Digital Signature Combined with Subliminal Channel and its Variants

Saumya Singh, Himanshu Agrawal

Abstract— **A subliminal channel or a covert communication channel, where the message is send to the authorized user. Only an authorized user can access this message. In digital signature implemented in a subliminal channel, subliminal message is embedded in the signature by the signer. Signature can we verified by any receiver but only authorized receiver can access the subliminal message. A discussion will be made on, 1.subliminal channel with two digital signature schemes constructed on discrete logarithms. 2. Threshold subliminal channel where message can be recovered with the help of t users among the authorized user. 3. A subliminal channel with an ID based signature scheme 4.Integrating subliminal channel with access control 5. An applications based on subliminal channel.**

Index Terms—**About four key words or phrases in alphabetical order, separated by commas.**

I. Introduction

Embedding subliminal message in the digital signature was introduced by Simmon, where the digital signature appears as a conventional digital signature. The subliminal channel has much application [10]. In digital signature, to communicate a signature α bits are used and to provide security against forgery, β bits are given, and α>β. Simmon explained that the channel is narrowband if it uses only a portion of α-β bits whereas if all or nearly all α-β bits are used then it is a broadband subliminal channel. Several narrowband subliminal channels were introduced by Simmon in which signer secret key is not known by receiver. Broadband channel was also presented by the Simmon , using DSA, in which the signer secret key is shared by receiver. Which make it prone to the forgery attack on the signer's given signature.

Besides Simmons's work, **Harn-Gong et.al.** proposed a scheme containing two digital signature with broadband subliminal channel[1], where the signer does not share secret key with the receiver but the size of the signature and secret key taken by the subliminal receiver and sender is very large. Therefore it does not provide protection against the forgery and conspiracy attack in which the receiver conspire to gain secret keys of both channel

Paper starts with two signature scheme combined with subliminal channel introduced by **Jan et.al. [1],** where different subliminal messages are embedded in the digital signature and then multiple receivers obtain the subliminal message from the received digital signature. Here the length is greatly minimized of the signature and length of both the secret keys of receiver and sender has been reduced efficiently. Conspiracy attacks still affects the scheme of Jan-Tseng broadband channel as it affects the Harn-Gong scheme of digital signature with subliminal channel. Both scheme has its security depends on the discrete lograthim problem computing difficulty.

Then the loop holes in the Jan-Tseng schemes was pointed, which was proved by **Lee et.al.** in 2003**[6]** and an improved version, Hess's proposed his work which is, ID- based digital signature scheme using bilinear pairing, against the security flaw. Lee-Lin proposed that Jan-Tseng scheme is vulnerable to dishonest subliminal receiver attack; attacker is one of the subliminal receivers who forge the subliminal message and send it to other subliminal receiver who extract it from the signature and accept it as a valid message. The ID dependent public key setting is an alternate option for public key setting based on certificate, particularly when an apt key management and medium key security is needed. **Xin et.al. [7]** proposed a scheme in which the subliminal message is covered by a temporary shared key produced by time stamp, an ID based signature scheme using bilinear pairing and it's security lies completely on the Diffie-Hellman problem of computation hardness assumption. One little drawback of the application, of ID-based signature scheme gets limited due to its easy construction of subliminal channel in the ID-based signature scheme. There scheme fulfill the properties, verifiability, non-repudiation, unforgeability and secure subliminal message.

Above all discussed subliminal channel, they all are separated. Therefore to compute a more extensive secret some subliminal receiver can cooperate together to find it . **lee et.al.[2]** proposed a threshold digital signature which is the modification of the Lee-Lin scheme which also verify the subliminal message to check its correctness. Use of A(t, n) concept in threshold system, where secret is shared among n users and it can be reconstructed with the cooperation of t or more subliminal receiver . **Huang et.al.** proposed multi –signature scheme for adhoc environment based on anonymity of threshold subliminal [4], in which a multi-signature scheme is proposed for discrete logarithm based keys or just a RSA –based keys and subliminal channel scheme combining threshold propoerties with a distinct characteristics of making the sender undistinguishable. The multi-signature is new signature in which multiple members of group, generate the signature with the help of many private keys. The feature making sender undistinguishable seems of extreme importance in prospect with security where the secret subliminal message is to be sent.

In the above scenario subliminal receiver will be able to get only one subliminal message. Two or more secret keys are required by the subliminal receiver in order to get two or more subliminal message. This is really unfeasible or not

Saumya Singh, Jaypee Institute of Information Technology Noida,Uttar Pradesh

Himanshu Agrawal, Jaypee Institute of Information Technology Noida,Uttar Pradesh

convenient when we talk about the hierarchical group of organization where the head has to maintain several secret keys. **Yang.et.al.** proposed the architecture of subliminal channel providing access control [5], which combine the concept of subliminal channel , digital signature and access control, so that the authorized receiver at the higher position can retrieve multiple subliminal message with the help of only one secret key. Two different scheme for user hierarchy have been proposed which is plaintext transmitted via subliminal channel and the other is cipher text transmitted via subliminal channel.

At last, paper discusses an application which uses the subliminal channel [10] , to notify the bank that he or she is suffering from blackmail and also on preventing people from generating false reports.

The rest of paper is described as follows. In section 2. Complete discussion on the digital signature combining subliminal channel and it modification as well as its variants. In section 3. Discussion has been made on the application based on subliminal channel and its usefulness. 4. The table has been made comparing the different variants and there advantages over others. Section 5. Conclusions and future work are made.

II. Various Digital Signature Combined Subliminal Channel Scheme

Many subliminal channel signature scheme are proposed by the different authors. Every scheme comes with its own pros cons. Each proposed scheme has its own benefits to cover the drawbacks of the other scheme and has its own disadvantages. This section summarize different digital signature scheme with subliminal channel. Different schemes have been described as follows: 1. Methodology, basic technique they have used 2.discription, every phase of signature generation and verification has been described 3. Security analysis which explains about the security provided by the particular signature scheme with subliminal channel.

A. *Discrete Logarithm based Digital signature with subliminal channel*

Methodology: Based on hardness of discrete logarithmic Problem

Description: There are two signature schemes, first one is for broad band channel and second one is for narrowband channel. The Jan-Tseng scheme consist of four stages: System initialization stage, Signature generation stage, Signature verification stage and the message recovery stage from subliminal channel.

1) A Broadband Subliminal Channel Integrating Jan-Tseng scheme

[System initialization]

q, large prime number, where it has a large prime factor q-1

1. p, a prime divisor and g, a generator having the order p in GF (q).
2. **Secret key of sender**: $x_1 є Z^*p$ and $x_2 є Z^*p$.
3. **Public key of sender**: $y = g^{-x1}.g^{-x2}$ mod q.

The secret keys are x_1 and x_2 are, among which at least one should be known by the subliminal receiver so that the subliminal message can be retrieved. Secret key, in a confidential manner is distributed to receiver by the signer .

Signer has public values as: (p, q, g, y)

Private Key of the first channel sender: (x_1)

Private Key of the second channel sender: (x_2)

[Signature creation and verification]

There is message m and subliminal message m_1 and m_2 which belong to Z*q, veiled in the first channel and second channel simultaneously.

the signature (e, s_1, s_2) is generated as follows:

$$e = h\,(g^{m1}.g^{m2} \text{ mod } q \,||\, m)$$
$$s_1 = m_1 + e \,.\, x_1 \text{ mod } p,$$
$$s_2 = m_2 + e \,.\, x_2 \text{ mod } p$$

Now, the signature (e , s_1, s_2) is send by the signer to the verifier.

When the signature (e, s_1, s_2) is received by ,any receiver the signature can be verified by calculating the given equation and whether the equation holds true or not.

$$e = h\,(g^{s1}.\, g^{s2}.y^{\,e} \text{ mod } q \,||\, m)$$

If true, then a valid signature of m.

[Message retrieval in subliminal channel]

Signature is verified by the first channel receiver and then it computes:

$$m_1 = s_1 - e.x_1 \text{ mod } p$$

The same process is followed by second channel receiver :

$$m_2 = s_2 - e.x_2 \text{ mod } p$$

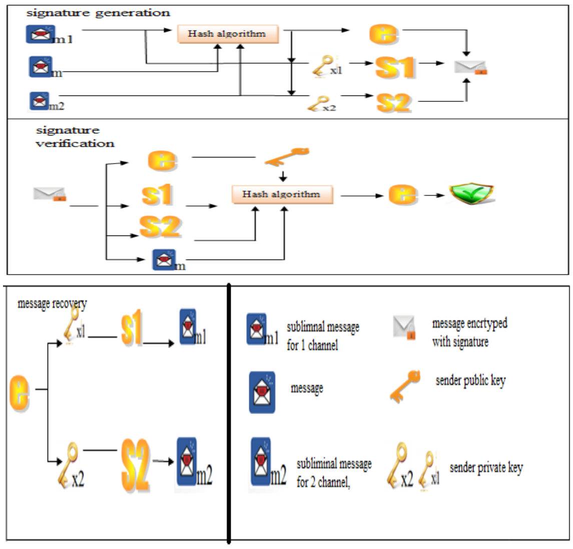


Figure 1:Broadband Subliminal Channel

2) A Narrowband Subliminal Channel Integrating Jan-Tseng Signature Scheme

[System initialization]

1. In this scheme ,a third channel is created by the signer.
2. q, prime number which is large ,where prime factor of q-1 is large.
4. p, is prime divisor and let a generator g having the order p in GF (q).
   Secret keys of sender: $x_1 є Z^*p$, $x_2 є Z^*p$ and $x_3 є Z^*p$
3. **Public key of sender**: $y = g^{-x1}.g^{-x2}.g^{-x3}$ mod q.

The secret keys are x_1 and x_2 , among which at least one should be known by the subliminal receiver so that the subliminal message can be extracted. Distribution of the Secret key by the signer to the receiver is done in a confidential manner .

Signer has Public values : (p, q, g, y)
First channel receiver secret key: (x_1)
second channel receiver secret key: (x_2)

[Signature creation and verification]

There is message m and subliminal message m_1, m_2 and random integer R which belong to Z*p, veiled in the first channel and second channel simultaneously.

The signer generates the signature (e, s_1, s_2) by computation as follows:

$$e = h\,(g^{m1}.g^{m2} \bmod q \,\|\, m)$$

$$s_1 = m_1 + e.\,x_1 \bmod p,$$

$$s_2 = m_2 + e.\,x_2 \bmod p$$

$$s_3 = R + e.\,x_3 \bmod p$$

Now, the signer sends the signature (e, s_1, s_2) to the verifier. Signature (e, s_1, s_2) is received by the any of the receiver, who can verify the signature by checking if the following equation is equal or not.

$$e = h\,(g^{s1}.\,g^{s2}.g^{s3}.y^{\,e} \bmod q \,\|\, m)$$

If it is true , then the signature is holds for m.

[Message retrieval in subliminal channel]

The signature gets verified by the authorized receiver and then computes:

$$m_1 = s_1 - e.x_1 \bmod p$$

Same process is followed by the second channel receiver. To excess the subliminal message

$$m_2 = s_2 - e.x_2 \bmod p$$

Security Analysis:

Size of the signature:

Size of the signature is greatly reduced in their scheme when related to the Harn et.al. scheme. Signature size in Harn et.al. scheme is 2048 bits and the2560 bits, size of the secret key, which means both keys are of 1024 bits each. While in their scheme the size of signature is 448 bits and 608 of broadband and narrowband simultaneously the size of the secret key of broadband and narrowband channel is 3|q| and |q|, where q is 160 bit.

Time complexity:

One way hash function h, needs T_h time for executing.

And modular multiplication needs time T_{mul} ,whereas modular exponentiation needs T_{exp}, computing Chinese remainder theorem comparing time is T_{CRT}. In the Horn-Gong scheme the time complexity of signature is $2T_{exp} + T_h + 2T_{mul} + 2T_{CRT}$, verification requires time complexity of $3T_{exp} + T_h + T_{mul}$ and message recovery needs $2T_{exp} + T_h$ whereas the scheme proposed for broadband and narrow band channel, requires time complexity for generation, ($2T_{exp}, T_h, 2T_{mul}$) ,($2T_{exp} + T_h + 2T_{mul}$ +) simultaneously , verification ($3T_{exp} + T_H + 2T_{mul}$), ($3T_{exp} + T_H + T_{mul}$) simultaneously and message recovery (T_{mul}) , ($2T_{exp} + T_h$) simultaneously.

B. *Various Digital signature scheme and threshold subliminal channel*

Threshold scheme A(t, n) grants to share the secret between n users where, secret can only be rebuild by the cooperation of t or more user. The threshold subliminal channel is equipped with the following characteristics: 1) The only work of sender is to develop a digital signature; 2)Subliminal message is extracted with the cooperation of group comprising of t or more 3) senders signature cannot be forged by the subliminal receiver; 4) It provides protection from the conspiracy attack; 5) Sublimnal message gets to be verified, which is sent by the sender. Many variations of signature of threshold subliminal channel have been developed [2, 3,4,8] which a step toward to provide more security to subliminal messages.

1) LEE-HO digital signature scheme with threshold subliminal channel

Methodology: Threshold system A(t, n) is the concept that secret is shared among n users , and the secret can only be computed with the help of t or more user cooperation.

Description: Lee-Ho consists of four stages Initialization stage, signature creation stage, signature verification and subliminal message retrieval and verification stage.

[Initialization phase]

1. A, is a sender u_1, u_2, u_3 , ……u_n, group B with n receivers.
2. q and p , two large primes with p|q-1
3. g_1,g_2……g_n, g_0, with order p in GF(q).
4. **Public key of A,** $y = \prod_{i=1}^{n} g_i^{\,xi} .g_0^{\,x}{}_0 \bmod q$
5. **Secret key of A,** x_1,x_2….. x_n, x_0 ….. Where x_i is secretly distributed to u_i.

[Signature creation]

A is the signer of message m.

1) u_i, has the identity Id_i, and m_o is the subliminal message. A (t-1) degree polynomial, A computes $f(x) = m0 + a_1x^1 + a_2x^2 + a_3x^3 + \ldots + a_{t-1}x^{t-1} \bmod p$, where $a_1 \ldots . a_{t-1} \epsilon$ Z*p. A secret shadow is computed then, m_i= f(Id_i) mod p for all u_i, i= 1,2…., n.

$$v = f(1) \bmod p \text{ and } R = (g_G^{m_G \oplus v}\, mod\ q) \bmod p.$$

2) $e = h(\prod_{i=1}^{n} g_i^{\,mi} . g_0^{\,k} mod\ p||m||R)$ where random number k ,one way hash function h , || is concatenation.
3) $s_i = m_i + e.x_i mod\ q$, where i= 1,2,….n , a s_g, conform the given equation as follows: $s_0.R = K + e.x_0 mod\ q$
4) Now, m has the signature as (e,$s_1, s_2 \ldots s_n, s_0, R$).

Message and signature is send to receiver B.

[Signature verification]

Receiver verify the signature by computing,

$$e = h\left(\prod_{i=1}^{n} g_i^{\,si} . g_0^{\,s_g R}. y^{-e} mod\ q||m||R\right).$$

Signature holds valid, if the above equation is true.

[Subliminal message retrieval]

Receiver will retrieve subliminal message m_i,

$$m_i = s_i - ex_i \bmod p.$$

The message can be verified by computing,

$$m_0 = f(0) = \sum_{i=1}^{t} m_i \prod_{j=1, j\neq i}^{t} \frac{0 - id_j}{id_i - id_j} \text{modp}.$$

(t-1) degree polynomial f(x) is reconstructed with the cooperation of all t receivers, and compute v=f(1) mod p, the validity of the subliminal message is checked as follows:

$$R = g_0^{\,m_0 \oplus v} modq) modp$$

If it holds the subliminal message is same as the message sent by the receiver.

Security Analysis

Secret shadow, till t users do not cooperate with each other the reconstruction of subliminal message is not possible as well as the signature cannot be forged because to make possible above three scenario attacker must reconstruct the polynomial f before which t shadows has to be retrieved, and getting the information of at least t shadows it is not easy as it is difficult as solving the discrete logarithm problem

III. MULTI-SIGNATURE SCHEME INTEGRATING THRESHOLD SUBLIMINAL CHANNEL OVER ADHOC-NETWORK

Methodology: A multi-signature scheme, which uses combination of discrete logarithm sort of keys and RSA type keys[3] with subliminal channel.

Description: In a multi signature design multi group members produce a special type of signature with the help of multiple private keys. A multi –signature scheme is used combined subliminal channel for the ad-hoc environment ,with a property to make sender of the subliminal message undistinguishable. It has five stages, initialization stage, subliminal message generation stage, signature creation stage, signature verification stage and subliminal message retrieval and verification stage.

[Initialization stage]
There are two type of keys are used in this signature scheme: DL type keys and RSA type keys.

- *DL –type keys generation*

1. p_i, $q_{i\,,}$ large prime that satisfy $q_i\,|\,(p_i\text{-}1)$.
2. g_i, denotes a prime subgroup of Z^*p_i, generated by g_i and order $q_{i.}$
3. **private key of receivers** : $x_i \epsilon Z^*q_{i\,,}$
4. **public key of receivers**: (y_i, p_i, q_i, g_i) where, $y_i = {g_i}^{x_i} mod\ p_i$

- *RSA-type keys generation*

1. p_{i1}, p_{i2}, be large primes,
2. $\Phi(n_i) = (p_{i1}\text{-}1)(p_{i2} - 1)$.
3. **Private keys of receivers**: (d_i, p_{i1}, p_{i2}) where, $d_i = {e_i}^{-1} mod \emptyset(n_i)$
4. **Public keys of receivers**: (e_i ,n_i) where, $e_i \in Z_{\emptyset(n_i)}$, such that gcd$(e_i, \emptyset(n_i)) = 1$ and $n_i = p_{i1}p_{i2}$.

Each user is required to send his key pair to the sender S(P_0) and then sender choses p, large prime less than p_{i1}'s, p_{i2} ‘s.

[Subliminal message preparation phase]
$M_{s,}$ be the subliminal message which belongs to GF(P)
P_1, p_2, ... , P_n is the receiver's m_s.

1) (t-1) degree polynomial $f(x) = m_G + a_1x^1 + a_2x^2 + a_3x^3 + \ldots + a_{t-1}x^{t-1}$ is chosen by S, in GF(P). A secret shadow is computed then, $m_i = f(id_i)$ for all P_i's, i=0, 1,2…., n.
2) S computes v=f(1) and $R = m_s \oplus v$).

[Signature generation phase]
Let m be the message signed, S computes,

1) $c_i \begin{cases} g^{m_i} & mod\ p_i & DL - type \\ {m_i}^{e_i} & mod\ n_i & RSA - type \end{cases}$,for i= 0, 1,...n;
2) $c = (m\|R\|c_0\|c_1\|c_2\| \ldots \|c_n)$
3) $s_i \begin{cases} m_i - cRx_i & mod\ q_i & DL - type \\ (c_i - \ cR)^{d_i} & mod\ n_i & RSA - type \end{cases}$, for i=1,2,…n

Signature is,

$$\sigma = (m, R\ , c, s_0, id_0, s_1, id_1, s_2, id_2 \ldots s_n id_n)$$

[Signature verification phase]
The signature is valid if it holds true,

$$c = (m\|R\|{g_0}^{s_0}{y_0}^{cR}\| \ldots \|{g_i}^{s_i}{y_i}^{cR}\|cR + s_{i+1}^{e_{i+1}}\| \ldots \|cR + s_n^{e_n})$$

[Subliminal message recovery and verification phase]
P_i receivers retrieves m_i:

$$m_i = \begin{cases} s_i + cRx_i & modq_i & DL - type \\ ({s_i}^{e_i} + cR)^{d_i} & mod\ n_i & RSA - type \end{cases}, \text{for i= 1,2,..n}$$

Any, t users will cooperate P_1, P_2,…, P_t to calculate f(x) in GF(P),

$f(x) = \sum_{i=1}^{t} m_i \prod_{j=1, j\neq i}^{t} \frac{x - id_j}{id_i - id_j}$, and recover the $m_{s.}$

Compute v=f (1), and compute R=H ($m_s \oplus v$).

Security Analysis

Secret shadow, subliminal message cannot be reconstructed unless the cooperation of t users as well as the signature cannot be forged because to make possible above three scenario attacker must reconstruct the polynomial f before which t shadows has to be retrieved , and getting the knowledge of at least t shadows it is as difficult as solving the discrete logarithm problem. People assume that it is multi-signature signed by n+1 user while only P_i user know that it is signed by t user, hence making the sender anonymous . Since, it uses two keys it is suitable for ad-hoc networks.

IV. RSA DIGITAL SIGNATURE MODEL INTEGRATING THRESHOLD SUBLIMINAL CHANNEL

Methodology: In this model, Lagrange interpolating polynomial is used. Between n subliminal receivers, the secret shadow of RSA is distributed.

Description: The digital signature combined threshold (t, l) subliminal channel design is based on RSA signature scheme, is efficient and secure. It consist of four stages; initialization stage, signature creation stage, signature verification stage and subliminal message retrieval and verification stage.

[Initialization phase]

1. A is the sender and v_1, v_2,…v_l are subliminal receivers with id's id_1, $id_{2\ldots\ldots..}id_{l.}$
2. p, q are two large primes, where m=pq,
3. $\Delta = (l\text{-}\ 1)!$, a ,b ϵ Z ø(m)* are secret of A such that,
$$a\Delta + d_0 = 1mod\emptyset(m)$$
4. **Public key of A**: (m, d_0) are public keys, where d_0 ϵ ${}_R$Zø(m)*, such that, d_0e_0= 1mod ø(m) where ø(m) is a Euler function.
5. **Private key of A:** e_0 where**,** e_0 ϵ Zø(m)*
6. A (t-1) degree polynomial ,$f(x) = ae_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{t-1}x^{t-1}$mod ø(n), where, a_1, a_2,…$a_{t-1}\epsilon_R$Zø(m)* are randomly selected by A. $e_i = f(id_i)$ where i= 1, 2,…,l,

e_i is secretly transferred to v_i from A.

[Signature generation phase]
Let m be the message and m_{sub} be the subliminal message, the identity number of the signature be u, where u<= m.
A computes,

$$r1 = (m_{sub} \oplus u \oplus m)^{d_0} mod\, m\, , r_2 = r_1{}^{b} mod\, m\, and$$

$$r = r_1 \| r_2\, ,$$

$$s_u = [H(m\|r\|u)^d]modm\, .$$

Signature is, (r, u, s_u).

[Signature verification phase]
Signature holds valid only when,

$$H(m\|r\|u) = s_u{}^{e} mod\, m.$$

[Message recovery and verification]
w, the current identity number of the signature and C={v_1,v_2…v_t}, who are t active subliminal receiver.
C computes,

1. if u>w , if not then there is resent attack.
2. $s_i = r_1^{\Delta e_i \prod_{j=1,j\neq 1}^{t} [\frac{-id_j}{id_i - id_j}]} mod\, m.$, for v_i.

All of the s_i are pooled and the C computes :

$$m_{sub} = [r_2 (\textstyle\prod_{i=1}^{t} s_i) mod\, m] \oplus u \oplus m.$$

Security Analysis

It is not possible to reconstruct subliminal unless t users do not cooperate with each other, as well as the signature cannot be forged, because to make possible above scenario attacker must reconstruct the polynomial f before which t shadows has to be retrieved , and getting the information of at least t shadows is as challenging as solving the problem of discrete logarithm. Signature and subliminal message cannot be resent by the adversary, which depends on the identity number (u, w) which is from 1 to m ,where m is very large that it is tough to factor. Subliminal message in this scheme is the random meaningful message and it secure from conspiracy attack.

V. Schnorr Digital Signature Scheme with Threshold Subliminal Channel

Methodology: Schnorr digital signature method is used along threshold subliminal channel, and it has its security based on double hard problem, discrete logarithm computation and factoring problem

Description: the Schnorr signature under modular m is used in this scheme. It consists of four stages; Initialization stage, signature creation stage, signature verification stage and message retrieval and verification stage.

[Initialization phase]

1. S is the sender and B=(v_1, v_2,….v_l) be the authorized receivers with identities id_1, id_2, ….id_l.
2. p, q with large primes of equal length such that p1 = (p-1)/2 and q1= (q-1)/2, two large primes .
3. Let, m=p,q and n= p1q1, and g ϵ Z_m* number of order n and modular m.
4. H{0, 1}*→ Z_n $H(0,1)^* \rightarrow Z_q 1$, both are one way hash function and (q1-1) = 2q2 ,which is large prime.
5. **Private key of A:** x , where v ϵ $z_q{}^*$, randomly selected by S and x= vq1.
6. **Public key of S:** (y, m) where, $y =$ g^xmod m
7. A chooses bϵZq1* and calculates e ϵ Z_{q1}*, such that, eb= 1mod(q1-1)
8. A (t-1) degree polynomial ,f(x) = e+ $a_1x + a_2x^2 + a_3x^3 + \ldots + a_{t-1}x^{t-1}$mod (q1-1), where, a_1, a_2,…a_{t-1}ϵZ_{q1}* are randomly selected by A. e_i = f(id_i) where i= 1, 2,…,l.

e_i is secretly transferred to v_i from A.

[Signature generation]
m_{sub} be the subliminal message, M be the message and when signature is generated timestamp T is also generated . A selects k ϵ Z_n*.
A computes:

$$c = [H_1(M\|T) \oplus m_s ub]^b mod\, q1,$$

$$r = g^{c+kq^1} mod\, m,$$

and

$$s = c + kq^1 + xH(M\|T\|r)modn$$

Signature is: (r, s)

[Signature verification phase]
The signature (r, s) finds to be valid if it follows:

$$g^s = ry^{H(M\|T\|r)} mod\, m$$

[Subliminal message recovery and verification phase]
C={v_1,v_2…v_t}, who are t active subliminal receiver, then C computes q1= (q-1)/2,

$$C = smodq^1 and\ s_i = c^{e_i \prod_{j=1,j\neq 1}^{t} \left(\frac{-id_j}{id_i - id_j}\right)} mod\, q^1.$$

The message can be verified, C pool all their s_i, and compute,

$$m_{ubs} = \left(\prod_{i=1}^{t} s_i\right) modq^1 \oplus H_1(M\|T).$$

Security Review

It is not possible to reconstruct Subliminal message , till t users co-operate as well as the signature cannot be forged because, to make possible above scenario attacker must reconstruct the polynomial f before which t shadows has to be retrieved , and getting the knowledge of at least t shadows it is as difficult as solving the problem of discrete logarithm. Signature and subliminal message cannot be resent by the adversary, because message and signature is sent with the time stamp which identifies if the message has been resent. It is secure from conspiracy attack. The security of this model is dependent on discrete logarithm computation, double hard problem and factoring problem.

C. ID-Based Digital Signature Integrating Subliminal Channel

Key management is simplified by the ID-based cryptosystem. ID-based signature is implemented by generating private key of the user through, private key generation (PKG), a trusted third party. Signers and PKG shares the secret key. Therefore a subliminal message is communicated to the PKG by the ID-based signer through the subliminal channel. Based on the bilinear pairing [6, 7] the ID-based signature scheme integrating subliminal channel is proposed.

VI. THE BROADBAND SUBLIMINAL CHANNEL IN HESS'S ID-BASED SIGNATURE SCHEME

Methodology: An Hess ID-based signature[6] with subliminal channel, whose security relies on the computation difficulty of Gap Diffie-Hellman problem(GDH) and Discrete logarithm problem , A category of problem where DDHP is easy and CDHP is hard .

Description: This scheme has four stages: signature initialization, signature creation, signature verification and message retrieval stage.

[Initialization phase]

1. G_0, a GDH group of prime order p
1. e: $G_0 \times G_0 \rightarrow G_{1'}$, is a bilinear pairing.
2. Q, is a generator of G_0 whose points will be located on elliptic curve.
3. Master key of trust authority (TA): s, where $s \in Z_p *$ and set $Q_{pub} = sQ$.
4. H_1:{0, 1}* → G_0 and H:{0, 1}* → Z_p , both be the cryptographic hash function
5. The system parameters are, $PARAMS\{G_0, G_1, p, Q, Q_{pub}, H, H_1\}$.
6. **Public Key:** P_{ID}, given identity id.
7. **Private Key**: $S_{ID} = sP_{ID}$.

The initialization stage is carried out by TA, and the subliminal receiver receives the secret key SID which is sent in a confidential environment by the signer.

[Signature generation]

Let the embedded subliminal message m_{sub} as an element R_{sub} of G_0.A computes,

$$r = e\ (R_{sub}, Q).$$
$$u = H(m \| r).$$
$$V = uS_{ID} + R_{sub..}$$

The signature is (V,u)

[Signature verification]

The receiver computes the equation for the verification of the signature validity:

$r = e\ (V, Q)\ e\ (P_{ID}, Q_{pub}{}^{-u})$.

Signature will be accepted if:

u= H $(m \| r)$.

[Message recovery]

Compute $R_{sub} = V - uS_{ID}$ and decodes R_{sub} to find m_{sub}.

VII.THE NARROWBAND SUBLIMINAL CHANNEL IN HESS'S ID-BASED SIGNATURE SCHEME

Methodology: An ID-based signature integrating subliminal channel, security is dependent on the computation hardness of Gap Diffie-Hellman problem (GDH) and Discrete logarithm problem and a class of problem where DDHP is easy CDHP is hard .

Description: It scheme has four stages; signature initialization, signature generation, signature verification and message recovery phase.

[Initialization phase]

1. G_0, is additive cyclic group and G_1 is a multiplicative cyclic group of prime order p.
2. e: $G_0 \times G_0 \rightarrow G_1$, is a bilinear pairing.
3. Q is a generator of G_0 whose points will be located on elliptic curve.
4. Master key of trust authority (TA): s, where $s \in Z_p *$ and set $Q_{pub} = sQ$.
5. Two cryptographic hash function, H_1:{0, 1}*→ G_0 and H:{0, 1}*→ Z_p.
6. The system parameters are, $PARAMS\{G_0, G_1, p, Q, Q_{pub}, H, H_1\}$.
7. Sender computes r' = $e(Q, Q)^{k'}$ where$k' \in_R Z_p{}^*$.
8. **Public Key**: P_{ID}, given an identity id.
9. **Private Key**:$S_{ID} = sP_{ID}$.

The initialization phase is carried out by TA, and the subliminal receiver receives the secret key SID,r' in a secret way by the signer.

[Signature generation]

Let the embedded subliminal message m_{sub}. A computes,

$r = e\ (Q, Q)^{k' + m_{sub}}$.

u= $H(m \| r)$.

$V = uS_{ID} + (k' + m_{sub})Q$.

The signature is (u, V).

[Signature verification]

The subliminal message computes the equation by verifying the validity of the signature

$r = e\ (V, Q)\ e\ (P_{ID}, Q_{pub}{}^{-u})$.

Signature will only be accepted if:

u= H $(m \| r)$.

[Message recovery]

Compute $r' = e(Q, Q)^{k'}$ .to get k'.

Since m_{sub} is random therefore,

$K = k' + m_{sub}$

Security Analysis

Bilinear pairing is used by the ID-based signature scheme, which makes the scheme efficient as well as gives proof of security, which is provided by relative Diffie Hellman problem. Since the key is generated by the PKG it is secure, because PKG can only know about the subliminal message and can recover the message from the signature. It protects from non-repudiation, because Trust Authority checks here recover the message means if signer has signed the message he cannot deny the it. Though, its broadband channel scheme is not safe from the message chosen attack.

VIII.XIN-LI ID-BASED SIGNATURE SCHEME INTEGRATING SUBLIMINAL MESSAGE

Methodology: ID-based signature scheme is used with subliminal channel whose security is based on hardness of computing Diffie- Hellman problem (CDHP).

Description: A novel ID-Based signature scheme [7] is proposed and then subliminal channel is constructed. It has properties like verifiability, enforgeability, non-repudiation etc. It consist of four stages: Initialization stage, signature creation, signature verification and message retrieval stage.

[Initialization stage]:

1. G_0, is additive cyclic group and G_1 is a multiplicative cyclic group of prime order p
2. e: $G_0 \times G_0 \rightarrow G_1$, is a bilinear pairing.
3. Q, is a generator of G_0 whose points will be located on elliptic curve.
4. Master key of trust authority (TA): s, where s ϵ $Z_p *$ and set $Q_{pub} = sQ$.
5. Ho:{0, 1}*→ G_0 and H_1:{0, 1}*× $G_1 \rightarrow Z_p$, both are cryptographic hash function.
6. The system parameters are,$\{G_0, G_1, p, Q, Q_{pub}, H_0, H_1\}$.
7. **Public Key**: $P_{ID} = H_0(ID)$, ID be the given identity.
8. **Private Key**: $S_{ID} = sP_{ID}$.

The initialization phase is carried out by TA, and the secret key S_{ID} is send by the PKG, to the user in a secret way. The user accepts it only if,

$$e(S_{ID}, Q) = e(P_{ID}, Q_{pub}),$$

[Signature generation]
Let the message to be signed be m and the signer selects random R ϵ $G_{0,}$ computes:
$v = H_1(m\|T, e(R, Q))$ and $U = R - vS_{ID}$,where time stamp T ,denotes at which time signature is generated.
The signature is: (T, v, U)

[Signature verification]
Signature is valid if, $v = H_1\left(m\|T, e(U, Q)e\left(P_{ID}, Q_{pub}\right)^v\right)$, it holds true.

[Message recovery phase]
PKG executes the following step to restorem_G,

$$t = H_2(m\|T, e(S_{ID}, H_3(m\|T))),$$
$$S_{ID} = sH_0(ID)$$
$$R = U + vS_{ID}, m_G = R/t$$

Security Analysis

Correctness of the algorithm is measured in this scheme using the properties of bilinear pairing. This scheme is secure from adaptive chosen message attack or existential forgery by the hardness assumption of Computational Diffie Hellman problem. At verifying stage the sender's identity is used ,therefore PKG can determine the corresponding signer of the subliminal message which provides non-repudiation. Since the message and signature is sent with the timestamp it is secure from the resending attack. Since only PKG and signer share hash function therefore adversary is not able to compute subliminal message from the signature.

D. ***digital signature with subliminal channel providing access control***

In above discussed schemes, each receiver can only get one subliminal message, if the receiver wants to get two or more subliminal message, then he is required to keep two or more secret keys. With the introduction of the access control, we use a user hierarchy, where, the receiver which is at higher position can access more than one subliminal message. Apart from this each subliminal receiver has to keep only one secret key and can use this secret key to retrieve the secret keys and subliminal message of other subordinates, and can access their secret information. Two different schemes have been proposed, 1) A subliminal channel transmitted in cipher text and 2) a subliminal channel transmitted in a plain text.

IX.DIGITAL SIGNATURE SCHEME WITH SUBLIMINAL PLAINTEXT CHANNEL

Methodology: The digital signature scheme with subliminal channel integrating access control is based on computing hardness of discrete logarithm problem (DLP).

Description:
shows the subliminal channel receivers hierarchy. User G_1 can access any information kept by other five user. $G_2, G_{3,} G_{4,} G_5, G_6$ are not allowed to access the information held by $G_{1.}$ This scheme consists of four phase, initialization phase, signature verification phase, signature generation phase and message recovery phase.

[Initialization phase]

1. G_s be the sender of the message and G_i be the receiver of the subliminal message.
2. p and q , two large primes with q|p-1
3. g_j generators with order q
4. **Public key of G_s**: $Y_s = \prod_{i=1}^{n} g_i{}^{-x_i} . g_7{}^{-x_s} \; mod \; p$.
5. **Secret key of G_s:** $x_s \; \epsilon \; Z_q *$
6. **Secret key of G_i′s:**x_i, where i=1,2,3,….,n.
7. **Secret key of G_j's** :If Gj has only one immediate predecessor G_i, $x_j = H(x_i, ID_j)$ else , G_s randomly chooses a secret key x_j for G_j.
8. ID_i , G_i identity where, i = 1,2,….,n.

G_2, G_3 will derive secret key of its subordinate G_5 where . G_s has to compute more than one public parameters:

$$r_{k5} = H(x_k, ID_5) \oplus x_5$$
$$where \; k = 2 \; and \; 3.$$

G_s transmits x_i to G_i

[Signature generation]
Sender signs a message m, and subliminal message $M_i \epsilon Z_q *$.
A chooses a random integer $R \epsilon Z_q *$. Then A computes,
$e = H\left(\prod_{i=1}^{6} g_i^{M_i} . g_7^R mod \; p\|m\right)$,
$s_i = M_i + ex_i mod \; q, i = 1, 2, \ldots, 6$
$s_R = R + ex_s mod \; q$.
Then the signature is, $(e, s_1, s_{2,} \ldots, s_6, s_R)$

[Signature verification phase]
The signature is valid if the following equation holds:

$$e = H\left(\prod_{i=1}^{6} g_i^{s_i} . g_7^{s_R} . y^e mod \; p\|m\right)$$

[Subliminal message recovery]

Subliminal message can be retrieved by three methods:

- Getting his/her own message

To restore M_i , x_i is used by the receiver,

$$\mathrm{M_i} = \mathrm{s_i} - \mathrm{ex_i} \mathrm{mod\ q}$$

- Getting subordinate's message

Subliminal receiver has a subordinate whose secret key is x_i. In order to get subordinate message , x_i is computed by the receiver and then x_j is used to get the message by computing:

$$\mathrm{M_i} = \mathrm{s_i} - \mathrm{ex_i} \mathrm{mod\ q}$$

- Getting the subliminal message M_5

  G_2, G_3 , compute secret values using their secret keys,

  $H(x_i, ID_5)$, i= 2 or 3, and derive $G_5's$ secret key x_5=$H(x_i, ID_5)\oplus$ r_{i5}, i=2 or 3. now M_5 can be recovered as,

$$\mathrm{M_i} = \mathrm{s_i} - \mathrm{ex_i} \mathrm{mod\ q}$$

X. DIGITAL SIGNATURE SCHEME WITH SUBLIMINAL CIPHER TEXT CHANNELS

Methodology: it uses symmetric key cryptosystem, in the scheme to secure the subliminal message embedded in the signature, while its security depends on Elagamal digital signature scheme.

Description: this scheme has four phases initialization phase, signature generation phase, signature verification phase and message recovery phase.

[Initialization phase]

1. A be the sender of the message and G_i be the receiver of the subliminal message.
2. p and q , two large primes with q|p-1
3. g, a generator with order q in GF(P).
4. **Public key of sender**: y_s, where,$y_s = g^{x_s} \mathrm{mod\ p}$.
5. **Secret key of A:** $x_s \in Z_q *$
6. **Secret key of $G_i's$:**x_i, where i=1,2,3,….,n.
7. ID_i , G_i identity where, i = 1,2,….,n.
8. E_x (), an encryption function with a symmetric key cryptosystem. D_x (), a decryption function with a symmetric key cryptosystem.

G_2, G_3 will derive secret key of its subordinate G_5 where . G_s has to compute more than one public parameters:

$$r_{k5} = H(x_k, ID_5)\oplus x_5$$

$$where\ k = 2\ and\ 3.$$

[Signature generation phase]

Let M, is the message signed be the sender and $M_i \epsilon Z_q *$ be the subliminal message, a random number k $\in Z_q *$ is

chosen by the A, and computes:

$c_i = E_{x_i}(M_i)$ i=1, 2, …. ,6 and
r=g^kmod p.

A finds s, to satisfy the equation,

H(m) = $x_s.H(c_1\|c_2\| ... \|c_6).r + ks\ mod\ q$.
The signature is, $(r, s, c_1, c_{2,...,}c_6)$.

[Signature verification phase]

If the following equation holds, the signature is true,

$$g^{H(m)} == y_s^{r.H(c_1\|c_2\|...\|c_6)}.r^s\ mod\ p.$$

[Message recovery phase]

- The receiver utilizes his secret key x_i to decrypt the cipher text as follows:

$$\mathrm{M_i} = \mathrm{D_{x_i}(c_i)},$$

- Getting subordinate's message

Subliminal receiver has a subordinate whose secret key is x_i. In order to get subordinate message, x_i is computed by the receiver and then x_j is used to get the message by computing

$$\mathrm{M_i} = \mathrm{D_{x_i}(c_i)},$$

- Getting the subliminal message M_5

  G_2, G_3 , use their secret keys to compute secret values, $H(x_i, ID_5)$, i= 2 or 3, and derive $G_5's$ secret key x_5=$H(x_i, ID_5)\oplus$ r_{i5}, i=2 or 3. now M_5 can be recovered as,

$$\mathrm{M_i} = \mathrm{D_{x_i}(c_i)},.$$

Security Analysis

Since the scheme is based on the hardness of discrete logarithm problem, the subliminal message cannot be accessed by the unauthorized user. Since the secret key of each user is signed with his own identity and predecessor secret key, therefore unless the one way hash function does not break the subordinate is not able to get the predecessor secret key. Since in plaintext scheme they only know the part of key therefore conspiracy attack is not possible and as with cipher text the hardness is based on Elgamal digital signature scheme.

Drawbacks of the above mentioned scheme is removed by Chang-Wu[9], who gave improved version of the subliminal channel with access control. They modified the generation procedure of of x_5 .Sender now computes $x_5^{'} = H(x_2 , ID_5), x_5^{''} = H(x_3 , ID_5)$, and the generates $G_5's$ secret key, $x_5 = g_7^{x_5^{'}x_5^{''}}$ Then the same procedure , same as Lee-Yang's procedure.

Here sender does not need to compute and make $r_{k5} = H(x_k, ID_5)\oplus x_5$ public. To compute M_5 , G_5 secret key has to be computed as

1) G_2 computes, $x_5^{'} = H(x_2, ID_5)$ and $r_{25} = g_7^{x_5'} \mathrm{mod\ p}$ and sends r_{25} to G_3
2) G_3 computes, $x_5^{''} = H(x_3, ID_5)$ and $r_{35} = g_7^{x_5''} \mathrm{mod\ p}$ and sends r_{35} to G_2
3) G_2 computes $x_5 = r_{35}^{x_5'} \mathrm{mod\ p}$.
4) G_3 computes $x_5 = r_{25}^{x_5''} \mathrm{mod\ p}$.

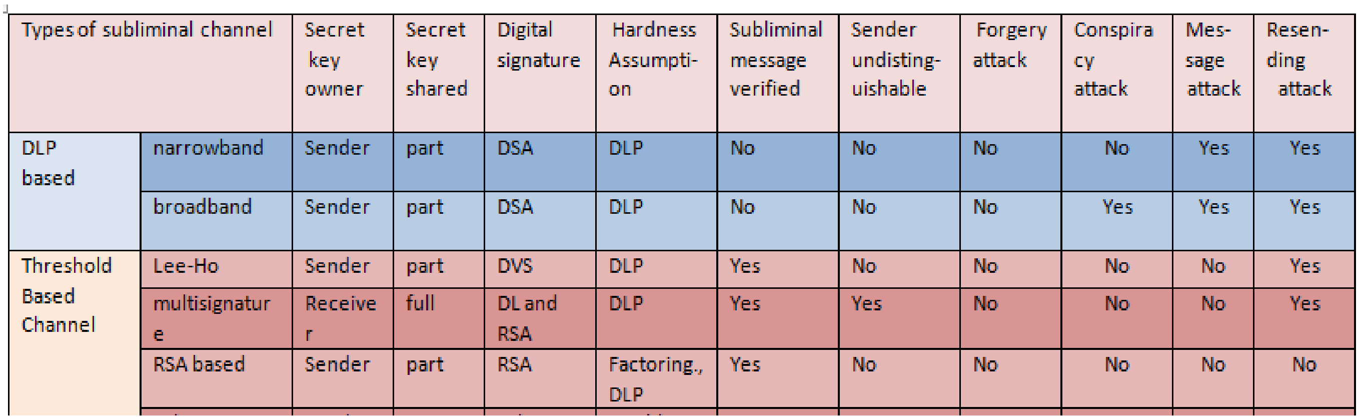
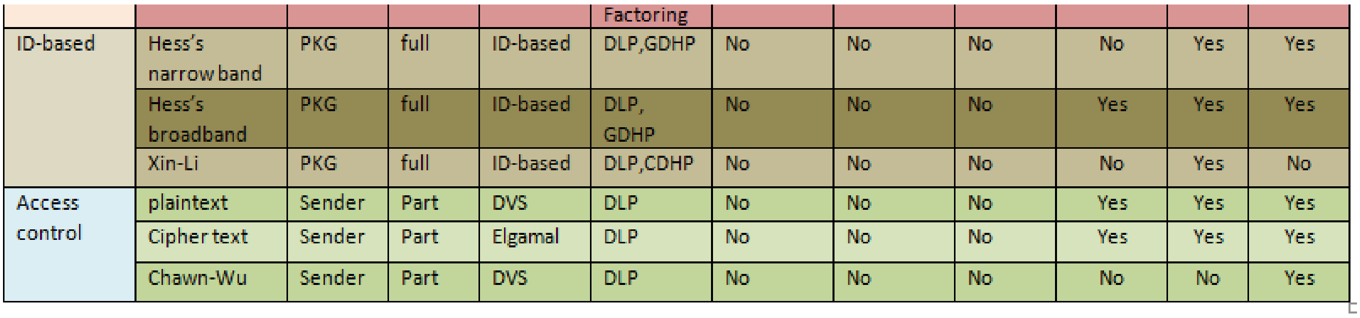


Figure 2:Differentiating Between different Types of Subliminal Channel



Types of subliminal channel		Secret key owner	Secret key shared	Digital signature	Hardness Assumpti-on	Subliminal message verified	Sender undisting-uishable	Forgery attack	Conspira cy attack	Mes-sage attack	Resen-ding attack
DLP based	narrowband	Sender	part	DSA	DLP	No	No	No	No	Yes	Yes
	broadband	Sender	part	DSA	DLP	No	No	No	Yes	Yes	Yes
Threshold Based Channel	Lee-Ho	Sender	part	DVS	DLP	Yes	No	No	No	No	Yes
	multisignature	Receiver	full	DL and RSA	DLP	Yes	Yes	No	No	No	Yes
	RSA based	Sender	part	RSA	Factoring., DLP	Yes	No	No	No	No	No
					Factoring						
ID-based	Hess's narrow band	PKG	full	ID-based	DLP,GDHP	No	No	No	No	Yes	Yes
	Hess's broadband	PKG	full	ID-based	DLP, GDHP	No	No	No	Yes	Yes	Yes
	Xin-Li	PKG	full	ID-based	DLP,CDHP	No	No	No	No	Yes	No
Access control	plaintext	Sender	Part	DVS	DLP	No	No	No	Yes	Yes	Yes
	Cipher text	Sender	Part	Elgamal	DLP	No	No	No	Yes	Yes	Yes
	Chawn-Wu	Sender	Part	DVS	DLP	No	No	No	No	No	Yes

Security Analysis

Since the scheme is based on the hardness of discrete logarithm problem, the subliminal message cannot be accessed by the unauthorized user. Since the secret key of each user is signed with his own identity and predecessor secret key, therefore unless the one way hash function does not break the subordinate is not able to get the predecessor secret key. Since in plaintext scheme they only know the part of key therefore conspiracy attack is not possible and as with cipher text the hardness is based on Elgamal digital signature scheme. They removed the drawback of Lee- Yang scheme by removing the message guessing attack and user key guessing attack to which the Lee-Yang scheme is vulnerable.

XI.AN APPLICATION BASED ON SUBLIMINAL CHANNEL

Subliminal channel has been proved fruitful for many applications such as:

1. The card holder's credit number and credit history can be hidden by the credit card provider.
2. If in a network everyone sends and receive signed messages and it is a spy network then, spies can send and receive their subliminal message in a digital signature to each other.

Since e-commerce is most popular these days, most of the criminal has taken their hold on it therefore eradicating malicious behavior and protecting one sensitive information is an important concern. Subliminal channel is mostly used method to send the secret message to the given receiver in a way to notify something important which is hidden from the other receiver. In this paper we have discussed the application in which, if someone is forcing the victim to transfer amount in his account, he can secretly send the subliminal message to his bank about being blackmailed by the criminal. In this process if any outsider checks the request message for transfer of amount to the bank by victim will not find anything doubtful, while checking the signature. Paper also clears the issue of false report generated by the victim of being blackmailed by the person.

To prevent higher level of security they are not transferring secret key in advance. They are constructing a session key according to RFC 2631.

Overview of application:

There are five parties in the given application:

Criminal(C) – vindictive person who blackmail a victim.

Victim(V) – A person who is blackmailed by a criminal.

Bank V(BV)- A bank which is responsible for victims transfer.

Bank C(BC)- A bank that has an account of criminal.

Official Agency(OA): An official law executive agency , which deals with illegal issue.

The process work as:

1. C threatens V, and blackmail him.
2. A forced message is sent to BV where in a secret message will be sent via subliminal message that the transfer is forced.
3. BV reports this blackmail to the OA.
4. OA sends the request to BC to freeze C's designated account after the funds have been transferred to the account.
5. OA reports the BC to continue the transfer processes, a session key is established by BV with BC via mutual authentication to transmit the transfer message.

Description:

The working of application is broadly divided into six phase, Constructing the session key model, Initialization phase, Login phase, Reporting blackmail to the official Agency phase, Freezing the account phase and Transfer phase.

1. ***Constructing the session key model:***
   The RFC 2631 was drawn up for this key agreement protocol. the session key in this protocol has two function:

1. V sends the transfer message to BV, then a session key will be generated to construct the subliminal channel.
2. Second session key is generated when BV reports blackmail to OA and BV sends transfer message of V to BC.

2. *Initialization phase:*

1. In this phase, Victim, Criminal, both the Banks and official authority generate their keys (P_x, S_x), where P_x is a public key and S_x be the secret key.
2. Victim and Criminal have their Account in BV and BC simultaneously.
3. M's, is a subliminal message according to victims login password .
4. $(ID_v, ACC_v, M_s{}')$, the victim's ID and Account in the BC's database.

3. *Login phase:*

Victim sends the forced transfer message to BV. BV checks the validity of message through timestamp which prevents from double sending.

1. K_{v-BV} , session key generated by both V and BV.

2. V computes:
   - k, where kϵ[0, p] and gcd(k, p-1)= 1;
   - $y_v = g^k \mathrm{mod}\, p$
   - $M_T = (ACC_v \| ACC_c \| AMOUNT)$ where, M_T is the transferred message ,ACC_c is the account of C and Amount is the amount to be transferred.
   - $r_v = H(y_V^k . PK_V^{(M_s + K_{V-BV})} \| M_t)$.
   - $s_{v_1} = K - k^{-1}\left(r_v + SK_v . H(M_T)\right)\mathrm{mod}p - 1$ and
   - $s_{V_2 =} M_s + K_{V-BV}\, \mathrm{mod}p$

Signature is, (S_{V_1}, S_{V_2})

3. Now, V sends to BV,
   - $C_{V-BV} = E(K_{V-BV}, \left(M_T \| s_{V_!} \| s_{V_2} \| Y_v \| r_v \| T_v\right))$.

T_{BV} , is the timestamp at which BV receives the ciphertext C_{V-BV}.

4. BV decrypts,
   - $\left(M_T \| s_{V_!} \| s_{V_2} \| Y_v \| r_v \| T_v\right) = D(K_{V-BV}, C_{V-BV})$
   - Validity of time is checked
     $(T_{BV} - T_V) \leq \tau$? where, τ is the expected time between Vand BV.
   - Then following equation checks the validity of signature:
     $$H\left(y_V^{s_{V1}} . g^{r_v} . PK_V^{H(M_r) + s_{V2}} \| M_T\right) = r_v?$$
   - After finding it true, it extract the subliminal message:
     $$M_s = \left(s_{v_2} - K_{V-BV}\right)\mathrm{mod}p.$$

$M_s \neq M_s{}'$, in the database of BV, transfer is forced, the transfer is normal.

4. *Reporting blackmail to the official Agency phase:*

When BV finds that V is under blackmail, It reports the OA.

1. K_{BV-OA}, session key of BV and OA.

2. $M_{blackmail}$, reporting message and is send to OA with V transfer message encrypted with session key:
   $$C_{BV-OA} = E(K_{BV-OA}, (M_{blackmail} \| M_T \| s_{v_1} \| s_{v_2} \| y_v \| r_v \| T_{BV} \| C_{V-BV} \| K_{V-BV}))$$

3. OA receives the message and perfoms the following function:
   - $(M_{blackmail} \| M_T \| s_{v_1} \| s_{v_2} \| y_v \| r_v \| T_{BV} \| C_{V-BV} \| K_{V-BV}) = D(K_{BV-OA}, C_{BV-OA})$
   - verifies the message as:
     $$H\left(y_V^{s_{V1}} . g^{r_v} . PK_V^{H(M_r) + s_{V2}} \| M_T\right) = r_v?$$
   - Session key is verified ,
     $$D(K_{V-BV}, C_{V-BV}) = (M_T \| s_{V_1} \| s_{V_2} \| y_V \| r_V \| T_v)?$$
4. Extract the subliminal message,
   $$M_s = (S_{v_2} - K_{V-BV}) \bmod p$$

If any mark found in M_S, OA freeze the account else if M_s is zero it rejects the request.

5. *Freezing the account:*

The account of C gets freezed at the BC.

1. OA does the following steps:
   - It chooses the parameter Kϵ[0, p] and gcd(k, p-1)
   - Generates freezing account message as, M_{FA}.
   - Computes:
     $$r_{OA} = g^K \bmod p$$
     $$s_{OA} = k^{-1}(M_{FA} - r_{OA} . SK_{OA}) \bmod p - 1$$

Signature (r_{OA}, s_{OA}) and M_{FA} is sent to BC as freezing witness.

2. BC verifies the validity,
   $$g^{M_{FA}} = PK_{OA}^{r_{OA}} . r_{OA}^{S_{OA}} \bmod p?$$

If the signature is true BC freezes the account.

6. *Transfer phase*

The BV transfers the money to the freezed account of C at BC.

1. $M_{transfer\ -continue}$ Message is send by OA to BV as:
   $$C_{OA-BV} = E(K_{BV-OA}, M_{transfer\ -continue})$$

2. BV decrypts the message C_{OA-BV} and constructs the session key K_{BV-BC}.

3. BV sends the encrypted V's transfer message and the receiving timestamp T_{BV} to BC as:
   $$C_{BV-BC} = E(K_{BV-BC}, \left(M_T \| s_{v_1} \| s_{v_2} \| y_v \| r_v \| T_{BV}\right))$$
4. BC does the following:
   - Decrypts message,
     $\left(M_T \| s_{v_1} \| s_{v_2} \| y_v \| r_v \| T_{BV}\right) = D(K_{BV-BC}, C_{BV-BC})$
   - checks the validity of signature:
     $$H\left(y_V^{s_{V1}} . g^{r_v} . PK_V^{H(M_r) + s_{V2}} \| M_T\right) = r_v?$$
   - If it is true it transfer the AMOUNT from $ACC_V - ACC_C$ and the decrypted message $\left(M_T \| s_{v_1} \| s_{v_2} \| y_v \| r_v \| T_{BV}\right)$ is stored in its database

and freezes the account in the content of freezing message and signature of OA.

C will not be able to withdraw the amount from the account ,OA will judge the case and finds out who is lying.

Security provided by the application:

This application is highly effective and works correctly[10], provides security and non-repudiation.the security provided by it as follows:

1. The account which is creating problem is traceable.
2. The application is able to distinguish between false and true report.
3. It provides non-repudiation in login phase and freezing account.
4. Secret has not to be shared in advance.

XII.CONCLUSION

In this paper we have discussed various types of digital signature with subliminal channel according to their hardness of the computing problem, their advantages and disadvantages. We represent the table of comparison between the entire algorithm in context of attacks they suffer from, Hardness assumption and secret key distribution. We conclude that above all algorithms discussed. They all suffer from common drawback that, they have to share with receiver their secret key which are a vulnerability to attack. In this paper we have discussed an application which provide to find the e-cash transfer blackmail message via subliminal channel . Our, future work will be to study algorithm where do not share their secret key and broadening the area of comparison among all the digital signature with subliminal channel as well we will try to cover advance application in subliminal channel.

REFERENCES

[1] J.Jan, Y. M. Tseng, “New Digital Signature with Subliminal Channel Based on Discrete Logarithm Problem, ” International Workshop on Parallel Processing, 21-24 Sep 1999, Wakamatsu Japan, pp.198-203

[2] N. Y. Lee and P. H. HO, “Digital Signature with a Threshold Subliminal Channel,” IEEE Transactions on consumers Electronics, vol.49, no.4, November 2003, pp. 1240-1242.

[3] G.Li, X. Xin and W.Li,”Digital Signature Scheme with a (t, l) Threshold Sublimnal Channel Based on RSA Signature Scheme,” Computational Intelligence and Security 2008, IEEE Computer security Press, vol.2, 13-17 Dec. 2008, Suzhou China pp.342-346.

[4] Husang. Z ., Chen. D. , Wang. Y. “Multi-signature with anonymous threshold subliminal channel for adhoc environment,” In Proceedings of the 19th International Conference on Advanced Information Networking and Application, 2005, 67-71.

[5] N.Y. Lee and S. Y. Yang, “The Design of integrating Subliminal Channel with Access Control,” Applied Mathematics and computation, Vol. 171, Dec 2005, No. 1, pp. 573-580

[6] F.Zhang, B. Lee, K.Kim, “Exploring Signature Scheme with Subliminal Channel,” SCIS 2003, The 2003 Symposium on Cryptography and information Security vol 1/2 , 26-29 Jan. 2003 , Itava, Japan , pp. 245-250.

[7] Xin Xiangjun, Li Qingbo, “Construction on Subliminal channel in ID-Based Signature,” Information Engineering, 2009. ICIE’09. Wase, International Conference on vol 2. 10-11 july 2009, pp. 159-162

[8] Xin Xiangjun, Zhi Guizhen, “A New Digital Signature Scheme with Threshold Subliminal Channel,” Information Engineering, 2009. ICIE’09. WASE International Conference on ,10-11 july 2009, Volume: 1 pp. 591-594

[9] Chin – Chen Chang and Chia-Chi Wu, “An Improvement of the Design of Integrating Subliminal Channel with Access control” in IAENG International Journal of Computer Science 32:4.

[10] Chin-Ling Chen, Ming-He Liu, “A traceable E-cash transfer system against blackmail via subliminal channel,” in Electronic Commerce Research and Application, Nov-Dec 2009, vol.8, pp. 327-333