Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 594-599, DOI : 10.14429/dsj.66.10799

An Authenticated Key Agreement Scheme using Vector Decomposition

Praveen I.*, Rajeev K., and M. Sethumadhavan
TIFAC CORE in Cyber Security, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham, Amrita University, Coimbatore - 641 112, India
**E-mail: i_praveen@cb.amrita.edu*

ABSTRACT

Encryption using vector decomposition problem (VDP) on higher dimensional vector spaces is a novel method in cryptography. Yoshida has shown that the VDP on a two-dimensional vector space is at least as hard as the computational Diffie-Hellman problem on a one-dimensional subspace under certain conditions. Steven Galbraith has shown that for certain curves, the VDP is at most as hard as the discrete logarithm problem on a one-dimensional subspace. Okomoto and Takashima proposed encryption scheme and signature schemes using VDP. An authenticated key agreement scheme using vector decomposition problem is proposed in this paper.

Keywords: Vector decomposition problem, distortion eigenvector space, key establishment

1. INTRODUCTION

Many public key cryptosystems are designed based on the hardness of discrete logarithm problem (DLP) or computational diffie-hellman problem (CDHP). Vector decomposition problem (VDP), initially proposed by Yoshida[1,2], was introduced as an alternative to these problems. Yoshida provided some sufficient conditions for the equivalence of VDP and CDHP. Duursma and Kiyavash[3] proved that genus 1 curves satisfying these conditions are supersingular. Supersingular curves are not preferred for the use of VDP due to the existence of *MOV - reduction* or *FR - reduction*. Hence higher genus curves are preferred for the use of VDP. Okamoto[7], *et al.* extended the idea of VDP into higher dimensional vector spaces. They introduced a homomorphic encryption and signature scheme using dual pairing vector spaces and a trapdoor function. Lim[6], *et al.* introduced key substitution attack on Okamoto and Takashima scheme[7]. We make use of the hardness of VDP, curves given in papers[3,7,8], the trapdoor given by Okamoto and Takashima[7] and a similar protocol given by So[9], *et al.* to construct an authenticated key agreement scheme and also prove that key substitution attack[6] is not possible in our scheme.

Certificateless public key cryptography was introduced by Al-Riyami and Paterson[10]. They introduced a key generating center (KGC) and shown that the trust required on KGC is much less than that required on private key generator (PKG) in identity based public key cryptography and certifying authority (CA) in traditional certificate based schemes. But the protocol lacks the resistance towards leakage of ephemeral keys[11]. Though Swanson and Jao[11] suggests that the problem can be fixed, they also claim that this fix is not strong. Mandt and Tan[12] proposed a protocol that satisfy all the security properties of Al-Riyami and Paterson protocol. But Swanson and Jao[11] proved that Mandit and Tan[12] protocol is not resistant towards the leakage of ephemeral information and also shown that Mandt and Tan protocol admits key compromise impersonation (KCI) attack. In all these schemes KGC can launch a man-in-middle attack. Lippod[13], *et.al.* proposed a scheme which is provably secure in a suitable security model, extended Carnetti-Krawczyk (eCK) model[11]. The scheme is secure under bilinear Diffie-Hellman assumption, but requires ten pairing computations per party. The number of pairing computations can be reduced to five pairings per party under gap bilinear Diffie-Hellman assumption.

We propose a scheme similar to Al-Riyami and Paterson[10]. The security of our scheme is depending on the hardness of vector decomposition problem (VDP). In our scheme KGC used in paper[10] is the master authority which also acts similar to private key generator (PKG) in the identity based encryption scheme by Boneh and Franklin[14]. But in each session of our scheme, entity chooses a new random number to establish the session key. Though PKG knows the private key, the presence of the random number makes this key as a partial private key and solves key escrow problem in identity based cryptography. The users are required to register with the master authority, PKG initially. PKG generates its own secret key, say, master secret key. By using this master key, secret keys are provided to users who register with it. The amount of trust invested on PKG in the proposed scheme is less than that required in Al-Riyami and Patterson, but our scheme requires a trusted directory of public keys. The knowledge of full secret key of the user will give negligible advantage to PKG. This is explained in detail in the later section. Hence we do not require the double encryption used in certificateless cryptographic schemes. Registration is a one time process. Once the

Received : 31 January 2016, Revised : 12 July 2016
Accepted : 19 July 2016, Online published : 31 October 2016

registration is successfully over, these registered users can communicate among themselves without contacting the PKG again. This reduces the key exchange traffic. Our scheme does not require digital certificates for authentication and thus solves the problem of managing too many digital certificates. Three points on an elliptic curve are used as public key and another point as private key and hence public and private keys are short. Moreover, our scheme requires no pairing computation during encryption and requires only six pairing computation during decryption. The scheme has both forward secrecy and backward secrecy. To provide freshness to the session key, we use a hybrid method suggested by Mitchell[15]. Our proposed scheme permits the user to choose the five random numbers out of six random numbers used for encryption (The remaining one is dependant on two of these five random numbers). The initiator can make use of one of the numbers as a counter based on real time. This provides freshness to the key and prevents replay attack.

2. PRELIMINARIES

A *bilinear map* is a function $e: G_1 \times G_2 \to G_3$ where G_1, G_2, G_3 are groups of finite order. The function *e*(. , .) is such that for all $u \in G_1$, $v \in G_2$, $e(u^a,v^b)=e(u,v)^{ab}$ where *a* and *b* are integers.

Definition 2.1 *A bilinear pairing on* (G, G') *is an efficiently computable map* $\phi : G \times G :\to G'$*, which is bilinear and non-degenerate where* G, G' *are groups of finite order.*

ie, for all $a, b, c \in G$,

$$\phi(a+b,c) = \phi(a,c)\phi(b,c) \tag{1}$$

$$\phi(a,b+c) = \phi(a,b)\phi(a,c) \tag{2}$$

$$\phi(a,b) \neq 1,\ \forall a \neq b \tag{3}$$

2.1 Vector Decomposition Problem

Okamoto and Takashima[7] introduced VDP in higher dimensions and the concept of dual pairing vector spaces. The higher dimensional VDP is defined as follows.

Definition 2.2 *Generalised Computational Vector Decomposition Problem (gCVDP): Let V be a vector space over the field* F_p *and* $\{P_1, P_2, .., P_n\}$ *be a basis for V. For a given* $Q \in V$ *, VDP with respect to the basis* $\{P_1, P_2, .., P_n\}$ *is to compute the element* $R \in V$ *such that* $R \in < P_1, P_2, .., P_m >$ *and* $Q - R \in < P_{m+1}, .., P_n >$*,* $m < n$*.*

Let $\lambda \in N$ be the security parameter of a set up algorithm that outputs a $n-$dimensional F_p- vector space *V*, $m < n$ and A be a probabilistic polynomial time machine.

Let $v = \sum_{i=1}^{n} x_i P_i$, where $P_1, P_2, .., P_n \in V$ and $x_1, x_2, .., x_n \in F_p$. The $gCVDP_{(m,n)}(\lambda)$ *advantage of A* is the probability of getting $w = \sum_{i=m+1}^{n} x_i P_i'$ where V and $(P_1, P_2, .., P_n)$ are given.

The gCVDP assumption is that for any polynomial time adversary A, the advantage $gCVDP_{(m,n)}(\lambda)$ *is negligible*[7].

Definition 2.3 *Generalised computational diffie hellman problem (gCDHP): Let V be a* $n-$*dimensional vector space over the field* F_p*. Let* $P_{m+1}, P_{m+2}, .., P_n$*,* $P'_{m+1}, P'_{m+2}, .., P'_n \in V$ *where m < n. Consider the vectors* $v = \sum_{i=m+1}^{n} x_i P_i$ *and* , $w = \sum_{i=m+1}^{n} x_i P_i'$ *, where* $x_1, x_2, .., x_n \in \mathsf{F}_p$.

Given v, P_i, P_i'*, i=m+1,…,n as above, gCDHP is to find* w.

Let *A* be a probabilistic polynomial time machine. The $gCDHP_{(m,n)}(\lambda)$ *advantage of A* is the probability of getting $w = \sum_{i=m+1}^{n} x_i P_i'$ where *V*, $(P_1, P_2, .., P_n)$ and $v = \sum_{i=m+1}^{n} x_i P_i$ are given.

The gCDHP assumption is that given any polynomial time adversary A, the $gCDHP_{(m,n)}(\lambda)$ *advantage of A is negligible*[7].

2.2 Trapdoor for VDP

For constructing a trapdoor for solving VDP in higher dimension, Okamoto and Takashima[7] introduced the concept called distortion eigenvector space for higher dimension. This vector space has efficiently computable distortion maps and bilinear operators.

Definition 2.4 *Distortion eigenvector space V is a* n *-dimensional vector space over F, that satisfies the following conditions:*

1. There exist *A*, *F* and $\{\varphi_{i,j}\}_{1 \le i,j \le n}$ such that: Let $A = (Q_1, Q_2, .., Q_n)$ be a basis of F_r -vector space *V* and F a polynomial-time computable automorphism on *V*. The basis *A* is called a distortion eigenvector basis with respect to *F*, if each Q_i is an eigenvector of *F*, their eigenvalues are different from each other, and there exist polynomial-time computable endomorphisms $\varphi_{i,j}$ of *V* such that $\varphi_{i,j}(Q_j) = Q_i$. We call $\varphi_{i,j}$ a distortion map.
2. There exists a skew-symmetric non-degenerate bilinear pairing $e : V \times V \to \mu_r$ where μ_r is a multiplicative cyclic group of order r.
3. There exists a polynomial-time computable automorphism ρ on *V* such that $e(v, \rho(v)) \neq 1$ for any v except for v in a quadratic hypersurface of $V \cong (F_r)^n$.

Lemma 1 (*Projection Operators*).*Let* $A = (Q_1, Q_2, .., Q_n)$ *be a distortion eigenvector basis of V, and* Q_i *has its eigenvalue* λ_i *of* F*. The following polynomial of* F *is a projection operator:* $Pr_j(v) = (\Pi_{i \neq j}(\lambda_j - \lambda_i))^{-1} \Pi_{i \neq j}(F - \lambda_i)(v)$.

Hence $Pr_j(Q_k) = 0$ for $k \neq j$ and $Pr_j(Q_j) = Q_j$.

Let *V* be a distortion eigenvector space and $(Q_1, Q_2, .., Q_n)$ be a distortion eigen basis of *V*. Consider the matrix $X = (x_{ij})$ such that $P_i = \sum_{j=1}^{n} x_{ij} a_j$ and $(P_1, P_2, .., P_n)$ is also a basis for *V*. Let $v = \sum_{i=1}^{n} y_i P_i$ be the vector in *V*. Our aim is to decompose v as the sum of two vectors where one lies in the subspace generated by $(P_1, P_2, .., P_m)$, $m < n$ and the other lies in the subspace generated by $(P_1, P_2, .., P_n)$. If $X^{-1} = (t_{ij})$, lemma 3 of Okamoto and Takashima[7] proves the function

$$VDeco(v, < P_j >, X, < P_1, P_2, .., P_n >) = \sum_{i=1}^{n} \sum_{k=1}^{n} t_{ij} x_{jk} \varphi_{ki}(Pr_i(v))$$

can be used to accomplish this goal.

3. OKAMOTO TAKASHIMA SCHEME AND KEY SUBSTITUTION ATTACKS

3.1 Public Keys in Okamoto and Takashima Scheme

Let V be a distortion eigenvector space and $F : V \rightarrow V$ be an endomorphism. Let $A = (Q_1, Q_2, .., Q_n)$ be a distortion eigenvector basis for V. Therefore, there exist $\lambda_1, \lambda_2, ..., \lambda_n$ such that $F(Q_1) = \lambda_1 Q_1$, $F(Q_2) = \lambda_2 Q_2, ..., F(Q_n) = \lambda_n Q_n$. Let φ_{ij} be the distortion map such that $\varphi_{ij}(Q_j) = Q_i$. $X = (u_{ij})$ is a matrix where $u_{ij} \in F_p$ such that $\det X \neq 0$. P_1, $P_2, .., P_n$ are points generated by X such that $P_j = X(Q_1, Q_2, .., Q_n)^T$. Let $B = \{P_1, P_2, .., P_n\}$. Hence B also forms a basis. Here (V, A, B) is the public parameter.

3.2 Equivalent Public Keys and Key Substitution Attack

In key substitution attack, a malicious adversary generates an alternate public key corresponding to the public key of an authorised user. Let pk and σ be the public key and signature of the authorised user for a given message. The adversary D tries to find an alternate public key pk' and a signature σ' corresponding to the parameters pk and σ of the user for the given message. That is, for a given message m , σ' is also a valid signature with respect to the new public key $pk'(\neq pk)$. To perform the attack, if the adversary does not require the secret key sk' , corresponding to the new public key pk' , it is called strong key substitution(SKS) attack, otherwise weak key substitution attack. Lim *et.al.*[6] showed the following Signature-equivalent public keys and Encryption-equivalent public keys existing in the Okamoto and Takashima scheme[7] and demonstrated a SKS attack.

3.2.1 *Signature-equivalent Public Keys*

Definition 3.1 *For two key pairs* (pk, sk) *and* (pk', sk') *in a signature scheme, the public key* pk' *is signature-equivalent to the public key* pk *if* $Verify(pk', m, Sign(sk, m)) = True$ *for any message* m .

Let the public parameters of the Okamoto and Takashima signature schemes are (V, A, B, h) with $B = (P_1, P_2, ..P_n)$ and a hash function h. Then (V, A, B', h) with $B' = (P'_1, P'_2, ..P'_n)$ such that $e(P_j, P'_j) = 1$ for $j = 1, 2, .., n$ forms the signature-equivalent public keys[6].

3.2.2 *Encryption-equivalent Public Keys*

Definition3.2 *Fortwokeypairs* (pk, sk) *and* (pk', sk') *inan encryption scheme, the public key* pk' *is encryption-equivalent to the public key* pk *if* $Decrypt(sk, Encrypt(pk', m)) = m$ *for any message m.*

The following encryption-equivalent public keys exist in the Okamoto and Takashima scheme. Let $pk = (V, A, B)$ with $B = (P_1, P_2, ..P_n)$. Then $pk' = (V, A, B')$ forms the set of equivalent keys with $B' = (P'_1, P'_2, ..P'_n)$ where

$$P'_i = \begin{cases} P_i + \sum_{k=m+1}^{n} z_{ik} P_k, & \textit{if } i \leq m \\ \sum_{k=m+1}^{n} z_{ik} P_k, & \textit{otherwise.} \end{cases}$$

4. PROPOSED AUTHENTICATED KEY AGREEMENT SCHEME

We propose an authenticated key agreement scheme using vector decomposition. The trapdoor function described in Section 2.2 is used for decryption and authentication in the proposed scheme. Let E / F_p be a hyper elliptic curve and $F : E \rightarrow E$ be an endomorphism. Let $A = (S, T, U)$ be a distortion eigen basis for $E[m]$, the set of m–torsion points on E for a prime m. Therefore, there exist λ_1, λ_2 and λ_3 such that $F(S) = \lambda_1 S$, $F(T) = \lambda_2 T$ and $F(U) = \lambda_3 U$. If $b_1 = S, b_2 = T, b_3 = U$, then φ_{ij} be the distortion map such that $\varphi_{ij}(b_j) = b_i$. Let $X = (u_{ij})$ be a matrix where $u_{ij} \in F_p$ and $\det X \neq 0$ ·

Let $B = \{P_1, P_2, P_3\}$, where P_1, P_2 and P_3 are points generated by X such that :

$P_1 = u_{11}S + u_{12}T + u_{13}U$, $P_2 = u_{21}S + u_{22}T + u_{23}U$ and $P_3 = u_{31}S + u_{32}T + u_{33}U$.

Hence B also forms a basis which is not a distortion eigenvector basis. Here the public parameters are E / F_p , (P_1, P_2, P_3) , (S, T, U). The transformation matrix X is kept as secret.

The proposed key agreement scheme could be implemented in networks. Our scheme consists of two phases. The device registration with private key generator (PKG) is performed in phase-I. Once the registration is successfully over, phase-II which contains data packet transmission and reception begins.

Master Key Device Registration:

- The PKG selects a distortion eigenvector basis, the transformation matrix $X_{KG} = (u_{ij})$ and generates (P_1, P_2, P_3) , as above. PKG selects a random number z which is the master secret key.

  A device Alice in the network want to register herself with PKG:

- There will be two device registration keys, namely $S_D R$ and $A_D R$ such that $S_D R = zA_D R$, embedded in the device.
- Alice selects a distortion eigenvector basis, its transformation matrix $X_A = (v_{ij})$ and generates (A, A_r, A_s) as above.
- Alice chooses a random number r_a and calculate $K_G = S_D R P_1 + A_D R P_2 + r_a P_3$. She sends a request to PKG along with K_G .
- On receiving the K_G , PKG uses

  $VDeco(K_G, < P_1 >, X_{KG}, (P_1, P_2, P_3))$ to get $S_D R P_1$ and

  $VDeco(K_G, < P_2 >, X_{KG}, (P_1, P_2, P_3))$ to get $A_D R P_2$.
- PKG verifies $S_D R P_1$ and $A_D R P_2$ and if it matches with that of Alice, PKG calculates Alice's secret key as $Sk_A = zA$ and encrypts zA as $K = zA + S_D R A_r + A_D R A_s$. PKG sends K to Alice.
- On receiving K , Alice uses

  $VDeco(K, < A >, X_A, (A, A_r, A_s))$ and retrieves the secret key zA.
- Alice confirms the originality by verifying whether

  $S_D R A_r = VDeco(K, < A_r >, X_A, (A, A_r, A_s))$ and

  $A_D R A_s = VDeco(K, < A_s >, X_A, (A, A_r, A_s))$.

  Any mismatch of the two equations will abort the process.

She uses this secret key for establishing any session key in the network. Once this registration is successfully over, Alice can communicate with any other registered device in the network using this scheme.

Data Packet Transmission:

Alice performs the following procedure for the key establishment and authentication.

- Choose the public keys of Bob B, B_r, B_s.
- Select random elements $k_1, k_2, k_3, d_1, d_2, d_3$ such that $k_1 B = d_1 Sk_A + d_2 A_r + d_3 A_s$ and fixes the X-coordinate of $k_1 B$, say *u*, as the session key.
- Calculate $B_c = k_1 B + k_2 B_r + k_3 B_s$.
- Let $d_1 zA = t_1$, $d_2 A_r = t_2$ and $d_1 k_1 A = t_3$.
- Alice sends (B_c, t_1, t_2, t_3) to Bob.

Data Packet Reception:

On receiving the packet, Bob performs decryption and verifies the genuineness of the source using the following procedure.

- Calculate $k_1 B$ using $VDeco(B_c, <B>, X_B, (B, B_r, B_s))$.
- Find u, the X-coordinate of $k_1 B$.
- Verify the originality using Weil Pairing,

$$e(t_1, k_1 B) = e(t_3, Sk_B) \quad (1)$$

$$e(t_1 + t_2, A_s) = e(k_1 B, A_s) \quad (2)$$

$$e(k_1 B + t_3, A_s) = e(t_1 + t_2 + t_3, A_s) \quad (3)$$

- If the above check fails, terminate and restart the procedure.

4.1 Correctness of the Scheme

Proposition 4.1 *The above scheme provides both confidentiality and authentication.*

Proof:

Confidentiality: Extracting $k_1 B$ from B_C is equivalent to solve VDP.

Authentication: The scheme provides entity authentication.

To extract d_1 and z from $t_1 = d_1 zA$, one should solve ECDLP and then apply integer factorization.

Since $K_1 B = d_1 zA + d_2 A_r + d_3 A_s$, it can also be done using the trapdoor function $VDeco(K_1 B, <A>, X_A, (A, A_r, A_s))$. Hence only Alice can perform this extraction.

Note that here t_1 is the component of B_c which is equal to $d_1 Sk_A$. Hence Alice computes $d_1 Sk_A$ without applying $VDeco$. In the verification process,

LHS and RHS of Eqn (1) simplifies to

$$e(t_1, k_1 B) = e(d_1 Sk_A, k_1 B) = e(d_1 zA, k_1 B) = e(A, B)^{d_1 z k_1}$$

and $e(t_3, Sk_B) = e(d_1 k_1 A, zB) = e(A, B)^{d_1 k_1 z}$ respectively.

Since Weil pairing is alternating, $e(A_s, A_s) = 1$.

Hence LHS and RHS of Eqn. (2) simplifies to :

$$e(t_1 + t_2, A_s) = e(t_1, A_s).e(t_2, A_s) = e(d_1 Sk_A, A_s).e(d_2 A_r, A_s)$$
$$= e(d_1 zA, A_s).e(d_2 A_r, A_s) = e(A, A_s)^{d_1 z}.e(A_r, A_s)^{d_2}$$

and

$$e(k_1 B, A_s) = e(d_1 Sk_A + d_2 A_r + d_3 A_s, A_s)$$
$$= e(d_1 zA + d_2 A_r + d_3 A_s, A_s) = e(A, A_s)^{d_1 z}.e(A_r, A_s)^{d_2},$$

respectively.

RHS of (3) can be simplified as

$$e(t_1 + t_2 + t_3, A_s) = e(k_1 B - d_3 A_s + t_3, A_s)$$
$$= e(K_1 B + t_3, A_s).e(A_s, A_s)^{-d_3} = e(k_1 B + t_3, A_s)$$

which is the LHS of (3).

4.2 Comparison with Okamoto and Takashima Scheme

The primary aim of Okamoto and Takashima encryption scheme was to construct a two party protocol to securely evaluate a 2DNF formula over n variables. In their scheme[7], the decryption requires the computation of ECDLP. Hence in Okamoto and Takashima encryption scheme, the message is selected from a logarithmically small space. The proposed scheme requires six pairing computations whereas Okamoto and Takashima scheme requires four pairing computations. The security of both schemes are based on the hardness of VDP. But the complexity of message extraction after performing vector decomposition in Okamoto and Takashima scheme is exponential (unless the message is selected from a logarithmically small space). Since our scheme requires only $k_1 B$ (and not k_1), the key establishment is accomplished by the decomposition of B_c which can be done in polynomial time. Hence the computational complexity of our scheme is less than that of Okamoto and Takashima scheme.

5. SECURITY ANALYSIS

Security of our scheme is based on the hardness of vector decomposition problem and elliptic curve discrete logarithm problem (ECDLP). Since the curve used satisfies Yoshida conditions[1], VDP is atleast as hard as CDHP and even after $MOV\text{-}reduction$ DLP is hard on these curves. Hence the scheme is secure. *Theorem*1 by Okamoto and Takashima[7] compares the hardness of *gCVDP* and *gCDHP*

Although most of the schemes can agree on general definitions, their ideas diverge when precision is required and all attacks must be considered relative to the protocol goals[16]. We consider two types of adversaries as explained by Al-Riyami and Paterson[10] and Swanson and Jao[11]. *Type-I adversary* or *outside adversary* is one who can replace the public key of the user, but does not have access to the master secret key. If the adversary make *ReplacePublicKey* command, alteration will be made in the public parameters of party B. In Section 5.2 and proposition 5.1 in Section 5.1, we shown that the advantage of such adversary is negligible. *Type-II adversary* or *inside adversary* has the access to master secret key but cannot alter the public keys. Any adversary who knows the master key used in the scheme or the partial private key used in some session, gets negligible advantage. This is because extracting $K_1 B$ from B_c requires solving VDP, and hence only the receiver can compute $e(t_1, K_1 B)$.

So if $e(t_1, K_1 B) \neq e(t_3, Sk_B)$, the receiver can realize that it has not been sent by Alice.

5.1 Key Substitution Attack

Proposition 5.1 *Let* B', B'_r, B'_s *be the public keyss such that, for random* c_{ij} *with* $i, j = 1, 2, 3$,

$B' = B + c_{12}B_r + c_{13}B_s$, $B'_r = c_{22}B_r + c_{23}B_s$,
$B'_s = c_{23}B_r + c_{33}B_s$.

Then B',B'_r,B'_s can not be used to decrypt the ciphertext encrypted using B,B_r,B_s in the proposed scheme.

Proof: The encryption in the proposed scheme gives $B_c = k_1B + k_2B_r + k_3B_s$ where B,B_r,B_s are the encryption-equivalent public keys of Bob. Consider the ciphertext $B'_c = k_1B' + k_2B'_r + k_3B'_s$, obtained using encryption-equivalent public keys B',B'_r,B'_s.

$$B'_c = k_1B' + k_2B'_r + k_3B'_s = k_1(B + c_{12}B_r + c_{13}B_s) + k_2(c_{22}B_r + c_{23}B_s) + k_3(c_{23}B_r + c_{33}B_s)$$

$$= k_1B + (k_1c_{12} + k_2c_{22} + k_3c_{32})B_r + (k_1c_{13} + k_2c_{23} + k_3c_{33})B_s$$

Let X' be the trapdoor corresponding to B',B'_r,B'_s.

Then $VDeco(B'_C, < B' >, X', (B', B'_r, B'_s)) = k_1B'$ and $VDeco(B'_C, < B >, X, (B, B_r, B_s)) = k_1B$.

Let the x-coordinate of k_1B and k_1B' be u and u' respectively. Then $u \neq u'$.

Proposition 5.2 *Let* A', A'_r, A'_s *be the public keys such that* $e(A, A') = 1$, $e(A_r, A'_r) = 1$ *and* $e(A_s, A'_s) = 1$. *Then* A, A_r, A_s *does not act as signature-equivalent public keys in the proposed scheme.*

Proof: When the signature is verified, the first equation gives, $e(t_1, k_1B) = e(t_3, zB) = e(A, B)^{d_1k_1z}$.

Extracting k_1B from B_C is equivalent to solve VDP. Since B',B'_r,B'_s are the encryption-equivalent public keys, the attacker is able to find k_1B'. The complexity of finding k_1B using k_1B' is equivalent to the complexity of solving DLP. Since the curves are chosen in such a way that MOV-*reduction* is not applicable, finding k_1B is a hard problem.

Even if the attacker finds d_1zA' and k_1B, the signature verification gives :

$$e(d_1zA', k_1B) = e(A', B)^{d_1k_1z} \neq e(A, B)^{d_1k_1z}.$$

5.2 Man-in-the-Middle Attack

Man-in-middle attack can succeed only when an attacker can impersonate, hence exposing pairing operations to terminate. If an adversary *D* want to disrupt the communication, one method is to multiply every element of the packet sent by the sender by some random number, say *y*. Then the tuple becomes (yB_c, yt_1, yt_2, yt_3).

Then Eqn. (1) will disagree, since $e(yt_1, yk_1B) = e(A, B)^{y^2d_1zk_1}$ and $e(yt_3, Sk_B) = e(A, B)^{yd_1k_1z}$. Hence the key agreement scheme process is abandoned.

If the adversary keeps the tuple (yB_c, t_1, yt_2, yt_3) so as to satisfy Eqn. (1), then there will be conflict while verifying Eqn. (2).

LHS of Eqn. (2) simplifies to

$$e(t_1 + yt_2, A_s) = e(t_1, A_s)e(yt_2, A_s) = e(A, A_s)^{d_1z} e(A_r, A_s)^{d_2y}$$

But RHS of (2) simplifies to

$$e(yd_1Sk_A + yd_2A_r + yd_3A_s, A_s) = e(A, A_s)^{yd_1z} e(A_r, A_s)^{d_2y}$$

Hence the key agreement process is abandoned.

If the adversary keeps the tuple $(yB_c, t_1, yt_2, y^2t_3)$, so as to satisfy Eqn. (1), the Eqn. (3) is not satisfied and any alteration in t_2 will affect the Eqn. (2) in the verification process.

In all these cases the process is aborted. So change in any of the elements in the packet (B_c, t_1, t_2, t_3), sent by the user will make the process abandoned. Hence the scheme is resistant towards man-in-middle attack.

5.3 Forward Security

If any adversary is not able to realise any of the previously established keys on compromise of a long term secret key of any user, then the scheme is called forward secure. Extracting k_1B from B_c is equivalent to solve VDP with respect to the basis (B, B_r, B_s). Since k_1 and k_2 are random, B_c is random for each session. The elements of F_p are uniformly distributed and k_1,k_2 are selected with a probability close to zero. Hence the advantage of the adversary is negligible. Long term secret keys *zA* or *zB* will not give any advantage to the adversary to compromise the previous session keys.

5.4 Unknown Key Share Attack

This attack is possible if any two devices in the network use the same public key, say, *B*. If an adversary registers with the master authority using the public key of an existing user, say Alice, then the secret keys of adversary and Alice will be *zB*.

Since $B_c = k_1B + k_2B_r + k_3B_s$, knowing zB or zA will not give any advantage in decomposing B_c or altering the equations used for security check.

6. CONCLUSION

Network infrastructure requires security at an optimized cost without losing the speed of communication. This necessitates the introduction of authenticated key agreement schemes. A solution based on vector decomposition problem is suggested in this paper. Our scheme is a homomorphic encryption scheme which is simple and secure even with short ciphertexts. Our scheme has lower computational complexity while maintaining the same security of Okamoto and Takashima[5] scheme. We also showed that the key substitution attack by Lim[6], *et.al.* is not possible in this scheme. Further, this scheme can be extended to a multiparty key agreement scheme.

REFERENCES

1. Yoshida, M. Inseparable multiplex transmission using the pairing on elliptic curves and its application to watermarking. *In* Proceedings of 5th Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography, University of Tokyo, 2003.
2. Yoshida, M.; Mitsunari, S. & Fujiwara, T. Vector decomposition problem and the trapdoor inseparable multiplex transmission scheme based the problem. *In* the 2003 Symposium on Cryptography and Information Security SCIS'2003. pp. 491-496.
3. Duursma, I.M. & Kiyavash, N. The Vector Decomposition

Problem for Elliptic and Hyperelliptic Curves. IACR Cryptology ePrint Archive(2005). https://eprint.iacr.org/2005/031.pdf [Accessed on 15 July 2016]

4. Duursma, I.M. & Park, S. ElGamal type signature schemes for n-dimensional vector spaces. IACR Cryptology ePrint Archive, 2006. https://eprint.iacr.org/2006/312.pdf [Accessed on 15 July 2016]
5. Galbraith, S.D. & Verheul, E.R. An analysis of the vector decomposition problem. *In* Proceedings of International Workshop on Public Key Cryptography, PKC 2008: Springer Berlin Heidelberg, 2008. pp. 308-327.
6. Lim, S.; Lee, E. & Park, C.M. Equivalent public keys and a key substitution attack on the schemes from vector decomposition. *Security Communication Networks*, 2014, **7**(8), 1274-1282. doi:10.1002/sec.860
7. Okamoto, T. & Takashima, K. Homomorphic encryption and signatures from vector decomposition. *In* Pairing Based Cryptography-Pairing 2008. Springer Berlin Heidelberg, 2008, pp. 57-74.
8. Takashima, K. Efficiently computable distortion maps for supersingular curves. In Algorithmic Number Theory, Springer Berlin Heidelberg, 2008. pp.88-101
9. So, H.K.H.; Kwok, S.H.; Lam, E.Y. & Lui, K.S. Zero-configuration identity-based signcryption scheme for smart grid. *In* Proceedings of 1st IEEE International Conference on Smart Grid Communications, SmartGridComm 2010: Gaithersburg, Maryland, USA, 2010. pp. 321-326.
10. Al-Riyami, S.S. & Paterson, K.G. Certificateless public key cryptography. *In* Advances in Cryptology-ASIACRYPT 2003. Springer Berlin Heidelberg 2003. pp. 452-473.
11. Swanson, C. & Jao, D. A study of two-party certificateless authenticated key-agreement protocols. *In* Progress in Cryptology-INDOCRYPT 2009. Springer Berlin Heidelberg, 2009, pp.57-71.
12. Mandt, T.K. & Tan, C.H. Certificateless authenticated two-party key agreement protocols. *In* Advances in Computer Science-ASIAN 2006. Secure Software and Related Issues, Springer Berlin Heidelberg, 2006, pp.37-44.
13. Lippold, G.; Boyd, C. & Nieto, J.G. Strongly secure certificateless key agreement. *In* Pairing Based Cryptography-Pairing 2009. Springer Berlin Heidelberg, 2009, pp.206-230.
14. Boneh, D. & Franklin, M. Identity-based encryption from the Weil pairing. *In* Advances in Cryptology- CRYPTO 2001. Springer Berlin Heidelberg, 2001, pp. 213-229.
15. Mitchell, C.J. Making serial number based authentication robust against loss of state. *ACM SIGOPS Operating Sys. Rev.*, 2000, **34**(3), 56-59. doi: 10.1145/506117.506124
16. Boyd, C. & Mathuria, A. Protocols for authentication and key establishment. Springer Science & Business Media, 2013, pp. 321

CONTRIBUTORS

Mr Praveen I. received his MSc (Mathematics) from Cochin University of Science and Technology. Presently he is working as an Assistant Professor in the Department of Mathematics, Amrtia Vishwa Vidyapeetham (University), Coimbatore. His research interests include: Pairing based cryptography and elliptic curve cryptography.

In the current study, he performed the literature review, identified the significance of vector decomposition problem in key agreement and designed the scheme.

Mr Rajeev K. received his MSc from University of Calicut. He currently serves as Research Associate at TIFAC CORE in Cyber Security, Amrtia Vishwa Vidyapeetham (University), Coimbatore. His research interests include: Pairing based cryptography and cryptographic boolean functions.

In the current study, he contributed in the security analysis.

Dr M. Sethumadhavan received his PhD (Number Theory) from Calicut Regional Engineering College. Currently, he is working as a Professor in the Department of Mathematics and Computer Science, Amrita VishwaVidyapeetham (University), Coimbatore. His current research interests include: Cryptography and image processing.

In the current study, he contributed in the initial idea and verification of the scheme.