IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
www.ijiset.com
ISSN 2348 – 7968

Comparison of 3-PEKE Protocol and Improved Parallel Message Transmission Key Exchange Protocol

[1]M.Ananthi ,[2]Dr.P.Rajkumar and [3]R.Logeswari saranya

[1]Department of Computer Science and Engineering,
INFO Institute of Engineering, Coimbatore, Tamil Nadu, India.

[2] Department of Computer Science and Engineering,
INFO Institute of Engineering, Coimbatore, Tamil Nadu, India.

[3]Department of Computer Science and Engineering,
INFO Institute of Engineering, Coimbatore, Tamil Nadu, India.

Abstract

A Novel three party simple 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. Improved Parallel message transmission protocol has been proposed to eliminate undetectable online password guessing attack. This paper presents the comparison of the three party simple key exchange protocol and improved parallel message transmission key exchange protocol.

Keywords:*Parallel message transmission,password-authentication, 3PEKE, guessing attack.*

1. Introduction

In cryptography, 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. Password-authenticated key agreement generally encompasses methods such as: Balanced password-authenticated key exchange augmented password-authenticated key exchange, Password-authenticated key retrieval, Multi-server methods, and Multi-party methods. 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 messages, 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. (The optimal case yields exactly one guess per run exchange.) Two forms of PAKE are Balanced and Augmented methods. Balanced PAKE allows parties that use the same password to negotiate and authenticate a shared key. Ingeneralthepasswordguessingattackscanbedividedint othreeclassesandtheyarelisted below:

•**Detectableon-linepasswordguessingattacks:**Anattackerattemptsto useaguessedpasswordinanon-linetransaction.He/Sheverifiesthecorrectnessofhis/her guessusingtheresponse from server.Afailedguesscanbedetectedandloggedbytheserver.

• **Undetectableon-line passwordguessingattacks:**Similar toDetectableon-line passwordguessingattack,anattackertriestoverifyapasswordguessinanon-linetransaction.However, afailedguesscannotbedetectedandloggedbyserver,asserverisnotabletodistinguishan honestrequestfromamaliciousone.

•**Off-linepasswordguessingattacks**:Anattackerguessesapasswordandverifieshis/herguess offline.Noparticipationofserveris required,sotheserverdoesnotnoticetheattack. Bellowing andMeritproposed Encryptedkey exchange protocol.Later many efficient key exchange protocols based on password have been developed. Recently thesetwopartykeyexchangeprotocolsareextendedtothreeparty,inwhich,thetwo parties initiallycommunicatesthepasswordswiththe trustedserversecurely.Laterthe server authenticatestheclientswhentheywanttoagreeuponasessionkey.Steineretalproposed threepartyprotocol.LaterLinetalshowedthatSTW-3PEKEprotocolfallstoundetectable on-line passwordguessingattack,off-linepasswordguessingattacksandproposedtwoversions ofimprovedthreepartykeyexchangeprotocols.ChangandChang.proposeda novelthreepartyencryptedkeyexchangeprotocol(ECC-3PEKEprotocol)withoutserver publickeyandclaimedtheprotocolissecure,efficientand practical.UnliketheirclaimsYoon andYoopointedoutanUndetectablepasswordguessingattackontheirprotocol,inwhich one party is able to know the other party's password and furthermore they presented an improvedversionofittoavoidtheaboveattack.Akeyrecoveryattackisalsoprovedon ECC-3PEKEprotocolusingthe Undetectableonlinepasswordguessingattackproposed by YoonandYoo.This paper presents the comparison of the three party simple key exchange protocol and improved parallel message transmission key exchange protocol.

Thepaperis organizedasfollows:section2brieflyreviews the3PEKEprotocol, section 3reviewsundetectablepasswordguessingattackon3PEKEprotocol.Section4 describesthecomparison of 3PEKEprotocolandtheconcludingremarksare made insection5.

2. REVIEW OF 3PEKE PROTOCOL

This sectionbriefly explains the3PEKE protocol. The notationsusedinthisprotocol arelistedbelow:

A,B : two communication parties

S: the trusted server

ID_A, ID_B, ID_S: the identities of A,B and S, respectivelyPW_A,PW_B: the passwords securely shared by A with S and B

EPW(.):a symmetric encryption scheme with a password PW

r_A, r_B: the random numbers chosen by A and B, respectively

p: a large prime,

g : a generator of order p – 1

R_A,R_B,R_S: the random exponents chosen by A,B and S, respectively.

N_A,N_B :NA=g^{RA}(mod p)and N_B=g^{RB}(mod p)

F_S(.):the one-way trapdoor hash function(TDF) where only S knows the trapdoor

f_K(.): the pseudo-random hash function (PRF) indexed by a key K

K_{AS},K_{AS}: a onetime strong keys shared by A with S and B with S, respectively.

The procedure followed in ECC-3 PEKE protocol is given below:

Step 1: A→B:

{ID_A, ID_B, ID_S,E_{PWA}(NA), F_S(rA),f_{KAS} (NA)}

User A chooses a random integernumber r_A and a random exponent $R_A \epsilon_R Z^*_p$, and then computes $N_A = g^{RA}$ and $K_{AS} = N_A{}^{RA}$.Then, A encrypts N_A by using his/her password PW_A like E_{PWA}, (N_A) and computes two hashvalues $F_S(r_A)$ and $f_{KAS}(N_A)$. Finally, Asends ID_A,ID_B,ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, f_{KAS} (N_A) }to B.

Step2: B→S:

{ID_A,ID_B,ID_S,$E_{PWA}(N_A)$,$F_S(r_A)$,$f_{KAS}(N_A)$,$E_{PWB}(N_B)$, $F_S(r_B)$, f_{KBS} (N_B)}.

User Bchooses a random integer r_B and a random exponent $R_B \epsilon_R Z^*_p$, and then computes $N_B = g^{RB}$and $K_{AB} = N_B{}^{RB}$. Then, B encrypts N_B by using his/her password PW_B like E_{PWB} , (N_B) andcomputes two hash values $F_S(r_B)$ and $f_{KAB}(N_B)$. Finally, B sends{ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$,f_{KAS} (N_A), $E_{PWB}(N_B)$, $F_S(r_B)$, $f_{KBS}(N_B)$} to S.

Step3: S → B:

{N_BR_S, f_{KAS}(ID_A, ID_B,K_{AS},$N_B{}^{RS}$), $N_A{}^{RS}$, f_{KBS}(ID_A, ID_B,K_{BS},$N_A{}^{RS}$)}

Server Sdecrypts $E_{PWA}(N_A)$ and $E_{PWB}(N_B)$ by using P_{WA} and P_{WB} to get N_A and N_B, respectively. Then, Sgets r_A and r_B from $F_S(r_A)$ and $F_S(r_B)$ by using a trap door, respectively. To authenticate A and B,S computes $K_{AS} = N_Ar_A$ and $K_{BS} = N_Br_B$and then verifies $f_{KAS}(N_A)$ and f_{KBS} (N_B), respectively. Ifsuccessful, S chooses a random exponent $R_S \epsilon_R Z^*_p$ and then computes N_AR_S and $N_BR_S$respectively. Finally, S computes two hash values f_{KAS}(ID_A, ID_B,K_{AS},$N_B{}^{RS}$)f_{KBS} (ID_A, ID_B,K_{BS},,$N_A{}^{RS}$), and sends {$N_B{}^{RS}$, f_{KAS} (ID_A, ID_B,K_{AS},$N_B{}^{RS}$),$N_A{}^{RS}$,f_{KBS}(ID_A, ID_B,K_{BS},$N_A{}^{RS}$)} to B.

Step 4: B → A:
{ N_B^{RS} , f_{KAS} (ID_A, ID_B,K_{AS},N_B^{RS}),f_k(ID_B,K)} By using K_{BS} = N_B^{rB} , Bauthenticates S by checking f_{BS}(ID_A, ID_B,K_{BS},N_A^{RS}).If successful, B computes thesession keyK = $(N_A^{RS})^{RB}$ = g^{RSRARB} and hash value f_K(ID_B,K), and then sends {N_B^{RS} , f_{KAS} (ID_A,ID_B,K_{AS},N_B^{RS}), f_K(ID_B,K)} to A

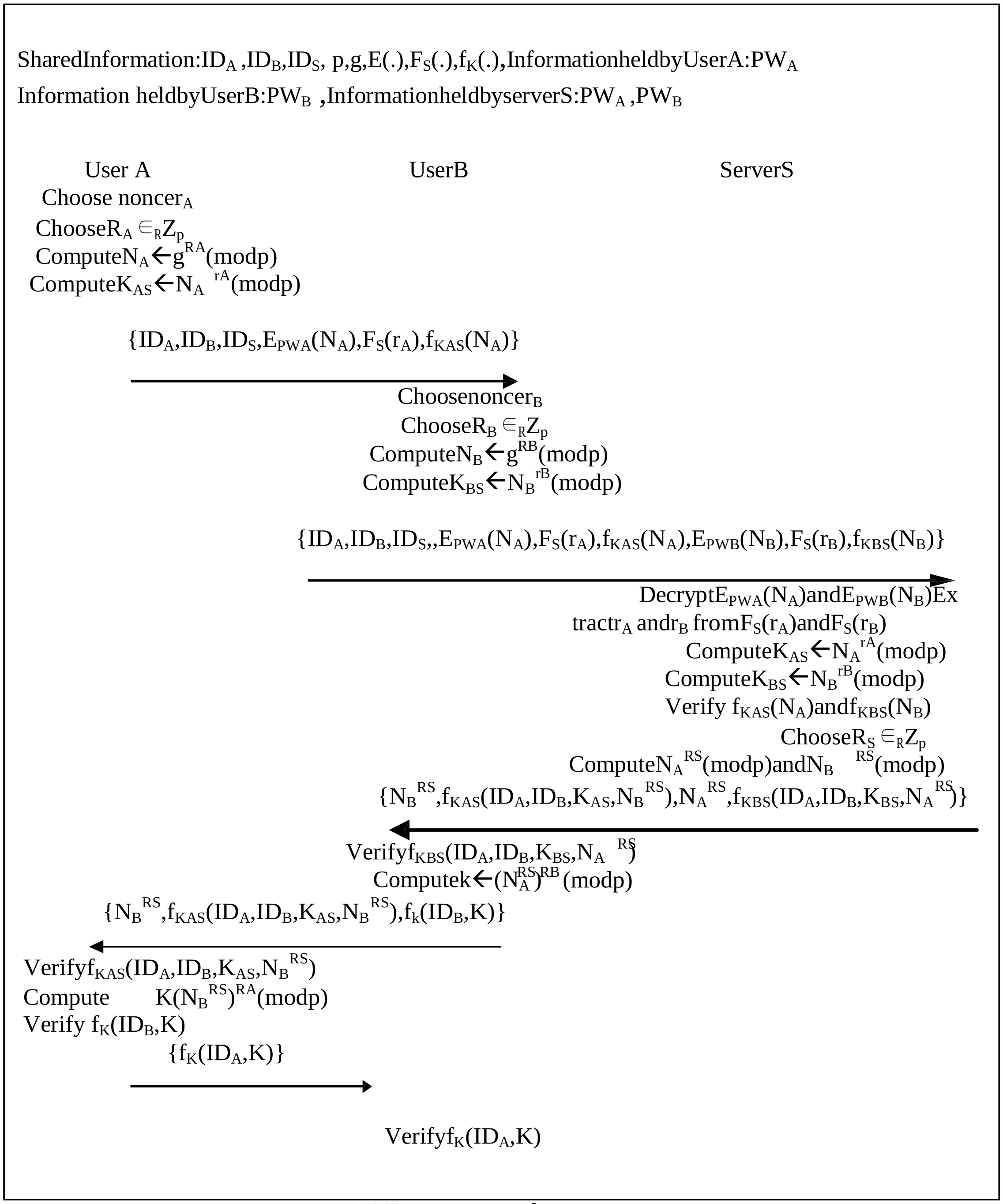

Fig1:3PEKEprotocol

Step5: A → B:
{f_K(ID_A,K)} By using K_{AS} = N_A^{rA}, A authenticates S by checking f_{KAS} (ID_A,ID_B,K_{AS},N_B^{RS}). If successful A computes the session key K = (N_B^{RS})R_A = g^{RSRARB},andauthenticates B by checking f_K(ID_B,K).
If authenticates is passed, A computes and sendsf_K(ID_A,K).

Step 6: B authenticates A by checking $f_K(ID_A,K)$.If successful, B confirms A’s knowledge ofthe session key $K = g^{RSRARB}$.Figure 1 illustrates 3PEKE protocol.

3. UNDETECTABLE ONLINE PASSWORD GUESSING ATTACKON 3PEKE PROTOCOL

SharedInformation:ID_A ,ID_B,ID_S,p,g,E(.),F_S(.),f_K(.),Information heldbyUserA:PW_A
InformationheldbyUserB:PW_B ,InformationheldbyserverS:PW_A ,PW_B

User A | Attacker B | ServerS

A → B: $\{ID_A,ID_B,ID_S,E_{PWA}(N_A),F_S(r_A),f_{KAS}(N_A)\}$

GuessapasswordPW$_A$’
DecryptN’$_A$ ($D_{PWA'}(N_A)$)
Choosenoncer$_B$
Compute$K_{BS} \leftarrow N'_A{}^{rB}$(modp)
Encrypt$E_{PWB}(N'_A)$
Compute$f_{KBS}(N'_A)$}

B → S: $\{ID_A,ID_B,ID_S,,E_{PWA}(N_A),F_S(r_A),f_{KAS}(N_A),E_{PWB}(N_B),F_S(r_B),f_{KBS}(N_B)\}$

Decrypt$E_{PWA}(N_A)$and$E_{PWB}(N'_A)$Extractr_A andr_B from$F_S(r_A)$and$F_S(r_B)$
Compute$K_{AS} \leftarrow N_A{}^{rA}$(modp)
Compute$K_{BS} \leftarrow N'_A{}^{rB}$(modp)
Verify$f_{KAS}(N_A)$and$f_{KBS}(N'_A)$Choose $R_S \in_R Z_p$
Compute$N_A{}^{RS}$(modp)and$N'_A{}^{RS}$(modp)

S → B: $\{N'_A{}^{RS},f_{KAS}(ID_A,ID_B,K_{AS},N'_A{}^{RS}),N_A{}^{RS},f_{KBS}(ID_A,ID_B,K_{BS},N_A{}^{RS})\}$

Verify$N'_A{}^{RS} = N_A^{RS}$
Iftrue,thenN’$_A$=N$_A$ andpw’$_A$=pw$_A$
Otherwise,guessapasswordpw*$_A$
DecryptN*$_A$ ($D_{PWA*}(N_A)$) Compute
$K_{BS}N^*_A{}^{rB}$(modp)
Encrypt$E_{PWB}(N^*_A)$
Compute$f_{KBS}(N^*_A)$}

B → S: $\{ID_A,ID_B,ID_S,,E_{PWA}(N_A),F_S(r_A),f_{KAS}(N_A),E_{PWB}(N^*_A),F_S(r_B),f_{KBS}(N^*_A)\}$

--
--
--

Fig2:Undetectableonlinepasswordguessingattackon3PEKE protocol

ISSN 2348 – 7968

This section demonstrates the undetectable password guessing attack on 3PEKEprotocol as proposed by Yoon and Yoo with the assumption of B as malicious party. Theprocedure of the above attack is given below:

Step1: A →B: {ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$,$f_{KAS}(N_A)$}

Step2: B recordsmessage {ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, $f_{KAS}(N_A)$} from A

Step3: B guesses a password PWA' from password dictionary and gets N'A

Step4: B chooses a random integer r_B and then computes $K_{BS} = N'_A{}^{rB}$. Then, B encrypts N'_A by using his/her password PWB like $E_{PWB}(N'_A)$ and computes two hash values $F_S(r_B)$ and $f_{KBS}(N'A)$.

Step5: B→S: {ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, $f_{KAS}(N_A)$, $E_{PWB}(N'_A)$, $F_S(r_B)$, $f_{KBS}(N'_A)$} Btransmits {ID_A, ID_B, ID_S,$E_{PWA}(N_A)$, $F_S(r_A)$, $f_{KAS}(N_A)$,$E_{PWB}(N_B)$, $F_S(r_B)$, $f_{KBS}(N_B)$}

Step6: S → B:{ $N'_A{}^{RS}$, $f_{KAS}(ID_A, ID_B,K_{AS},N'_A{}^{RS})$, N_A^{RS} , $f_{KBS}(ID_A, ID_B,K_{BS},N_A^{RS})$} Afterreceiving the messageS can authenticate A and B by verifying $f_{KAS}(N_A)$ and $f_{KBS}(N'_A)$,respectively. S will compute $f_{KAS}(ID_A, ID_B, K_{AS}, N'_A{}^{RS})$ and $f_{KBS}(ID_A, ID_B,K_{BS},N_A^{RS})$ to B.

Step7: After receiving the message B simply compares $N'_A{}^{RS} = N_A^{RS}$. If $N'_A{}^{RS} = N_A^{RS}$, it followsthat PWA' = PWA.

4. IMPROVED PARALLEL MESSAGE TRANSMISSION KEY EXCHANGE PROTOCOL

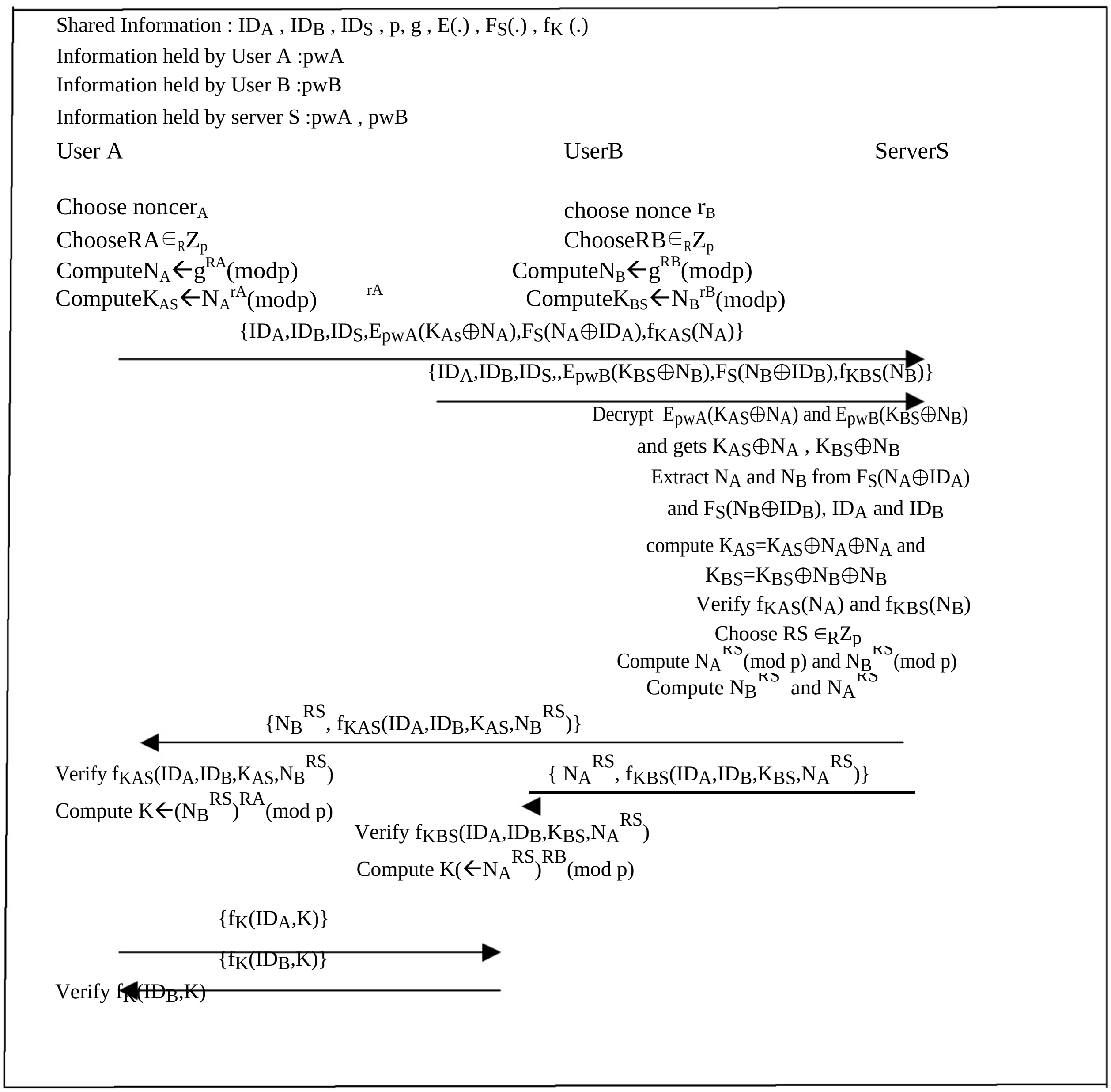

Fig 3.Improved parallel message transmission key exchange protocol

To overcome the Undetectable on- line password guessing attack, an extension is made on the 3PEKEprotocol. The procedure of the protocol is as follows:

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

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

Client A generates two random numbers R_A andr_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 $K_{AS}=N_A^{rA}$ (modp). Next, A sends these three messages to S via his/her own private communication channel.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 numbersR_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.

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

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

Once receiving the message sent from A and B , S first utilizes a trapdoor to obtain NA⊕IDA and NB⊕IDB from FS(NA⊕IDA) and FS(NB⊕IDB) then retrieves NA= NA⊕ID A⊕IDA and NB= NB⊕IDB⊕IDB, respectively. Next it uses the passwords pwA and pwB 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 proceduresof this protocol. Otherwise, S terminates this protocolat current session. Next, S computes N_B^{RS}, N_A^{RS}, andcorresponding 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.

3. B → A: $f_K(ID_B, K)$.

4.A → B: $f_K(ID_A, K)$.

Upon obtaining the transmitted messages sentfrom S, B first verifies $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$ to authenticate S. If this verification is passed, B believesthe 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. Finally, B sendsthe $f_K(ID_B, K)$ 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 $f_K(ID_A, K)$. 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. Figure 3 illustrates the proposed protocol.

5. Security and Efficiency Analysis

The following are the security requirements to be met by a password key exchange protocol.

- Mutual authentication
- Resistance to the password guessing attacks.
- Transmission round and computation complexity.

5.1. Mutual authentication

- First, A and B use the trapdoor function F_S to hide the random number r_A&r_B and pwA&pwB to encrypt N_A& N_B in step 1, as described in section 4 . since only S knows the trap door , pwA&pwB , only S can authenticate A/B after receiving the message sent in step 1.
- Second, S sends {N_B^{RS}, $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$} to A,{ N_A^{RS}, $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$} to B in step 2. This message can be used to authenticate 'S' as mentioned in step 2 in section 4.
- Third, A and B derive key from N_B^{RS} and N_A^{RS} respectively, as mentioned in step 2 in section 4. With the help of $f_K(ID_B, K)$,$f_K(ID_A, K)$ A and B can authenticate each other.

5.2. Resistance to the password guessing attacks

Perfect forward secrecy: The enhanced protocolhas the perfect forward secrecy. The session key is computed as follows: $K=(N_B^{RS})^{RA}$ (mod p)=$(N_A^{RS})^{RB}$
(mod p). If the attacker gets {N_B^{RS}, $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$} or {$N_A^{RS}$, $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$}, then in order to obtain the session key, he should

know RB or RA. Since this is not possible he cannot get the key.

Known-Key Security: In the enhanced protocolas RA, RB are randomly chosen by A and B, and are independent among protocol executions. This leads to the in-vulnerability of Known-Key security.

Server spoofing: The server computes $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$, $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$ and sends to A and B, respectively. A and B can verify the iden-
tity of server or authenticate the server by computing $f_{KAS}(ID_A, ID_B, K_{AS}, N_B^{RS})$, $f_{KBS}(ID_A, ID_B, K_{BS}, N_A^{RS})$, respectively. Thus, the attacker cannot impersonate the server to deceive the client.

Man-in the middle attack: Suppose the attacker frames his own message i.e. $E_{PWc}(K_{CS} \oplus N_C)$, $F_S(N_c \oplus ID_C)$, $f_{KCS}(N_c)$ with the correct guesses password andsends to server. The server will decrptE$_{PWC}(K_{CS} \oplus N_C)$ and gets '$K_{CS} \oplus N_C$' and obtains '$N_C \oplus ID_C$' from $F_S(N_C \oplus ID_C)$. Finaly, S computes hash value which will not match with the received hash value. Hence the protocol gets terminated and not allowing man-in the middle to mount any attack.

5.3. Transmission round and computation complexity

The development of an efficient protocol should take the number of transmission rounds (and steps) and the computation complexity into account. The proposed protocol requires four message transmission rounds. Table 1 shows the performance comparison analyses of the proposed protocol.

Table1comparison between 3PEKE protocol and the improved protocol

	3PEKE protocol	Improved protocol
Communication party	A B S	A B S
Modular exponential operation	3 3 4	3 3 4
Symmetric encryption/decryption	1 1 2	1 1 2
PRF operation	4 4 4	4 4 4
TDF operation	1 1 2	1 1 2
Random number	2 2 1	2 2 1
XOR operation	0 0 0	0 0 0
Transmission round	5	2

6. Conclusion

Though the password-key exchange protocol is in-vulnerable to undetectable on-line pass-word attacks, its modular exponential operations are expensive. The designed protocol is developed with reduced modular exponential operation on server side. The above results show that the proposed protocol is secure, efficient and practical

Referenece

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

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

[2] **S.M. Bellovin, M. Merrit.** Encrypted key exchange:password-based protocols secure against dictionary attacks. *Proceedings of IEEE sysmposium on re-search in security and privacy, IEEE Computer society press*, 1992, 72-84.

[3] **M. Steiner, G. Tsudik, M. Waidner.** Refinement andextention of encrypted key exchange. *ACM OperatingSystems Review*, *Vol*. 29, *No*. 3, 1995, 22-30.

[4] **C.L. Lin, H.M. Sun, M. Steiner, T. Hwang.** Three-party excrypted key exchange without server public-Keys. *IEEE Communication letters*, *Vol*. 5, *No*. 12, 2001, 497- 499.

[5] **C.C. Chang, Y.F. Chang.** A novel three party encryp-ted key exchange protocol. *Computer Standards andInterfaces*, *Vol*. 26 , *No*. 5, 2004, 471-476.

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

[7] **N.W. Lo, K.-H. Yeh.** Cryptanalysis of two three-partyencrypted key exchange protocols. *Computer Stan-dards& Interfaces*, *Vol*. 31, *issue* 6, *Nov*. 2009, 1167-1174.

[8] **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.

M.Ananthi, B.E (CSE), M.E (NE), (Ph.D)(Network Security) received B.E degree from Anna University, Chennai, M.E degree from Anna University Coimbatore. She has Engineering teaching experience of 6 years. She is an active member of ISTE, she is the author of over 6 technical publications in various international and national journal proceedings. Her research interest is in Network Security.

Dr.P.Rajkumar, M.E (CSE), Ph.D(Network Security) received M.E degree from Anna University Chennai, Ph.D degree from Anna University Chennai. He has Engineering teaching experience of 8 years. He is an active member of ISTE, He is the author of over 8 technical publications in various international and national journal proceedings. His research interest is in Network Security.

R.Logeswarisaranya,B.E (CSE), M.Tech (IT), received B.E degree from Anna University, Chennai, M.Tech degree from Anna University Coimbatore. She has Engineering teaching experience of 3 years. She is an active member of ISTE,