# Performance Analysis Of 3pek Exchange Protocol Using Parallel Message Transmission Technique

[1]P.Rajkumar, [2]C.Manoharan and [3]M.Ananthi
[1,3]Department of Computer Science and Engineering,
INFO Institute of Engineering, Coimbatore, Tamil Nadu, India.
[2]Department of Mechanical Engineering,
Annai Mathammal sheela Engineering College, Tamil Nadu, India.

**Abstract**

*This paper presents the Performance analysis of three party Encrypted key exchange protocol using parallel message transmission Technique. Three party Encrypted key exchange protocol was proposed and it was claimed to be secure and efficient practically. An undetectable online password guessing attack on the above protocol was demonstrated and it has overridden the claim of three party key exchange protocols. Parallel message transmission protocol has been proposed to eliminate undetectable online password guessing attack.*

***Keywords****: parallel message transmission, 3PEKE.*

## 1. Introduction

In Cryptography, a password-authenticated key agreement is an interactive method for two or more parties to communicate. The key exchange protocol is one of the most elegant ways of establishing secure communication between pair of users by using the session key. The session key which is exchanged between two users, assures the secure communication for later sessions. In the line of key exchange protocol development, password based key exchange mechanism achieved attention due to its simplicity and wide range of applicability, as it requires the users to remember the password. Such protocol should not be vulnerable to any type of off-line, undetectable or detectable on-line password guessing attacks, since the passwords are of low entropy. The password guessing attacks can be divided into three classes, namely

- Detectable on-line password guessing attacks
- Undetectable on-line password guessing attacks
- Off-line password guessing attacks.

Such password guessing attacks are undesirable in communication network and it reduces the network efficiency, for that intensive research work has been undertaken in the development of secure and efficient key exchange protocol.

## 2. Literature review

The review of Literature given in this section is centered upon various key exchange protocols for secured communication. Since the first proposal of Bellovin and Merrit (1992) Password Authenticated Key Exchange (PAKE), many efficient key exchange protocols based on password have been developed. The two party key exchange protocols were extended to three party, in which the two parties initially communicate the passwords with the trusted server securely. Later the server authenticates the client when they want to agree upon a session key. The three party protocol is introduced by Steiner et al

(1995). Subsequently Ding and Hoster (1995) published on-line and off-line guessing attacks on Steiner's protocol. Later Lin et al (2001) proposed two versions of improved three party protocol one with server's public key and another without.

Chang and Chang (2004) proposed a novel three party encrypted key exchange protocol without server public key and claimed the protocol is secure, efficient and practical. Unlike their claims, Yoon and Yoo (2008) pointed out an Undetectable on-line password guessing attack on their protocol, in which one party is able to know the other party's password and furthermore they presented an improved version of it to avoid the above attacks. Lo and Yeh (2009) pointed out undetectable password guessing attack on Yoon and Yoo protocol and proposed an enhanced protocol. But the enhanced protocol falls to Undetectable On-line password guessing attack, if client 'B' intercepts the message coming from client A'. To eliminate this Undetectable on-line password guessing attack, an extension is done on the existing protocol.

## 3. Objective of this study

1. To design a Key exchange protocol which is in-vulnerable to undetectable on-line password attack with reduced transmission round for secured communication.
2. To fabricate parallel message transmission technique that achieves better performance efficiency by requiring fewer transmission rounds.
3. To design three party key exchange protocols that does not use server's public key.
4. To verify that the protocol is secure, efficient and practical, with reduced modular exponential operation on server side.

## 4. Motivation

Over recent year's cryptography have become popular tremendously. A password authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password. In the most stringent password-only security models, there is no requirement for the user of the method to remember any secret or public data other than the password. Password Authenticated Key Exchange (PAKE) is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of message, such that an unauthorized party (one who controls the communication channel but does not possess the password) cannot participate in the method and is constrained as much as possible from guessing the password. Two forms of PAKE area Balanced and Augmented methods. Balanced PAKE allows parties that use the same password to negotiate and authenticate a shared key.

Encrypted Key Exchange (EKE), PAK and PPK, SPEKE (Simple Password Exponential Key Exchange), J-PAKE (Password Authenticated Key Exchange by Juggling), Augmented PAKE is a variation applicable to client /server scenarios, in which an attacker must perform a successful brute-force attack in order to masquerade as the client using stolen server data.

Although several of the forms of EKE were later found to be flawed, the surviving, refined and enhanced forms of EKE effectively make this the first method to amplify a shared password into a shared key, where the shared key may subsequently be used to provide a Zero- knowledge password proof or other functions. In the most general form of EKE, at least one party encrypts an ephemeral (one time) public key using a password, and sends it to a second party, who decrypts it and uses it to

negotiate a shared key with the first party. Steiner et al (1995) proposed 3PEKE protocol. Lin et al (2000) showed that 3-PEKE suffers not only undetectable on-line password guessing attacks but also off-line password guessing attacks. Evidence indicates that key exchange protocols are vulnerable to un-detectable on-line password guessing attacks and the above forms the foundation for the works presented here.

## 5. Proposed protocol

In this section, a new protocol namely three party Encrypted key exchange protocol has been proposed and it is implemented using parallel message transmission technique. In the Encrypted key exchange protocol each participant only shares a password in advance with the trusted server that helps any two participants to establish a session key. Parallel message transmission mechanism is to achieve fewer transmission rounds where two clients make request to the server simultaneously and the server responds to both the clients' parallely (i.e. A→S and B→S).

There are four steps in the proposed protocol.

**Step 1:**

Client A generates two random numbers $R_A$ and $r_A$,and calculates $E_{pwA}(K_{AS}\oplus N_A)$, $F_S(N_A\oplus ID_A)$ and $f_{KAS}(N_A)$, where $N_A=g^{RA}$ (mod p) and $K_{AS}=N_A^{rA}$ (mod p). Next, A sends these three messages to S via his/her own private communication channel.

A→S: $ID_A$, $ID_B$, $ID_S$, $E_{pwA}(K_{As}\oplus N_A)$, $F_S(N_A\oplus ID_A)$, $f_{KAS}(N_A)$.

Meanwhile, client B calculates $N_B=g^{RB}$(mod p), $K_{BS}=N_B^{rB}$ (mod p), $E_{pwB}(K_{BS}\oplus N_B)$, $F_S(N_B\oplus ID_B)$ and $f_{KBS}(N_B)$ with two newly generated random numbers $R_B$ and $r_B$. Then, B transmits $E_{pwB}(K_{BS}\oplus N_B)$, $F_S(N_B\oplus ID_B)$ and $f_{KBS}(N_B)$ to S via his/her own private communication channel.

B→S: $ID_A$, $ID_B$, $ID_S$, $E_{pwB}(K_{BS}\oplus N_B)$, $F_S(N_B\oplus ID_B)$, $f_{KBS}(N_B)$.

Here Client A and B communicates with the server S parallely.

**Step 2:**

Once receiving the message sent from A and B , S first utilizes a trapdoor to obtain $N_A\oplus ID_A$ and $N_B\oplus ID_B$ from $F_S(N_A\oplus ID_A)$ and $F_S(N_B\oplus ID_B)$ then retrieves $N_A=N_A\oplus ID_A\oplus ID_A$ and $N_B=N_B\oplus ID_B\oplus ID_B$, respectively. Next it uses the passwords $pw_A$ and $pw_B$ and decrypts $E_{pwA}(K_{As}\oplus N_A)$ and $E_{pwB}(K_{Bs}\oplus N_B)$, respectively, and gets $K_{AS}\oplus N_A$ and $K_{BS}\oplus N_B$. Now, $K_{AS}=K_{AS}\oplus N_A\oplus N_A$ and $K_{BS}=K_{BS}\oplus N_B\oplus N_B$ will be determined. $f_{KAS}(N_A)$ and $f_{KBS}(N_B)$ are computed. S verifies whether computed value $f_{KAS}(N_A)$(or $f_{KBS}(N_B)$) and received value $f_{KAS}(N_A)$ (or $f_{KBS}(N_B)$) are identical or not. If this verification holds, S continues the residual procedures of this protocol. Otherwise, S terminates this protocol at current session. Next, S computes $N_B^{RS}$, $N_A^{RS}$, and corresponding hashed credential $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$ and $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$. Finally, S sends $\{N_B^{RS}, f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})\}$ to A and $\{N_A^{RS}, f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})\}$ to B simultaneously.

S → A: $N_B^{RS}$, $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$,

S→ B: $N_A^{RS}$, $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$.

**Step 3:**

Upon obtaining the transmitted messages sent from S, B first verifies $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$ to authenticate S. If this verification is passed, B believes the received $N_A^{RS}$ is valid and then computes the session key $K=(N_A^{RS})^{RB}$ (mod p) and $f_K(ID_B, K)$. Otherwise, B terminates this protocol.

B → A: $f_K(ID_B, K)$

B sends the $f_K(ID_B, K)$ to A. Note that $f_K(ID_B, K)$ will be used by client A to verify the legality of client B and the established session key K. At the same time, A verifies $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$ to authenticate S. If this verification does not hold, A terminates this protocol. Otherwise, A

computes the session key $K=(N_B^{RS})^{RA}$ (mod p) and $f_K(ID_A, K)$.

**Step 4:**

$A \rightarrow B$: $f_K(ID_A, K)$.

Finally, A sends the $f_K(ID_A, K)$ to B. After A and B successfully examine the validation of the incoming messages $f_K(ID_B, K)$ and $f_K(ID_A, K)$, both of them can ensure that they actually share the secret session key $K=(N_B^{RS})^{RA}$ (mod p)$=(N_A^{RS})^{RB}$(mod p) at present. Otherwise, the protocol will be terminated.

**6. Performance and Analysis**

The development of an efficient protocol should take the number of transmission rounds (and steps) and the computation complexity into account. Figure 1. Shows the performance comparison analyses of the transmission round in the enhanced protocol and existing protocol. From the view point of the transmission round, the enhanced protocol adopts the parallel message transmission mechanism (i.e. A→S and B→S) to achieve fewer transmission rounds than the existing protocols (i.e. A→B→S).

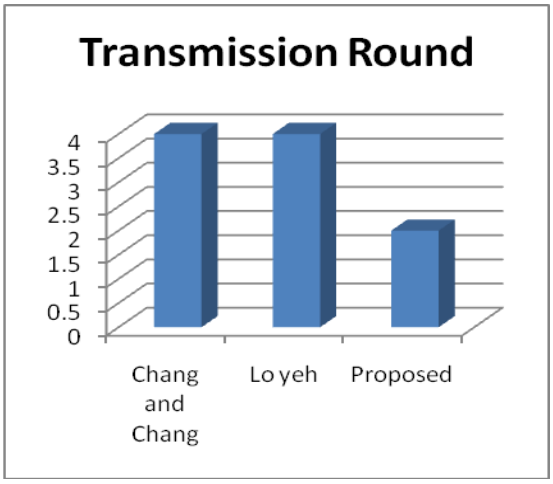


**Figure 1: Transmission round in Existing and Proposed Protocol**

The modular exponential operations are reduced since client A sends $E_{pwA}(K_{AS}\oplus N_A)$, $F_S(N_A\oplus ID_A)$, $f_{KAS}(N_A)$ to S and client B sends $E_{pwB}(K_{BS}\oplus N_B)$, $F_S(N_B\oplus ID_B)$, $f_{KBS}(N_B)$ to S. S decrypts $E_{pwA}(K_{AS}\oplus N_A)$ and $E_{pwB}(K_{BS}\oplus N_B)$ and gets $K_{AS}\oplus N_A$ and $K_{BS}\oplus N_B$ respectively. Next S extracts $N_A$ and $N_B$ from $F_S(N_A\oplus ID_A)$, $F_S(N_B\oplus ID_B)$ and $ID_A$,$ID_B$. Now, $K_{AS}$ and $K_{BS}$ $N_A\oplus N_A$ and $K_{BS}=K_{BS}\oplus N_B\oplus N_B$. Since $E_{pwA}(K_{AS}\oplus N_A)$, $F_S(N_A\oplus ID_A)$, $E_{pwB}(K_{BS}\oplus N_B)$,$F_S(N_B\oplus ID_B)$ are arranged in a proper sequence two modular exponential operations are reduced on the server side as shown in Figure 2, and hence computation complexity is reduced.

The purpose of experimental results is to show the total running time needed for the operations involved in various steps of the proposed protocol. A data set is generated for problem (p) of size 2048 bits. The steps in the protocol are: TDF, pseudorandom hash function, computing $N_A$, computing $K_{AS}$, symmetric encryption.

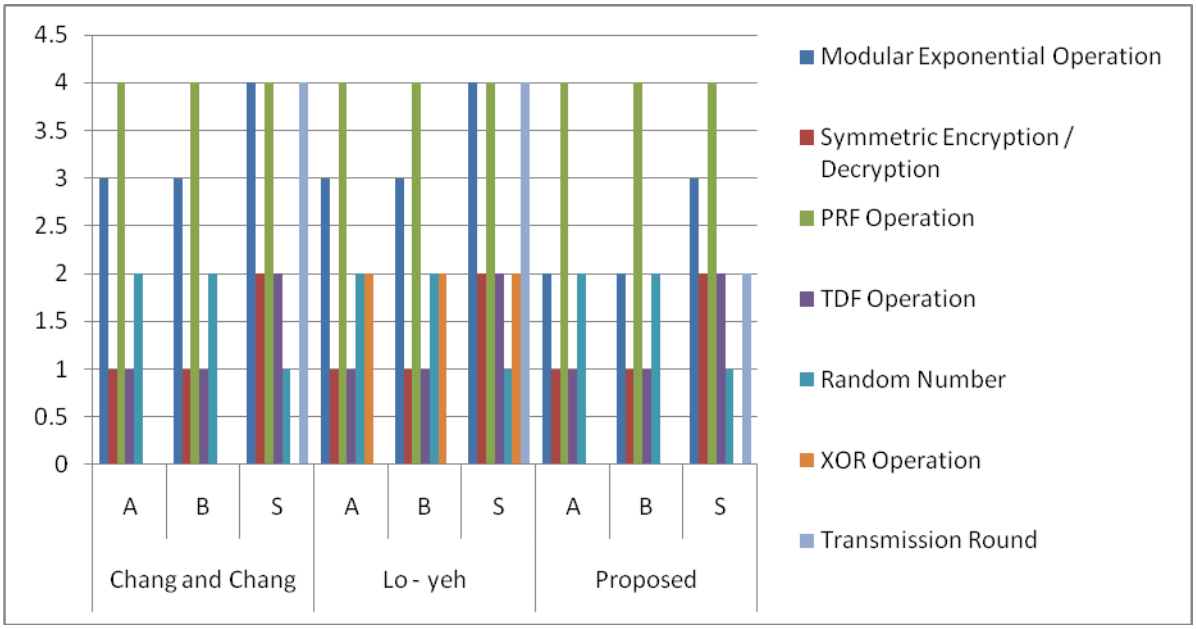


**Figure 2: Performance Analysis**

## 7. Conclusion

Parallel Message Transmission technique for encrypted key exchange protocol, which is in-vulnerable to undetectable on-line password attacks, with reduced transmission rounds has been proposed. The designed protocol is developed with reduced modular exponential operations on the server side. The protocol achieves better performance efficiency by requiring only four transmission rounds and the performance is analyzed on a set of experiments. The results show that the protocol is secure, efficient and practical.

## 8. References

**[1] K. Kobara and H. Imai.** Pretty-simple password-authenticated key exchange under standard assumptions. IEICE Transactions, E85-A (10):2229-2237, Oct. 2002

**[2] M. Abdalla and D. Pointcheval.** Simple Password-Based Encrypted Key Exchange Protocols. Proc. of Topics in Cryptology - CT-RSA 2005, LNCS 3376, pp. 191-208,

**[3] E.J. Yoon, K.Y. Yoo**. Improving the novel three-party encrypted key exchange protocol. Computer Stan-dards and Interfaces, 30, 2008, 309-314.

**[4] W. Diffie, M. Hellman**. New Directions in cryptography. IEEE Transactions on Information theory, Vol. 22, No. 6, 1976, 644-654.

**[5] Y. Ding, P. Horster**. Undetectable Online password guessing attacks. ACM operating systems Review, Vol. 29, No. 4,pp 77-86 (1995)

**[6] Rajkumar and C.Manoharan**," Parallel Message Transmission Technique for Password Key Exchange Protocol" European Journal of Scientific Research, Vol.77 No.4 (2012), pp.471-476.

**[7] Fuw-Yi Yang**, Improvement on a Trap door Hash Function, International Journal on Network Security, Vol 9, No 1, pp 17-21,(2009).