2012.

[4] Matthew A. Ezell, Gary L. Rogers, "A Framework for Federated Two-Factor Authentication Enabling Cost Effective Secure Access to

Distributed Cyberinfrastructure", Proceedings of the 1st Conference of the Extreme Science and Engineering Discovery Environment: Bridging from the eXtreme to the campus and beyond, article no 7, 2012.

[5] J. Katz, R. Ostrovsky, and M. Yung "Efficient and Secure Authenticated Key Exchange Using Weak Passwords". Journal of the ACM, Vol. 57, issue 1, pp. 78–116, 2009.

[6] A. Groce, J. Katz "A New Framework For Efficient Password-based Authenticated Key Exchange", In proceedings of 17th ACM Conference on Computer and Communications Security, pp. 516–525. ACM Press, New York, 2010.

[7] J. Katz and V. Vaikuntanathan "Password-based Authenticated Key Exchange Based on Lattices", In Advances in Cryptology, volume 5912 of LNCS, pp. 636–652. Springer, 2009.

[8] Wang, Y.G.: "Password protected smart card and memory stick authentication against off-line dictionary attacks". Information Security and Privacy Research IFIP Advances in Information and Communication Technology, vol. 376, pp. 489–500. Springer Boston, 2012. Available at http://coitweb.uncc.edu/ yonwang/papers/smartcard.pdf.

[9] Amutha Prabakar Muniyandi, Rajaram Ramasamy, "Password Based Remote Authentication Scheme using ECC for Smart Card", Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 549-554, 2011.

[10] Jan Camenisch, Anna Lysyanskaya, "Practical Yet Universally Composable Two-Server Password Authenticated Secret Sharing", Proceedings of the 2012 ACM conference on Computer and communications security, pp. 525-536, 2012.

[11] Wei-Kuo Chiang and Jian-Hao Chen, "TW-KEAP: An Efficient Four-Party Key Exchange Protocol for End-to-End Communications", Proceedings of the 4th international conference on Security of information and networks, pp. 167-174, 2011.

[12] Maryam Saeed, Hadi Shahriar Shahhoseini, "An Improved two-party Password Authenticated Key Exchange Protocol without Server's Public Key", IEEE 3rd International Conference on Communication Software and Networks (ICCSN-2011), pp. 90-95, 2011.

[13] J. Xu, W.-T Zhu, and D.-G Feng. "An improved smart card based password authentication scheme with provable security." Computer Stan- dards & Interfaces 31, pp. 723–728, 2009.

[14] Kyung-kug Kim, "An Improved Anonymous Authentication and Key Exchange Scheme", Proceedings of the CUBE International Information Technology Conference, pp. 740-743, 2012.

[15] M. Saeed, H.S. Shahhoseini, "APPMA - An Anti-Phishing Protocol with Mutual Authentication", Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC20 10), pp. 308-313, June. 2010.