An Efficient Three-Party Authenticated Key Exchange Protocol for Mobile-Commerce Environments Using Elliptic Curve Cryptography

Nishant Doshi

***Abstract*—In the three party authentication key exchange (3PAKE) protocol, more than two parties can communicate and set up common shared secret key using the server. Recently, Tan et al. proposed an enhanced 3PAKE scheme based on elliptic curve cryptography (ECC) to minimize the operations and make compatible for mobile commerce environments. However, Nose showed the scheme of Tan et al. is susceptible to the impersonation attack and the man-in-middle attack. However, in this paper we have shown that Tan et al. protocol is susceptible to the known session-specific temporary information attack and the clock synchronization attack too. Afterwards, we have proposed the protocol that withstands against the above mentioned attacks. In addition, our proposed approach is based on the hash function in place of the encryption/decryption function that was used in Tan et al. scheme.**

***Index Terms*—Cryptography, 3PAKE, authentication, key exchange, elliptic curve cryptography**

I. Introduction

IN this digital era, the communication network can become handy using many digital devices and social networking. However the channel that will be used by this can be eavesdropped (by the attacker) so the messages can be modified and harm the end users. Even the attacker can impersonate like some user to another user and do the harmful activity. Therefore, user authentication is an important issue for the security in various e-commerce applications like [4-5]. In order to achieve this, in [1], the authors have firstly proposed the concept of two party authentication key exchange protocol in which two parties will communicate and share a common session/ephemeral key (after authentication each one), that will be used for the future communication. After that there are many techniques [2-3, 6-14, 30] proposed in literature to improve upon the basic 2PAKE scheme of [1].

In a multi-party communication, where there are more than two parties who wants to set-up a common session key, the 2PAKE protocol fails. Because, by applying the notion of the 2PAKE protocol to multiparty, each pair of party requires to set up a session key so that the number of keys increased with more parties and so thus the communication overhead is also increased too. This will lead to a 3PAKE protocol in which more than two parties can communicate efficiently [32]. The desirable attributes of the schemes require to be known key security, forward secrecy, key compromise impersonation, unknown key share and key control [27,31].

The 3PAKE protocols can be divided in two categories i.e. password based and non-password based. In the password based [15-20] approach, each participating party share a password with trusted server and that also used for authentication, thus eliminating the storing of multiple password at the each user side. In non-password based approach [21-24], each party can use the known symmetric key cryptosystems like AES, DES etc. and at the end this lead to a high computation cost. One can also classify the 3PAKE schemes using sever based approaches i.e. server based and non-server based. On the server based approach two or more parties can interact with each other based on the centralized trusted server. While in non-server based approach [24], there is no need to contact the intermediate server. Our approach is based on the password based authentication scheme using the trusted server. Now we will give the overview of 3PAKE protocols that are based on the trusted server approach.

In the mobile-commerce environment, the aim of the protocol is to achieve the security while maintaining the as much as less computation to avoid the computation overhead. Indeed in [22], the authors proposed the 3PAKE scheme that requires less round for the key setup based upon the scheme of [25]. However, it still requires high computation overhead and also susceptible to the stolen-verifier attack. The ECC technique can achieve the same security level as with smaller key size e.g. 1024-bit DLP have security level as that of 160-bit ECC [23, 33-34] and thus preferable for mobile commerce environment. Therefore, in [23], the authors proposed the 3PAKE protocol based on the ECC technique to reduce the message length and achieve the less communication overhead. However, it's susceptible to the unknown key-share attack. Therefore in [26] and afterwards in [27,35], the authors proposed the enhanced version the 3PAKE protocol as compare to [23].

One of the 3PAKE scheme, of ID-based on the ECC technique has been proposed in the [29]. Recently in [28], the authors shows that the scheme of [27] is suffering from the impersonation and the man-in-middle attack and suggest for the enhanced scheme in future. However, in this paper we have shown that the scheme of [27] is also susceptible to the known session-specific temporary information attack and the clock synchronization attack too. Thereafter we have proposed the scheme that requires less computation and still withstand against the proposed attacks.

Organization of the paper : Section 2 describes the literature survey and motivation for our proposed scheme. Section 3 gives the preliminaries that we will use throughout the paper.

Section 4 gives the scheme of Tan et al. Section 5 gives the cryptanalysis of the Tan et al scheme. In section 6, we have given our proposed scheme. Section 7, gives the security analysis and our justification against resilience to the different attacks. Section 8 gives the performance comparison of the proposed scheme. Conclusion and references are at the end.

II. Literature Survey and Our Contribution

In this section, we will show the step wise improvements in the field of 3PAKE protocols start from the scheme of [22] and state the place where our scheme fits as in Table 1.

Ref	Approach and the limitations
[22]	Scheme : • Use the technique of the [25] to give the 3PAKE scheme. • Use less number of rounds. Limitations : • Requires high computation and computation overhead. • Susceptible to the stolen-verifier attack.
[23]	Scheme : • It is based on the Elliptic Curve Cryptography. • It requires less message length and thus less communication overhead. Limitations : • It is susceptible to the unknown key-share attack, parallel attack and impersonation attack.
[26]	Scheme : • It uses the smart card and the public key cryptography (PKC) technique. • This scheme is an improvement of [23] scheme to withstand for unknown key share attack. Limitations : • It is not a proper 3PAKE protocol [27].
[27]	Scheme : • Enhanced protocol for the mobile-commerce environment. Limitations : • It is susceptible to impersonation attack, man-in-middle attack, clock synchronization attack and known session-specific temporary information attack.
[28]	Scheme : • The authors have shown the attacks on the scheme of [27]. Limitations : • There is no any proposed scheme given by the authors.
Our Scheme	It requires less computation overhead and it can withstand against all above specified attacks.

TABLE I
Comparison of different Schemes

A. Our Contribution

As shown in the table 1, there are schemes available in the literature that can be applied to mobile-commerce environment (i.e. resource constrained). However, as they are susceptible to one or more attacks, they are impractical to use in the real time. Also they are using the secure symmetric cryptosystem which increase the computation overhead too.

Therefore, in this paper we have proposed a scheme that users the fewer computation as compare to its predecessors and still withstand against the almost all of the previously mentioned attacks. Moreover, we have made scheme based on the single type hash function only that reduce the computation overhead as compared to previous schemes.

III. Preliminaries

In his section we have given the notations (Table 2) that we will use throughout this paper.

Notation	Meaning
S	A trusted authentication server
A	Initiator
B	Responder
ID_x	Identity of party x
p, q	The large prime satisfies $q \vert p-1$
g	An element (or generator of group G) of order p
x, y	The private/public key pair, $y = g^x \ mod \ p$
T_x	The time stamp of the party x
H	A secure cryptographic hash function
X	An attacker

TABLE II
Notations

IV. Review of Tan et al Scheme [27-28]

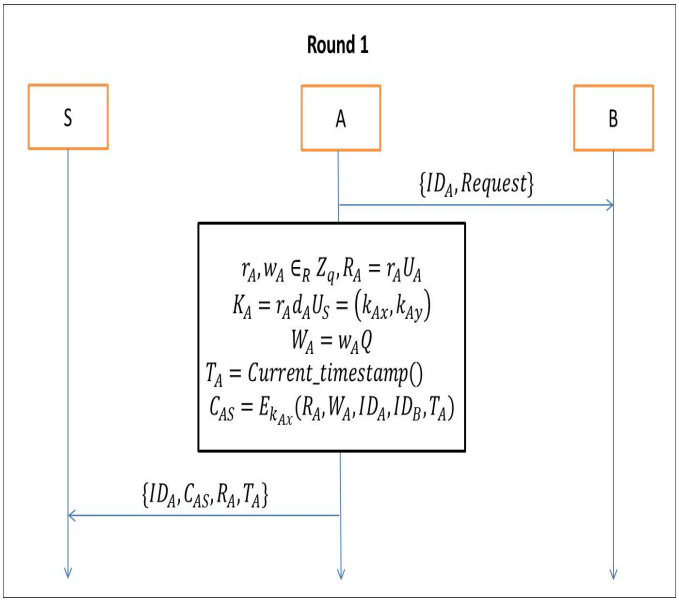
The protocol of [27] is divided into two phase i.e. system initialization and authentication key exchange.

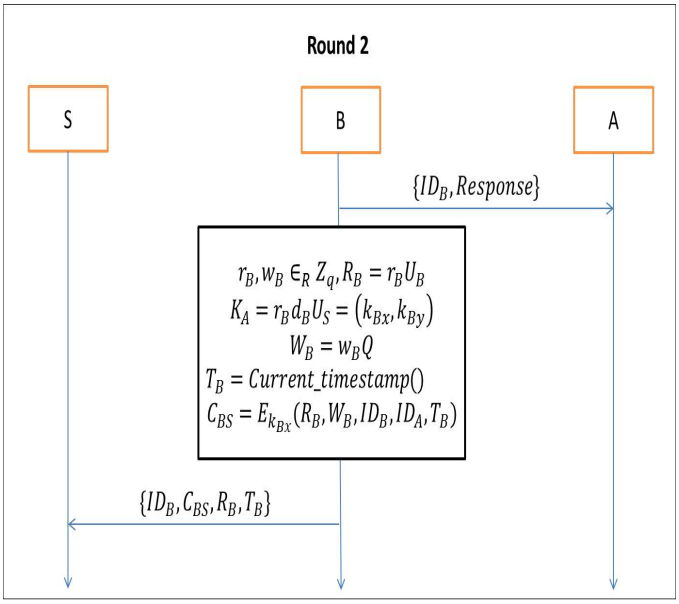
A. System Initialization Phase

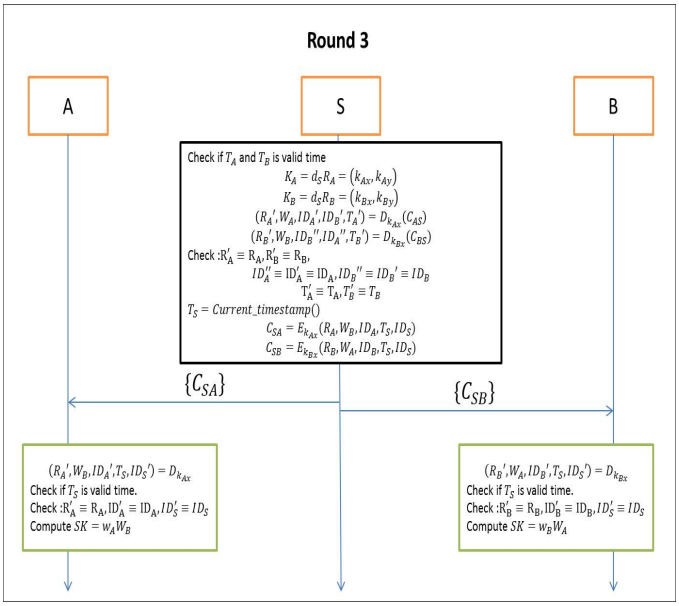
- S selects the elliptic curve $E_q\,(a,b) : y^2 = x^3 + ax + b \ (mod \ q)$ over a finite field F_q generated by point Q and a secure symmetric encryption/decryption algorithms $E_K(\cdot)/D_K(\cdot)$, then make it public.
- Each user u generates its private key d_u and compute the public key $U_u = d_u Q$ and then S signed the $cert_u = \{u, U_u\}$.
- S will generate its own private key d_s and compute the public key $U_s = d_s Q$ and made the U_s publically.

B. Authentication Key Exchange Phase

In this phase, both A and B authenticates each other and set the shared session key using three rounds as follow. Here *Request* denotes a request that initiates by A to communicate with B. Same way, *Response* denotes the response from B to A.







V. Cryptanalysis of Tan et al Scheme

The first three attacks are taken from the [28] while the remaining is proposed by us.

A. Impersonation of the initiator [28]

An attacker X can impersonate as A to the B as follows.

X generates $r_X, w_X \in_R Z_q, R_X = r_X U_X, K_X = r_X d_X U_S = (k_{Xx}, k_{Xy}), W_X = w_X Q, T_X = Current\_timestamp(), C_{XS} = E_{k_{Xx}}(R_X, W_X, ID_A, ID_B, T_X)$. It will send the $\{ID_A, Request\}$ and $\{ID_A, C_{XS}, R_X\}$ to B and S respectively. In the Similar way the remaining of the protocol is runs. At last X and B having $SK = w_X W_B$ and $SK = w_B W_X$ respectively. The more details of this attack can be found in the [28].

B. Impersonation of the responder[28]

An attacker X can impersonate as B to the A as follow.

X generates $r_X, w_X \in_R Z_q, R_X = r_X U_X, K_X = r_X d_X U_S = (k_{Xx}, k_{Xy}), W_X = w_X Q, T_X = Current\_timestamp(), C_{XS} = E_{k_{Xx}}(R_X, W_X, ID_B, ID_A, T_X)$. It will send the $\{ID_B, Response\}$ and $\{ID_B, C_{XS}, R_X, T_X\}$ to A and S respectively. In the Similar way the remaining of the protocol is runs. At last X and A having $SK = w_X W_A$ and $SK = w_A W_X$ respectively. The more details of this attack can be found in the [28].

C. Man-in-the-Middle Attack[28]

As the X can impersonate as A and B so thus X can reside between A and B. X can trace all their communication and then impersonate them both at the same time. This is clear from above two sub-sections. The more details of this attack can be found in the [28].

D. Known session-specific temporary information attack

As specified by [36] and later enhanced by [37], in the Known session-specific temporary information attack if an attacker can have initial generated secrets $(r_A, w_A \ and \ etc)$ then it can not able to get the session key. However as we can see that in all of the schemes of [22-23,26-27,29], they follow the same approach i.e. the session key will be $SK = w_A w_B Q$. Therefore, if the initial secrets are disclosed to the attacker then the schemes of [22-23,26-27,29] are susceptible to the Known session-specific temporary information attack.

E. Clock Synchronization Attack

In a large area network (say WAN, mobile network etc.), the parties are at far distance and so thus the clock synchronization of both parties is tough and unpredictable. Therefore, if we use the scheme of [27] then it fails as it depends on the timestamp of both parties. This will apply to any protocol that uses the timestamp to avoid the reply attack. In order to deal with

this problem, one can use the nonce based technique for this type of network. Therefore, we can say that the scheme of [27] is suitable (even if it resist to all attacks) in a local area network where exact time synchronization is possible, while not suitable for the mobile commerce network (i.e. large area network).

VI. The Proposed Scheme

The proposed scheme is divided into two phase i.e. system initialization phase and authentication key exchange phase.

A. System initialization phase

- S selects the elliptic curve $E_q\,(a,b) : y^2 = x^3 + ax + b\ (mod\ q)$ over a finite field F_q generated by point Q and a secure Hash function $H(\cdot)$, then make it public.
- Each user u generates its private key d_u and compute the public key $U_u = d_u Q$ and then S signed the $cert_u = \{u, U_u\}$. Here (d_u, U_u) is said to be key pair for user u.
- S will generate its own private key d_s and compute the public key $U_s = d_s Q$ and made the U_s publically.

B. Authentication key exchange phase

This phase contains the three round strategy same as of [27].
Round 1: This round is initiated by A (the initiator) to communicate with B.

- It generates $r_A \in_R Z_q$ and calculates $R_A = H(r_A||d_A)\ Q\ , W_A = d_A U_S$.
- $C_{AS} = H(R_A||W_A||ID_A||ID_B)$.
- $A \rightarrow B : (ID_A, Request)$.
- $A \rightarrow S : (ID_A, ID_B, R_A, C_{AS})$.

Round 2: This round is initiated by B (the responder) to communicate with A.

- It generates $r_B \in_R Z_q$ and calculates $R_B = H(r_B||d_B)\ Q\ , W_B = d_B U_S$.
- $C_{BS} = H(R_B||W_B||ID_A||ID_B)$.
- $B \rightarrow A : (ID_B, Response)$.
- $A \rightarrow S : (ID_A, ID_B, R_B, C_{BS})$.

Round 3: This round is to set a session key based on the previous rounds.
S will perform the following steps after receiving messages from A and B.

- It computes $W_A = d_s U_A, W_B = d_s U_B$.
- It calculates $C'_{AS} = H(R_A||W_A||ID_A||ID_B)$ and $C'_{B??} = H(R_B||W_B||ID_A||ID_B)$.
- If $C_{AS} \neq C'_{AS}$ then
  - This is a sender impersonation attack. It will send the message to A.
- If $C_{BS} \neq C'_{BS}$ then
  - This is a receiver impersonation attack. It will send the message to B.
- It computes $C_{SA} = H(R_A||R_B||ID_A||ID_B||W_A)$ and $C_{SB} = H(R_A||R_B||ID_A||ID_B||W_B)$
- $S \rightarrow A : (R_B, C_{SA})$
- $S \rightarrow B : (R_A, C_{SB})$

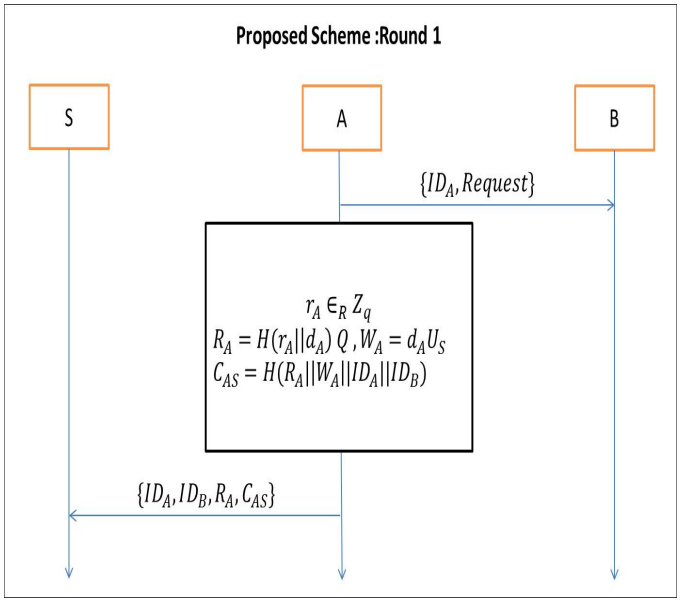
A will perform the following steps after receiving R_B, C_{SA} from S.

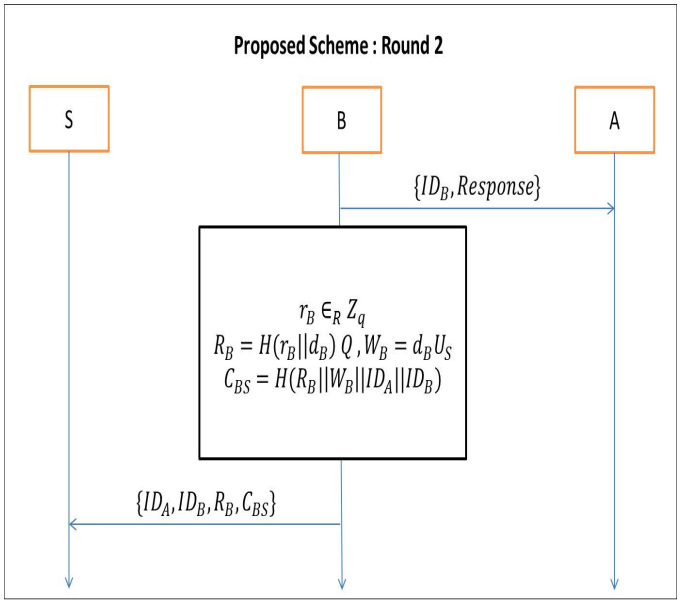
- It computes $C'_{SA} = H(R_A||R_B||ID_A||ID_B||W_A)$ from received R_B and the values generated in *Round 1*.
- If $C'_{SA} \neq C_{SA}$ then
  - This is an attack. It will send message to S.
- It compute $SK = H(r_A||d_A)\ R_B$

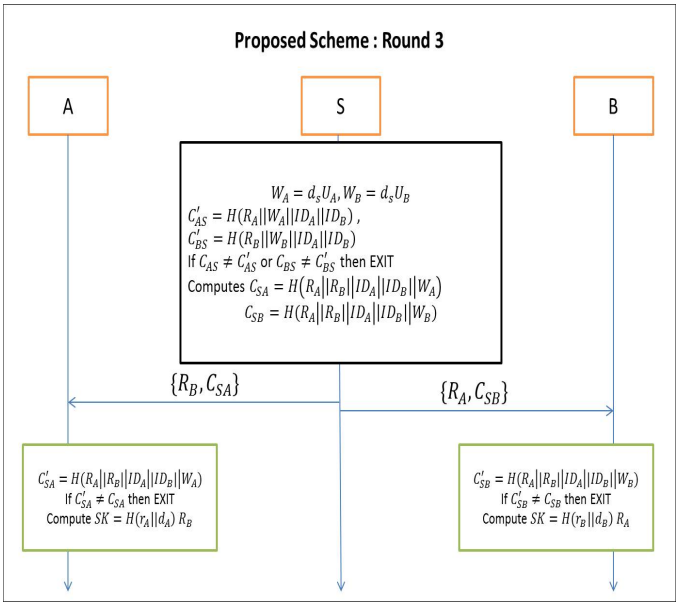
B will perform the following steps after receiving R_A, C_{SB} from S.

- It computes $C'_{SB} = H(R_A||R_B||ID_A||ID_B||W_B)$ from received R_A and the values generated in *Round 1*.
- If $C'_{SB} \neq C_{SB}$ then
  - This is an attack. It will send message to S.
- It compute $SK = H(r_B||d_B)\ R_A$

The sequence of steps for the proposed scheme is shown in the following diagrams pictorially.







VII. Security Analysis

Our proposed scheme is based on the ECC. Therefore, the hardness of our system is based on the secure hash function and the DLP problem as given in below definitions.

Definition 1: (Hash function) A secure hash function H is a collusion resistance one way function in which if given a, it's easy to compute $H(a) = b$, but given b it's hard to compute a.

Definition 2: (Discrete Log Problem) Given $Y_1, Y \in E_q(a, b)$, it is hard to find m such that $Y_1 = m\ Y$.

Now, based on above hardness we will show that our proposed scheme is resisted against many attacks.

A. Impersonation of the initiator attack

Let us assume that attacker X wants to impersonate as A to the B. However, X cannot have d_A from the U_A due to the hardness of the DLP as per definition 2. Therefore, X will do the following

- It generates $d'_A, r_X \in_R Z_q$ and calculates $R_X = H(r_X||d'_A)\ Q$, $W_X = d'_A U_S$.
- $C_{XS} = H(R_X||W_X||ID_A||ID_B)$.
- $X \rightarrow B : (ID_A, Request)$.
- $X \rightarrow S : (ID_A, ID_B, R_X, C_{XS})$

S will perform the following steps after receiving messages from X and B.

- It computes $W'_X = d_s U_A, W_B = d_s U_B$.
- It calculates $C'_{XS} = H(R_X||W'_X||ID_A||ID_B)$ and $C'_{BS} = H(R_B||W_B||ID_A||ID_B)$.
- As $C_{XS} \neq C'_{XS}$
  - This is a sender impersonation attack. It will send the authentication fail message to the A.

Therefore, our scheme is secure against initiator impersonation attack. ■

B. Impersonation of the responder attack

Let us assume that attacker X wants to impersonate as B to the A. however, X cannot have d_B from the U_B due to the hardness of the DLP as per definition 2. Therefore, X will do the following

- It generates $d'_B, r_X \in_R Z_q$ and calculates $R_X = H(r_X||d'_B)\ Q$, $W_X = d'_B U_S$.
- $C_{XS} = H(R_X||W_X||ID_A||ID_B)$.
- $X \rightarrow A : (ID_B, Response)$.
- $X \rightarrow S : (ID_A, ID_B, R_X, C_{XS})$

S will perform the following steps after receiving messages from A and X.

- It computes $W_A = d_s U_A, W'_B = d_s U_B$.
- It calculates $C'_{AS} = H(R_X||W_A||ID_A||ID_B)$ and $C'_{XS} = H(R_B||W'_X||ID_A||ID_B)$.
- As $C_{XS} \neq C'_{XS}$
  - This is a receiver impersonation attack. It will send the authentication fail message to the B.

Therefore, our scheme is secure against the receiver impersonation attack. ■

C. Resistance to the parallel/reply attack

Let us assume that attacker X have values $(ID_A, ID_B, R_A, C_{AS})$ from the past session. In the current session, X will replace the parameters $(ID_A, ID_B, R'_A, C'_{AS})$sent by A to S. The round 3 of the protocol is works as follow

S will perform the following steps after receiving messages from X and B.

- It computes $W_A = d_s U_A, W_B = d_s U_B$.
- It calculates $C'_{AS} = H(R_A||W_A||ID_A||ID_B)$ and $C'_{BS} = H(R_B||W_B||ID_A||ID_B)$.
- If $C_{AS} \neq C'_{AS}$ then
  - This is a sender impersonation attack. It will send the message to A.
- If $C_{BS} \neq C'_{BS}$ then
  - This is a receiver impersonation attack. It will send the message to B.
- It computes $C_{SA} = H(R_A||R_B||ID_A||ID_B||W_A)$ and $C_{SB} = H(R_A||R_B||ID_A||ID_B||W_B)$
- $S \rightarrow A : (R_B, C_{SA})$
- $S \rightarrow B : (R_A, C_{SB})$

A will perform the following steps after receiving R_B, C_{SA} from S.

- It computes $C'_{SA} = H(R'_A||R_B||ID_A||ID_B||W'_A)$ from received R_B and the values generated in *Round 1*.
- As $C'_{SA} \neq C_{SA}$
  - This is an attack. It will send message to S.

In the same way, if X try to reply the messages of B even then that is detected by our protocol. Therefore, our scheme is secure against the reply/parallel attack. ■

D. Known key security attack

In the known key security attack, if current session key is compromised then X cannot able to get the past session keys.

In the proposed scheme, the session key is generated based on the irreversible one way hash function. And due to the property of the hash function, no two output values will same or related for the different inputs. In addition, X cannot derive the past session keys from recorded messages due to the DLP problem of definition 2.

Therefore, our scheme is secure against the known key security attack. ■

E. Perfect forward secrecy

In perfect forward secrecy, compromise of the long term secrets of three parties cannot compromise the past sessions. One can divide this into two different types i.e. perfect forward secrecy (PFS) and master key forward secrecy (MFS).

In PFS, even if the long term secrets of A and B compromise than also the past sessions are secure. In our proposed approach we are using random r_A, r_B for every session, that cannot be determine by the attacker due to irreversible hash function property.

In MFS, even if the long term secrets of S compromise than also the past session are secure. In our proposed approach we are using random r_A, r_B for every session, that cannot be determine by the attacker due to irreversible hash function property. Therefore, X cannot calculate the $H(r_A||d_A)$ *or* $H(r_B||d_B)$.

Therefore, our scheme is secure against the PFS or MFS attack. ■

F. Key compromise impersonation resilience attack

In the key compromise impersonation attack, even if secret key of A is given to X, then also X cannot able to impersonate as another user i.e. B. In the proposed scheme, in order to impersonate as B, X requires the secret key d_B , but it is not possible to recover from U_B due to DLP hardness.

Therefore, our scheme is secure against the key compromise impersonation attack. ■

G. Unknown key share attack

In the unknown key share attack, after the successful run of protocol, A will assume that he had setup the session key B, but B assume that he had setup the session key with C. However, in the proposed scheme we are using ID as the authentication and it will publish by the trusted server S during the system initialization phase. Therefore, session key will be only create/set if correct IDs will be checked beforehand in the Round 3. And that we are checking in the proposed scheme.

Therefore, our scheme is secure against the unknown key share attack. ■

H. Key control attack

In the key control attack, one party can control the key. However, in the proposed scheme the key is made based on secrets or communication between two or more parties. In addition the key space is large enough so that X cannot determine the key by brute force attack (DLP hardness). Here, none of the parties can force the session key to be a pre-selected value.

Therefore, our scheme is secure against the key control attack. ■

I. Outsider attacks

In the outsider attack, X will wiretaps the communication between A, B and S to get the session key. However, in the proposed scheme, the session key is set based on the hash function and secret values of the parties. Therefore, X cannot create the same secret values due to DLP hardness.

Therefore, our scheme is secure against the outsider attack. ■

J. Stolen verifier attack

In stolen verifier, X will use the pre-shared secret value to impersonate as A. However, as the predecessor ECC based system, in our proposed approach we use the hash function and ECC to authenticate user. Therefore, we are not using pre-shared secret value.

Therefore, our scheme is secure against the stolen verifier attack. ■

K. Man-in-the-middle attack

As one can see that attacker X cannot employ the impersonate of the initiator or responder attack. Therefore, it is not possible for A to be fooled into believing X as B, and the B cannot be fooled into believing X as A.

Therefore, our scheme is secure against the man-in-the-middle attack. ■

L. Known session key security attack

A protocol is said to be known session key secure, if past disclosure of session keys cannot disclose the current session's session key. In our proposed protocol, we will use the output of the hash function. As per definition 1, our hash function is collusion resistance one way, therefore the output of two different inputs has no any relation. Thus compromise of past session keys have no any relation to current or future session keys. Therefore, an attacker X cannot determine the next session keys based on the known session security.

Therefore, our scheme is secure against the known session security attack. ■

M. Clock synchronization problem

As our approach uses the nonce based technique, even if the message can be delayed due to large area network, then also A and B can be able to set a common session key.

Therefore, our scheme is secure against the clock synchronization problem. ■

N. Known session specific temporary information attack

In the known session specific temporary information attack, even if X learns the r_A, r_B then also it cannot get the session key. In the proposed scheme, the session key is calculated based on the $H(r_A||d_A)$ *or* $H(r_B||d_B)$, that X cannot calculate without the secret parameters of A or B. X cannot compute the session key from the (R_A, R_B, Q, d_A, d_B) due to the DLP problem.

Therefore, our scheme is secure against the known session specific temporary information attack. ■

O. Key offset attack

In this attack, X can able to modify, delete, and add in messages during the communication between three parties. However, in the proposed scheme, X cannot able to generate the W_A *or* W_B as it doesn't have the secrets of A or B. Therefore, even if X changes the C_{AS} *or* C_{BS} , it can easily detectable by S and the session is stopped.

Therefore, our scheme is secure against the key offset attack. ■

VIII. Performance Analysis

We have compared our scheme with existing schemes based on the different attacks and the resulting analysis is given in below Table 3. In the Table 4 and 5, we have given the comparison based on the message length and time analysis. We have assumed as our predecessor schemes [22-23, 26-27, 29] that the elliptic curve is about 160 bits and the output size of the hash function is 128 bits. As we only send the one element of 160 bits and an element of hash function, the total message length is (160+128)=288 bits. As that of [27], we have assumed that, in the proposed scheme, each party's ID is not required while communication with another party. In table 5, $T_{HASH}, T_{MUL}, T_{EMUL}, T_{ED}, T_{EXP}$ represents the time for one hash function execution, time for one modular multiplication execution, time for one elliptic curve point multiplication execution, time for one symmetric encryption/decryption execution and time for one modular exponent execution respectively.

IX. Conclusion and Future Work

In this paper we have shown that the scheme of Tan et al, is vulnerable to impersonation attack, man-in-the-middle attack, clock synchronization problem, the high computation problem and known session specific temporary information attack. Therefore, we have proposed the enhanced 3PAKE scheme that requires less number of computations and moreover do not require any encryption/decryption technique as of their predecessor system. Our proposed scheme is based on the elliptic curve cryptography technique. Therefore, the proposed protocol is well suited for the mobile commerce environment as of its predecessor systems. We will extend the proposed scheme to the electronic payment scheme.

References

[1] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*, may 1992, pp. 72 –84.

[2] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology CRYPTO 93*, ser. Lecture Notes in Computer Science, D. Stinson, Ed. Springer Berlin Heidelberg, 1994, vol. 773, pp. 232–249. [Online]. Available: http://dx.doi.org/10.1007/3-540-48329-2_21

[3] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology EUROCRYPT 2000*, ser. Lecture Notes in Computer Science, B. Preneel, Ed. Springer Berlin Heidelberg, 2000, vol. 1807, pp. 139–155. [Online]. Available: http://dx.doi.org/10.1007/3-540-45539-6_11

[4] F.-C. Chang, H.-C. Huang, and H.-M. Hang, "Layered access control schemes on watermarked scalable media," *The Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 49, pp. 443–455, 2007. [Online]. Available: http://dx.doi.org/10.1007/s11265-007-0095-0

[5] J.-S. Pan, M.-T. Sung, H.-C. Huang, and B.-Y. Liao, "Robust vq-based digital watermarking for memoryless binary symmetric channel," in *Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on*, vol. 5, may 2004, pp. V–580 – V–583 Vol.5.

[6] Y. J. Choie, E. Jeong, and E. Lee, "Efficient identity-based authenticated key agreement protocol from pairings," *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 179 – 188, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0096300304000785

[7] X. Tian, D. Wong, and R. Zhu, "Analysis and improvement of an authenticated key exchange protocol for sensor networks," *Communications Letters, IEEE*, vol. 9, no. 11, pp. 970 – 972, nov. 2005.

[8] T.-Y. Youn, Y.-H. Park, C. Kim, and J. Lim, "Weakness in a rsa-based password authenticated key exchange protocol," *Information Processing Letters*, vol. 108, no. 6, pp. 339 – 342, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020019008001816

[9] J.-H. Yang and C.-C. Chang, "An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computers and Security*, vol. 28, no. 34, pp. 138 – 143, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404808001120

[10] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895 – 2903, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025510001519

[11] T.-Y. Wu and Y.-M. Tseng, "An efficient user authentication and key exchange protocol for mobile clientserver environment," *Computer Networks*, vol. 54, no. 9, pp. 1520 – 1530, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128609003910

[12] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient and secure dynamic id-based remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, pp. 305 – 309, 2011, special Issue of Computer Communications on Information and Future Communication Security. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366410000861

[13] H. Debiao, C. Jianhua, and H. Jin, "An id-based client authentication with key agreement protocol for mobile clientserver environment on ecc with provable security," *Information Fusion*, vol. 13, no. 3, pp. 223 – 230, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1566253511000029

[14] S. H. Islam and G. Biswas, "A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1892 – 1898, 2011, mobile Applications: Status and Trends. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121211001646

[15] M. Bellare and P. Rogaway, "Provably secure session key distribution: the three party case," in *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, ser. STOC '95. New York, NY, USA: ACM, 1995, pp. 57–66. [Online]. Available: http://doi.acm.org/10.1145/225058.225084

[16] Y. Ding and P. Horster, "Undetectable on-line password guessing attacks," *SIGOPS Oper. Syst. Rev.*, vol. 29, no. 4, pp. 77–86, Oct. 1995. [Online]. Available: http://doi.acm.org/10.1145/219282.219298

	[22]	[23]	[26]	[27]	[29]	Proposed
Resistance to the Impersonation of the initiator attack	NO	NO	NO	NO	YES	YES
Resistance to the Impersonation of the responder attack	NO	NO	NO	NO	YES	YES
Resistance to the parallel/reply attack	NO	NO	YES	YES	YES	YES
Resistance to the Known key security attack	YES	YES	YES	YES	YES	YES
Resistance to the Perfect forward secrecy attack	YES	YES	YES	YES	YES	YES
Resistance to the Key compromise impersonation attack	YES	YES	YES	YES	YES	YES
Resistance to the Unknown key share attack	YES	NO	YES	YES	YES	YES
Resistance to the Key control attack	YES	YES	YES	YES	YES	YES
Resistance to the Outsider attacks	NO	NO	NO	YES	YES	YES
Resistance to the Stolen verifier attack	NO	NO	NO	YES	YES	YES
Resistance to the Man-in-the-middle attack	NO	NO	NO	NO	YES	YES
Resistance to the Known session key security attack	NO	NO	NO	NO	YES	YES
Resistance to the Clock synchronization problem	YES	YES	YES	NO	NO	YES
Resistance to the Known session specific temporary information attack	NO	NO	NO	NO	NO	YES
Resistance to the Key offset attack	YES	YES	YES	YES	YES	YES

TABLE III
COMPARISON BASED ON THE RESISTANCE TO THE DIFFERENT ATTACKS

	[22]	[23]	[26]	[27]	[29]	Proposed
Communication times	7	6	6	6	6	6
Bandwidth	5824 bits	832 bits	832 bits	832 bits	832 bits	228 bits

TABLE IV
COMPARISON BASED ON THE COMMUNICATION OVERHEAD

Computation costs	[22]	[23]	[26]	[27]	[29]	Proposed
For initiator A	$4T_{EXP}+1T_{MUL}+4T_{HASH}$	$5T_{EMUL}+2T_{ED}$	$5T_{EMUL}+2T_{ED}$	$5T_{EMUL}+2T_{ED}$	$3T_{EMUL}+3T_{HASH}$	$3T_{EMUL}+3T_{HASH}$
For responder B	$4T_{EXP}+1T_{MUL}+4T_{HASH}$	$5T_{EMUL}+2T_{ED}$	$5T_{EMUL}+2T_{ED}$	$5T_{EMUL}+2T_{ED}$	$3T_{EMUL}+3T_{HASH}$	$3T_{EMUL}+3T_{HASH}$
For server S	$1T_{EXP}+2T_{MUL}+6T_{HASH}$	$2T_{EMUL}+4T_{ED}$	$2T_{EMUL}+4T_{ED}$	$2T_{EMUL}+4T_{ED}$	$2T_{EMUL}+6T_{HASH}+2T_{INV}$	$2T_{EMUL}+4T_{HASH}$

TABLE V
COMPARISON BASED ON THE COMPUTATION OVERHEAD

[17] H.-B. Chen, T.-H. Chen, W.-B. Lee, and C.-C. Chang, "Security enhancement for a three-party encrypted key exchange protocol against undetectable on-line password guessing attacks," *Computer Standards and Interfaces*, vol. 30, no. 12, pp. 95 – 99, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548907000633

[18] C.-L. Lin, H.-M. Sun, and T. Hwang, "Three-party encrypted key exchange: attacks and a solution," *SIGOPS Oper. Syst. Rev.*, vol. 34, no. 4, pp. 12–20, Oct. 2000. [Online]. Available: http://doi.acm.org/10.1145/506106.506108

[19] R. Lu and Z. Cao, "Simple three-party key exchange protocol," *Computers and Security*, vol. 26, no. 1, pp. 94 – 97, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404806001246

[20] H.-Y. Chien and T.-C. Wu, "Provably secure password-based three-party key exchange with optimal message steps," *The Computer Journal*, vol. 52, no. 6, pp. 646–655, 2009. [Online]. Available: http://comjnl.oxfordjournals.org/content/52/6/646.abstract

[21] C.-L. Lin, H.-M. Sun, M. Steiner, and T. Hwang, "Three-party encrypted key exchange without server public-keys," *Communications Letters, IEEE*, vol. 5, no. 12, pp. 497 –499, dec. 2001.

[22] T.-H. Chen, W.-B. Lee, and H.-B. Chen, "A round- and computation-efficient three-party authenticated key exchange protocol," *Journal of Systems and Software*, vol. 81, no. 9, pp. 1581 – 1590, 2008, gauging the progress of Software Architecture research: three selected papers from Working IEEE/IFIP Conference on Software Architecture (WICSA) 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121207003135

[23] J.-H. Yang and C.-C. Chang, "An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-

commerce environments," *Journal of Systems and Software*, vol. 82, no. 9, pp. 1497 – 1502, 2009, sI: QSIC 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121209000880

[24] M. Hlbl, T. Welzer, and B. Brumen, "Two proposed identity-based three-party authenticated key agreement protocols from pairings," *Computers and Security*, vol. 29, no. 2, pp. 244 – 252, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740480900090X

[25] C. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, pp. 161–174, 1991. [Online]. Available: http://dx.doi.org/10.1007/BF00196725

[26] Q. Pu, X. Zhao, and J. Ding, "Cryptanalysis of a three-party authenticated key exchange protocol using elliptic curve cryptography," in *Research Challenges in Computer Science, 2009. ICRCCS '09. International Conference on*, dec. 2009, pp. 7 –10.

[27] Z. Tan, "An enhanced three-party authentication key exchange protocol for mobile commerce environments," *Journal of Communications*, vol. 5, no. 5, 2010. [Online]. Available: https://academypublisher.com/ academz3/ojs/index.php/jcm/article/view/0505436443

[28] P. Nose, "Security weaknesses of authenticated key agreement protocols," *Information Processing Letters*, vol. 111, no. 14, pp. 687 – 696, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020019011001074

[29] Y. C. Debiao He, "An id-based three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments," Cryptology ePrint Archive, Report 2011/195, 2011. [Online]. Available: http://eprint.iacr.org/2011/195

[30] M. Hlbl, T. Welzer, and B. Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," *Journal of Computer and System Sciences*, vol. 78, no. 1, pp. 142 – 150, 2012, jCSS Knowledge Representation and Reasoning. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0022000011000031

[31] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *Crytography and Coding*, ser. Lecture Notes in Computer Science, M. Darnell, Ed. Springer Berlin Heidelberg, 1997, vol. 1355, pp. 30–45. [Online]. Available: http://dx.doi.org/10.1007/BFb0024447

[32] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and extension of encrypted key exchange," *SIGOPS Oper. Syst. Rev.*, vol. 29, no. 3, pp. 22–30, Jul. 1995. [Online]. Available: http://doi.acm.org/10.1145/206826.206834

[33] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[34] N. Koblitz, "Elliptic curve cryptosystem," *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.

[35] Z. Tan, "A communication and computation-efficient three-party authenticated key agreement protocol," *Security and Communication Networks*, pp. n/a–n/a, 2012. [Online]. Available: http://dx.doi.org/10.1002/sec.622

[36] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology EUROCRYPT 2001*, ser. Lecture Notes in Computer Science, B. Pfitzmann, Ed. Springer Berlin Heidelberg, 2001, vol. 2045, pp. 453–474. [Online]. Available: http://dx.doi.org/10.1007/3-540-44987-6_28

[37] Z. Cheng, M. Nistazakis, R. Comley, and L. Vasiu, "On the indistinguishability-based security model of key agreement protocols-simple cases," Cryptology ePrint Archive, Report 2005/129, 2005. [Online]. Available: http://eprint.iacr.org/2005/129

Nishant Doshi He had done B.E. from DDU, India in 2007. Then He joined DA-IICT, India for M.Tech. and completed in 2009. After, M.Tech. he had done job of lecturer at V.V.P. college, India. Currently he is working as a full time Ph.D. research scholar at S V National Institute of Technology, India from 2010 onwards. He had been reviewer for IEEE Transaction on Computers, Elsevier journal of system and software,IJNS,IJCA and other international conferences like PDCTA, CCSIT, DPPR, ICCAIE,ISIEA,ITCA,ACSIT,NetCom,ICISC etc. He had been Programme committee member in DPPR, PDCTA, CCSIT etc. He is serving as Editorial Board member in international journals like IJICS,IJCTCM,IJIST,IJPLA,IJESA,IJASSN,IJFLS etc.