IJCTA, 9(10), 2016, pp. 4639-4645

Password Authentication Using Vector Decomposition

***Sreedevi M **Praveen I**

Abstract : The vector decomposition problem (VDP) is a computational problem on which security of many public key cryptosystems relies. Yoshida proposed VDP and also proved that VDP on two-dimensional vector space is at least as hard as the computational Diffie-Hellman Problem on its one-dimensional subspace. Okamoto and Takashima generalized VDP into higher dimensional vector spaces and provided a homomorphic encryption scheme. They also provided a protocol to securely evaluate a 2DNF formula. Partial password authentication is a novel method in financial cryptography, an authentication method which requires only arbitrary characters of the existing password. Using the homomorphic encryption scheme of Okamoto and Takashima, we propose a similar protocol to securely evaluate a 2DNF formula which provides partial password authentication.

Keywords : Vector decomposition problem, 2-DNF formula, Partial passwords

1. INTRODUCTION

Partial password authentication is a novel method in cryptography and getting familiar currently. Many online banking sites bring into play partial password authentication as one their authentication methods. Partial passwords can be described as a subset of characters from a full password. Since the user enters only a part of the password, full password is not revealed and hence guessing attacks and dictionary attacks possibility become less. As the user does not give the whole password in any instant, the number of attempts required to break the whole password increases. So that it can withstand dictionary attacks etc. Vector Decomposition Problem (VDP) was presented as another option for computationally hard problems like Discrete Logarithmic Problem (DLP) or Computational Diffie-Hellman Problem (CDHP). VDP was initially put forward by Yoshida[8]. The detailed study of VDP was done by Duursma,Kiyavash[2] and Galbraith, Verheul[3]. Yoshida proved equivalence of VDP and CDHP. In their paper ,Du-ursma and Kiyavash[2] demonstrated that genus 1 curves satisfying the conditions for equivalence of VDP and CDHP are super singular curves. MOV- reduction and FR- reduction attacks are possible in this curves. So the use of higher genus curves are required for VDP based schemes.

Okamoto and Takashima[6] extended VDP in to higher dimensions and proposed a homomorphic encryption scheme. The homomorphic encryption scheme is constructed on the trapdoor bijective function which is the secret key of VDP. As an application of homomorphic encryption, a Two party Protocol to securely evaluate a 2 DNF formula(over n variables) for higher dimensional n variables(assignments) was put forward by Okamoto and Takashima[6]. A disjunctive normal form (DNF) is a standardization of a boolean logical formula which contains only disjunctions and conjunctions of terms. 2-DNF can also be described as an OR of ANDs, or as a sum of products. A 2-DNF is a DNF formula where each term has at most 2 variables. Here we are considering a 2DNF

* TIFAC CORE in Cyber Security Amrita School of Engineering, Coimbatore Amrita Vishwa Vidyapeetham Amrita University India Email: sreedevim16@gmail.com,

** Dept of Mathematics Amrita School of Engineering, Coimbatore Amrita Vishwa Vidyapeetham Amrita University India Email: i_praveen@cb.amrita.edu

formula ψ over $y_1, y_2.....y_n$ (n variables) over (n variables) is of the form $\square_{i=1}^{n}(\square_{i,1}\ \square\square_{i,2})$ where (λ_i, 1 Λ λ_i, 2) = $y1, y...yn$

We propose a scheme for attaining authentication using partial entries of an existing password. Our scheme makes use of VDP based homo morphic encryption by Okamoto and Takashima[6] and a similar protocol used in[6] to securely evaluate a 2DNF formula in a two party protocol.

The rest of this paper is organized as follows: Section 2 explains about password authentication schemes, Section 3 gives some preliminaries and definitions. In section 4, we propose a partial password authentication scheme and also prove the correctness. Section 5 explains conclusion and future work.

2. PASSWORD AUTHENTICATION SCHEMES

In this section, various Password authentication schemes are discussed.

A. Password Authentication

Password is a set of characters or a word which only the claimant knows and kept as a secret from those who do not have access rights. The existing password authentication schemes can be categorized into strong and weak password authentication systems. Stronger password authentication protocol schemes are not supported in some environments. Weak password authentication schemes are using easier designs and implementations. To prove identity or access rights one has to provide a secret word. There are so many password based authentication schemes and some of the schemes are discussed below.

1. **Challenge Response :** In password authentication scheme, user needs to prove identity showing that she knows the password. Password is kept as a secret which only the user knows. But there can be many attacks possible in passwords as the user needs to send it through network. But however in challenge-response authentication scheme, she needs to just prove that she knows some secret which the user and the verifier have agreed upon previously. Mainly there are four different types of challenge-response password authentication scheme. Symmetric-Key Cipher, Hash Functions, Asymmetric-Key Cipher and Digital Signatures. In symmetric-key cipher, common key is used for both encryption and decryption. In asymmetric key cipher, public key is used for encryption and private key which only the user knows is used for decryption. Hash function based password authentication schemes work on by checking a hash value when user enters secret input. Digital signature schemes are used to authenticate documents and are verifiable in public. By verifying the digital signature, anybody can confirm that it is created by legitimate user.
2. **Zero Knowledge authentications :** In zero-knowledge authentication schemes, the user need not disclose the password. Instead user only needs to prove that she knows something which already the verifier and claimant agreed upon. The interactions are secure as secret is not revealed. The chance of guessing attacks is very less in this authentication scheme.
3. **One Time Password :** A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a session. OTP is valid only till that session expires. Security aspects, it is more secure than using a password for authentication, especially a user-created weak password. This can be used as second level of authentication where user already provided some other secret such as PIN, User ID for first level of authentication.
4. **Partial Password authentication :** A partial password [1] is a mode of password authentication which is getting popular now a days. This password authentication is mainly used in online banking and some financial sectors. Partial passwords can be described as a subset of characters from a full password. As only a part of the password is entered by the user, full password is not revealed and this makes guessing and dictionary attacks possibility very less. The user does not enter the whole password. So even if somebody is observing the data entered by the user for authentication, extracting the password requires

more number of trials. This partial password is able to withstand shoulder surfing attacks, key logging, man-in-the-middle attacks, phishing. David Aspinall of the University of Edinburgh and Mike Just of Glasgow Caledonian University [1] have studied various attacks possible on partial password authentication schemes. In their study, they have observed that many passwords used are very common and many letters are repeating. “a” was most used second letter character in the leaked database’s eight-letter passwords nearly 20 percent of the time, while “password” was the most-used password. Aspinall and Just have surveyed the major British banks, as well as banks in other countries that use partial passwords, and found that partial password scheme is efficient. Just has mentioned in their paper that a bank which uses short PIN as the first level of authentication is giving some additional level of security using the partial password authentication scheme.

3. BASIC DEFINITIONS AND PRELIMINARIES

Bilinear pairings are considered as one of the most important applications in public key cryptography. In 1988 Burt Kaliski used Bilinear Pairings in Cryptography in his PhD thesis. He did an innovative work on bilinear pairings for constructing pseudo-random number generators. But pairings came in to the picture of public key cryptography as the attack on elliptic curve cryptography namely MOV-reduction. But by the beginning of the millennium, pairing has become one of the most important tool in many cryptographic schemes such as identity based encryption, digital signatures, short signatures etc.

A. Bilinear Pairings

A bilinear map is a function $e : G_1 \times G_2 \rightarrow G_3$ where G_1

G_2 and G_3 are groups of large prime order.

The function $e(. . .)$ is such that for all $u \in G_1$, $v \in G_2$, $\in (u^a , v^b) = e(u, v)\, ab$, where a and b are integers[7]. Due to the property that they associate pairs of elements from G_1 and G_2 with an element in G_3, bilinear maps are termed as pairings.

Definition III.1. A bilinear pairing on (G_1, G_2) is an efficiently computable map $: G_1 \times G_1 : \rightarrow G_2$, which is bilinear and non-degenerate.

For all $a, b, c \in G$,

1. □ $(a + b, c)$ = □ (a, c) □ (b, c) 2. □ $(a, b + c)$ = □ (a, b) □ (a, c)

3. □ (a, b) $1, a$ $\neq$ b .

B. Vector Decomposition Problem (VDP)

The VDP is a computational hard problem on which the security of many public key cryptosystems relies. For certain curves, VDP is equivalent to CDHP in a cyclic group. To use VDP in cryptography setting up a trapdoor is required. Here we consider an l1 dimensional vector space. The collection of m-torsion points on an elliptic curve forms a vector space.

Definition III.2. Let V be a vector space over the field Fp and {P1, P2} is a basis for V . Let Q □ V . For a fixed base {P1, P2} VDP is defined as: Given Q □ V , compute the element R □ V such that R □ < P1 > and Q – R □ < P2 >.

Theorem III.1. [8] The following theorem of Yoshida Compares the hardness of VDP in a two dimensional vector space to that of CDHP in its one dimensional subspace. The VD Problem on V is at least as hard as CDH Problem on V′ C V if for any e □ V′ there are isomorphism fe, □ e: V → V which satisfy the following conditions

- For any *v*, □ *e*(V) and *fe*(*v*) are effectively defined and can be computed in polynomial time
- *e*, Fe(*v*) forms an F- basis for V
- There are α1; α2; α3 with
  $fe(e) = \alpha 1(e)$
  $fe(\square\, e\,(e)) = \alpha\, 2e + \alpha 3 \square\, e(e),$
  $\alpha 1, \alpha 2, \alpha 3 \quad 0$
- The elements α1,α2,α3 and their inverses can be computed in polynomial time.

Definition III.3. Let G be a group of exponent R and order R^2. Let f : G → G be a group isomorphism computable in polynomial time. A pair of elements S, T∈ G is an eigen vector base with respect to f if

1. G = < S, T >
2. $f(S) = \lambda_1 S$ and $f(T) = \lambda_2 T$ for some distinct nonzero
   $\lambda_1, \lambda_2 \in Z/rZ$

Definition III.4. An eigen vector base {S, T} is said to be a distortion eigen vector base If there are group homomorphism

$\square_1 : < S > \to < T >$ and

$\square_2 : < T > \to < S >$

computable in polynomial time and if an integer *d* not congruent to zero (mod *r*) is given such that

$$\square_2(\square 1(S)) = dS$$

Definition III.5. VDP in higher dimension Let V -be a l_1 Dimensional Fr vector space. Given *b*1….bl1 ∈ V and $\neq$

$x1 \ldots\ldots xl1 \in$ Fr and $v = \sum_{i=1}^{l1} x_i b_i$

The CVDP(l_1, l_2) is to find $v = \sum_{i=1}^{l2} x_i b_i$ which is in a subspace of V generated by the vectors $b_1 \ldots . b_{l2}$

Definition III.6. Projection Operator A :{$a_1 \ldots . a_{l1}$} be a distortion eigenvector basis of V, and a_i has its eigenvalue λ of *f*. The *j*th projection operator with respect to A such that

$Pr_j(a_k) = 0$ for $k \quad j$ and $Pr_j(a_j) = a_j$ is given by the polynomial of *f* $Pr_j \leftarrow \Pi_{i \neq j} (\lambda_i - \lambda_j))^{-1}\, \Pi_{i \neq j}(f - \lambda_i)$

If A = {$a_1 \ldots . a_{l1}$} be a distortion eigenvector basis of a vector space V and B = {$b_1 \ldots . b_{l1}$} is a basis generated from A with transformation matrix X = (*xij*) such that *bi* = ∑*xijaj* and *c* is a linear combination of vectors from B, then a one way function is defined as

$$\text{VDeco}(c, b_j, \text{X}, \ldots b_{l_1}) = \sum_{i=1}^{l_1} \sum_{k=1}^{l_1} t_{ij} x_{jk} (\Pr_i(c))$$

Lemma : If V is a distortion eigenvector space and (a_1, $a_2 \ldots a_{l1}$) is a distortion eigenvector basis with (b_1, $b_2 \ldots . b_{l1}$) generated by X = (*xij*) such that bi =∑*xijaj*, then V Deco solves VDP in polynomial time.

C. A Homomorphic encryption scheme based on Vector Decomposition

A homomorphic encryption scheme is constructed on the trapdoor bijective function is discussed in this section. This scheme is proposed by Okamoto and Takashima [6]. The homomorphic encryption scheme includes Key generation, Encryption and Decryption.

Key Generation

Let V : be a l1 dimensional vector space with distortion eigenvector

basis A: {*a*1,...., *a*l1}and trapdoor X= (*xi*,*j*) with *x*{*i*,*j*} Fr, *i*,*j* = 1,...l1

Bi = $\sum x_{i,j} a_j$ and B : (*b*1,.....,*b*l1}) (Basis generated using trapdoor). Here Secret key- Sk is X and Public key forms the set Pk is (V,A,B)

Encryption:

Enc(Pk,(m_1,.....,ml_2))

The message space is l_2. User enters the password bits.$n = l_2$

(m_1,.....,m_{l2}) □ {1….T} r_{l2},....r_1 □ Fr

Encrpted ciphertext is computed as

$c \leftarrow \sum 11i = 1mibi + \sum 12 = 1ribi$

Return Cipher text *c*.

After encryption function cipher text is returned.

Decryption:

Dec(S_k,*c*)

$b' \leftarrow$ VDeco(*c*,<*b*1,...., bl_2 >, X, B)}

$m'_1 \leftarrow \text{Dlog}_{bi}(b'_i)$ for $i = 1,.....l_2$

Return plain text (m'_1,...m'_{l2})

D. 2-DNF formula : In boolean logic, a disjunctive normal form (DNF) is a logical formula that contains disjunction and conjunctions. It is also defined as a sum of products. A 2-DNF is a DNF formula where each term has size at most 2. A 2DNF formula , over *y*1, *y*2... *yn* is of the form

□$_{i=1}^{n}$ (□$_{i,1}$ □□$_{i,2}$) (λi,1 Δ λi, 2) where (λi, 1Δ λi, 2) = *y*1, *y*2,...yn

As an application of homomorphic encryption, a Two party Protocol to securely evaluate a 2 DNF formula (over *n* variables) for higher dimensional n variables(assignments) is presented above and that scheme is used here. We consider a two party protocol between Alice and Bob. where Bob knows l2 dimensional secret input *m*1, *m*2....mn and Alice knows secret 2DNF formula ψ .Let l1 be the dimension of vector space, l2 be the dimension of subspace(Message space). (l1 > l2).n be the number of variables. (n = l1).VDP based homomorphic encryption can be used to securely evaluate two party protocol.

6. PROPOSED WORK

Here we propose our scheme based on VDP for partial password authentication by evaluating a 2DNF formula. We construct a two party protocol between Alice (server) and Bob (User) similar to one that is given in[6]. Alice builds the 2-DNF formula from the full password of Bob and uses this formula for validating the partial password Bob enters each time. The security of the system is that Alice cannot distinguish the assignments or inputs which the Bob enters when Alice asks for Password. And Bob knows whether the password is authenticated. Only Bob needs to enter the arbitrary positions in the password. Here Alice acts as verifier and Bob acts as claimant.

The following procedure is used for partial password authentication:

- Alice executes **Gen**(1^k) to compute Sk, Pk and sends Pk = (A_1, A_2,....A_n) to Bob.
- Bob encrypts the password(m_1, m_2,....*mn*) using Pk of Alice and sends C = $m_1A_1 + m_2A_2 +....+ m_nA_n$.
- Alice use VDeco (C,<A_i>, X, Pk) = m_iA_i

  for $i = 1,2..,l_1$.

  Let x_i be the *x*-coordinate of m_iA_i and let $x_i = x_{i1}\, x_{i_2}..x_{l_2}$, $l_2 < l_1$

- Alice calculates

$$\psi\ (x_{1,}x_2 \ldots x_n) = \left(\sum_{i=1}^{n} \lambda_{i11} . \lambda_{i21}, \ldots \sum_{i=1}^{n} \lambda_{i1/_2} . \lambda_{i2l_2} \right)$$

Where $\lambda_{i1j}, \lambda_{12j} \in \{x_{i1}, x_{i2}, \ldots x_{il_2}, 1 - x_{i1}, 1 - x_{i2}, \ldots 1 - x_{il_2}\}$for $j = 1,2 \ldots l_2$

- Alice generates $C_{11}= , \lambda_{i1,1} . \lambda_{i2,1}$ and
  $C_{i2} = . \lambda_{i1,12}\ \ \lambda_{i2,12}$ using Pk.
  i.e., $c_{i1} = \lambda_{i11} A_1 + \lambda_{i1l2Al2} + r_{i1l2\ +\ 1Al2\ +1} + _{ri1nAn}$
  $C_{i2} = \lambda_{i21} A_1 + \lambda_{i122Al2} + r_{i2l2\ +\ 1} A_{l2\ +\ 1} + _{ri2nAn}$
- Alice asks the i^{th} element m_i for arbitrary $i = 1,2,..,n$.
- Bob enters m_i for the corresponding i asked by Alice.
- When Bob enters m_i, the system generates $m_i A_i$
- Alice computes $\overset{*}{c_{i1}} = c_{i1} + \sum_{k=1}^{l_1} t_{i1k^{A_k}}; \overset{*}{c_{i2}} = c_{i2} + \sum_{k=1}^{l_1} t_{12k^{A_k}}$ and

  $E_k \sum_{i=1.}^{n} (\text{ti1kci2} + \text{t12kci1}) + \sum_{\mu \neq k,\ k=1}^{11} (\mu_{k\ \mu} A_\mu)$ and sends it.
- Alice generates random numbers $t_{ijk}(i = 1,2..\ n, j = 1, 2,\ \ k = 1, 2 \ldots .\ 11)$ such that $t_{ijk} = 0$
- Alice gets $(E_1, E_2,..,E_{l_2})$
- After getting $(E_1, E_2,..,E_{l_2})$Alice computes,

  $Z_k = \Pi_{i=1}^{n}\ e(\text{V Deco}(c_{i1} * < A_k >), \rho(e(\text{V Deco}(c_{i2} * < A_k >))) / e(\text{V Deco }(E_{k,} <A_k>, \rho(<A_k>)$
  for k = 1;, 2...
  Here V Deco(cij ,< Ak >) = V Deco(cij ,< Ak >,X;, Pk)
- Alice verifies the authentication by checking
  $Z_k = (e(A_k), \rho(A_k))^{W} k$ K=1,2…l2

Correctness of the scheme : Proposition: The proposed scheme above provides partial password authentication, with partial entries of the existing password.

Proof. Initially Alice computes Wk = $\sum_{i=1}^{n}, \lambda_{i1,1k.}\ \lambda_{i2,1k} + t_{i1,1k.} t_{i2,\ k}$

After getting $(E_1, E_2,.., E_{l_2})$Alice computes numerator as

$$e(\text{VDeco }(c_{i1} *<A_k>), \rho(\text{V Decom }(c_{i2} <A_k>))) = e(\text{Ak}, \rho(\text{Ak}))$$

$$\sum_{i=1,}^{n} k\ \lambda_{i1k}\ \lambda_{i2,\ k} . e(\text{Ak}, \rho(\text{Ak})) \sum_{i=1,}^{n} \lambda_{i1k}\ t_{i1k} . \lambda_{i2k}\ t_{i2k}$$

And then Alice computes denominator as

$$e(\text{V Deco}(E_k ,<A_k>), \rho(<A_k>) \text{ for } k = 1;2 \ldots 12 = e(A_k , \rho(A_k)) \sum_{i=1}^{n}, \lambda_{i1k}\ t_{i1k,} \lambda_{i2k}\ t_{i2k}$$

Hence $Z_k = \Pi_{i=1}^{n} e(\text{V Deco }(c_{i1} *<A_k>), \rho(e(\text{V Deco }(c_{i2} * <A_k>))) / e(\text{V Deco}(E_k ,<A_k>), \rho(<A_k>)$

Partial password is authenticated if $Z_k = (e(A_k), \rho(A_k))^{W} k$ K = 1,2…l_2

5. CONCLUSION AND FUTURE WORK

Partial password authentication is a novel method in cryptography. This helps the user to make the number of attempts of an attacker for breaking the password increase. Though the number of attempts increases, maintaining security is a major problem. Hence simple encryption methods based on harder assumptions are required. As a solution, we propose a method based on VDP. The method we have proposed in this paper is simple and secure.

6. REFERENCES

1. Aspinall, David, and Mike Just. "Give Me Letters 2, 3 and 6!: Partial Password Implementations and Attacks." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013. 126-143.
2. Duursma,I., Kiyavash,N.: The vector decomposition problem for elliptic and hyperelliptic curves. J. Ramanujan Math. Soc., 20, No. 1 (2005) 5976.
3. Galbraith, S.D., Verheul, E.: An analysis of the vector decomposition problem. In:Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 30827. Springer, Heidelberg (2008)
4. Silverman, J.H.: A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties. Pairing 2010. LNCS, vol. 6487, pp. 377-396. Springer, Heidelberg
5. Miller, V.,S.: The Weil pairing, and its efficient calculation. Journal of Cryptology 17(4), 235-261 (2004)
6. Okamoto,T.,. Takashima,K.: Homomorphic encryption and signatures from vector decom-position. In Pairing, pages 57-74, 2008
7. Praveen I, Sethumadhavan, M.: A More Efficient and Faster Pairing Computation with Cryptographic Security. In Proceedings of the first international conference on security of internet of things 2012 Aug 17 (pp. 145-149). ACM.
8. Yoshida, M.: Inseparable multiplex transmission using the pairing on elliptic curves and its application to watermarking. In: Fifth Conference on Algebraic Geometry,Number Theory, Coding Theory and Cryptography, Univ. of Tokyo (2003)
9. Duursma, I. M., Park, S. : ElGamal type signature schemes for n-dimensional vector spaces. IACR Cryptology ePrint Archive, 2006, 312.
10. On the Vector Decomposition Problem for m-torsion points on an Elliptic Curve Negar Kiyavash1 and Iwan Duursma Coordinated Science Laboratory, 1308 W.Mainst., Urbana, IL - 61801