Identity hiding by blind signature scheme

Conference Paper · December 2003

CITATIONS
0

READS
77

3 authors, including:

Salah Albermany
University Of Kufa
20 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Hamza Ali
University of Basrah
18 PUBLICATIONS **26** CITATIONS
SEE PROFILE

Identity Hiding by Blind Signature Scheme

Salah, Albermany,
Hamza A. Ali
and Abdulameer, K. Hussain

Computer Science Department, Zarka Private University, Jordan.

Abstract
Public key schemes use two keys, i.e. public key used for encryption and private key used for decryption. But still there is a major problem in these schemes, as cryptanalyst has access to the public key and the sender's identity, which might help him or her to break the system. This paper presents a method for public key hiding, i.e. the public key of the receiver will not be used directly in the encryption process rather a pseudo key will be used. This scheme guarantees reducing the risk of breaking both the encryption algorithm and the public-private key pair. Furthermore, this pseudo public key is generated independent of the sender, i.e. as blind signature is achieved by using another key as well as reduces breaking encryption method. This method is designed and experimented with to fit a group users-group manager environment.

Keywords
Cryptography, Public key, Blind Digital signature, DSS, Authentication.

1. Introduction

Public-key cryptography and related standards and techniques underline security features of many Netscape products, including signed and encrypted email, form signing, object signing, single sign-on, and the Secure Sockets Layer (SSL) protocol [1]. All communication over the Internet uses the Transmission Control Protocol/Internet Protocol (TCP/IP). It allows information to be sent from one computer to another through a variety of intermediate computers and separate networks before it reaches its destination.

The great flexibility of TCP/IP has led to its worldwide acceptance as the basic Internet and intranet communications protocol. Various ways of interference are common in communication systems although it is done by the utilization of TCP/IP [2], they can be summarized in the following.

Passive interference: As information leaks from the transmission channel, the privacy is compromised but the data remains intact. This is called eavesdropping, e.g. someone could learn your credit card number, record a sensitive conversation, or intercept classified information.

Active interference: This interference can be one of the followings:

- ***Tempering:*** Information is changed, delayed or replaced in transit, then sent on to the recipient. e.g. someone could alter an order for goods or change a person's resume.
- ***Impersonation:*** Information passes to a person who poses as the intended recipient. Impersonation can take two forms:

(1) *Spoofing:* A person can pretend to be someone else. e.g. a person can pretend to have the email address ameer@hotmail.com, when he is not.
(2) *Misrepresentation.* A person or organization can misrepresent itself. e.g. suppose the person with email address salah@yahoo.com pretends to be a representative salesman for a company when he or she is really just a person that takes credit-card payments but never sends any goods.

Common cryptosystems used for internet security are of two types. They can be either symmetric (secret key), where only one key is used for both sender and receiver or asymmetric (public key) where two keys are used, one public and the other is private . Examples of the most commonly used of the first type are Data Encryption Standard (DES) [3], triple DES [4], Advances Encryption System (AES) [5] and International Data Encryption Algorithm (IDEA) [6], while examples of the second type are RSA [7], ElGamal [8] and DSA [9]. There are some systems that employ mixed techniques of both types such as Pretty Good Privacy (PGP) [10]. It employs IDEA for data encryption and RSA for key distribution. Besides, there are many different security protocols such as Internet Protocol security (IPsec) [11], Virtual Privacy Network (VPV) [12] and many more.

As this paper will utilize the public-key systems for strong ways of digital signature and blind signature to group users, its definition, together with RSA scheme and blind signature will be presented in section 2 and 3. The proposed system for identity hiding using blind signature will be outlined in section 4. Then section 5 includes the suggested algorithm for the proposed system while few implementation examples are shown in section 6. Finally, the paper is concluded in section 7.

2. Background

2.1 Public-Key Encryption

Public-key encryption involves a pair of keys, public key KU and private key KR, associated with an entity that needs to authenticate its identity electronically, signs or encrypts data. Diffie and Hellman [13] achieved the astonishing idea of public key algorithm. It is found suitable for both security and authentication. It relies on two keys, one for encryption and a different but related one for decryption, where it is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key. One key is published (public), while the other is kept secret (private). Data encrypted with any one of them can only be decrypted with the other.

The implementation of this algorithm for security is illustrated in figure 1. For a message M to be sent from sender A to receiver B, it is encrypted using the receiver's public key KU_b, resulting into ciphertext C as

$$C = E_{KU_b}(M) \qquad (1)$$

while at the receiver, plaintext is recovered by a decryption process using the private key KR_b as

$$D_{KR_b}(C) \text{ ==> } M \qquad (2)$$

i.e. this message can only be recovered by the person who has the private key.
However, if the message is enciphered with the sender's private key, them it can be recovered by anybody who is using the public key. This ensures the authentication of the sender, i.e. digital signature.

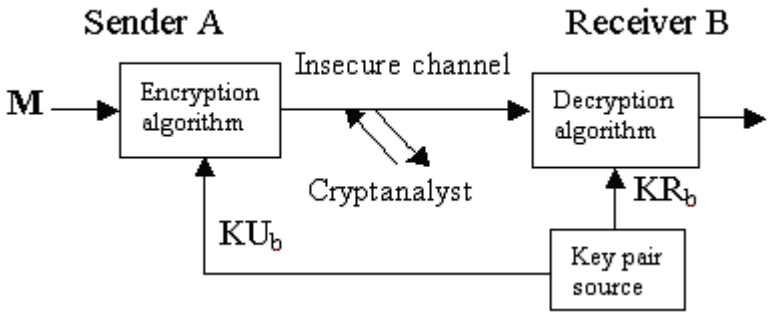

Fig 1. The Public Key Cryptosystem for security.

2.2 RSA Scheme

The most commonly used implementations of public-key encryption are based on algorithms patented by Rivest Shamir and Adleman, called RSA [7]. RSA scheme is based on modular arithmetic and relies in its security strength on the difficulty of factoring prime numbers. public and private keys are required for all users. For example having two users A & B, let e_A, N_A, e_B & N_B be the **public keys** and d_A & d_B be the **private keys** for these users, respectively. Simply, to sign a document M by sender A, the private key of the sender is first used to calculate a ciphertext called the signature S

i.e.

$$S = D_A(M) = (M)^{d_A} \bmod N_A \qquad (3)$$

This cryptogram is transmitted over an insecure channel. Any one can use the public key of A to recover the message M′ by performing the inverse of equation 3, i.e

$$E_A(S) = (S)^{e_A} \bmod N_A \Longrightarrow M' \qquad (4)$$

If M′ = M, then the message is authentic and we are sure that the message has been sent by the user who claims to be the sender. This is an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Communicator can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed, i.e. digitally signed.

For security, on the contrary, to send encrypted data to someone using RSA scheme, you encrypt the data with that person's public key. The receiver then decrypts the received cryptogram with the corresponding private key.

Data integrity is checked by this method, too. If M′ = M (i.e. they match), the data has not been changed since it was signed. If they don't match, the data may have been tampered with, or the signature may have been created with a private key that doesn't correspond to the public key presented by the signer.

Compared with secret-key system, public-key system requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key system for key distribution, which are used for encryption by secret-key cryptosystem, such as in PGP. This is the approach used by the SSL protocol [1].

2.3 Key Length and Encryption Strength

In general, the strength of any encryption method is related to the difficulty of discovering the key. It depends on both the cipher used and the length of the key, e.g. the difficulty of discovering the key for the RSA cipher depends on the difficulty of factoring large numbers, a well-known mathematical problem.

Generally, longer keys provide stronger encryption. Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher. Roughly speaking, 128-bit RC4 encryption is 3 x 1026 times stronger than 40-bit RC4 encryption.

Different ciphers may require different key lengths to achieve the same level of encryption strength. The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values. Thus a 128-bit key for use with a symmetric-key encryption cipher would provide stronger encryption than a 128-bit key for use with the RSA public-key encryption cipher. This difference explains why the RSA public-key encryption cipher must use longer keys, such as 512-bit key (or more) to be considered cryptographically strong, whereas symmetric key ciphers can achieve approximately the same level of strength with a 64-bit key. Due to the fast development of fast computers, even this level of strength may be vulnerable to attacks in the near future. For this reason, the U.S. Government for example restricts export of cryptographic software to a limited key length
of not longer than 40 bits for DES.

3. Blind signature

Blind signature scheme is proposed by David Chaum [14] in 1983. It is based on RSA signatures. It is a way of signing electronic data that can be authenticated without revealing the identity of the person who it was signed for [15]. In a blind signature scheme, the signers neither know the messages they sign, nor the signatures the recipients obtain for their messages. The signers have individual private signing keys and distribute their corresponding public verifying keys, just as in normal cryptographic signature schemes. Public verifying keys are distributed via authentication channels.

To clarify blind signature, chaum used RSA scheme as follows. Suppose Alice has a message M that she wishes to have it signed by Bob, and she does not want Bob to learn anything about M. Let (N, e) be Bob's public key and (N, d) be his private key. Alice generates a random value r such that gcd(r, N) = 1 and sends M' to Bob.

$$M' = r^e M \bmod N \qquad (5)$$

The value M' is "blinded" by the random value r, and hence Bob can derive no useful information from it. Bob returns the signed value S' to Alice, where S'.

$$S' = (M')^{d} \bmod N \qquad = r\,M^{d} \bmod N \qquad (6)$$

Since $S'=r\,M^{d} \bmod N$, Alice can obtain the true signature S of M by computing

$$S = S'\,r^{-1} \bmod N \qquad (7)$$

Now Alice's message has a signature she could not have obtained on her own. This signature scheme is secure provided that factoring and root extraction remains difficult. However, regardless of the status of these problems the signature scheme is unconditionally "blind" since r is random number. The random r does not allow the signer to learn about the message even if the signer can solve the underlying hard problems.

On a spectrum between keeping individuals accountable and protecting their identities against unduly propagation or misuse, blind signature schemes tend toward the latter extreme. In many applications this strongly privacy oriented approach is not acceptable in all circumstances. While the identities of honest individuals are protected in a perfect way, criminal dealings of not so honest individuals who exploit such systems to their own advantage are protected just as perfectly. For example, Naccache and van Solms [16] have described "perfect crimes" where a criminal blackmails a customer to withdraw a certain amount of money from his or her account by using a blind signature scheme and then deposit the amount into the criminal's account.

Trustee based blind signature schemes have been proposed to strike a more acceptable balance between keeping individuals accountable and protecting their identities. Stadler, Piveteau and Camenisch [17] have proposed fair blind signatures. Fair blind signatures employ a trustee who is involved in the key setup of the scheme and in an additional link-recovery operation between a signer and the trustee. The trustee can revoke the "blindness" of certain pairs of messages and signatures upon request. The link-recovery operation allows the signer or the judge to determine for each transcript M, S of the signing operation, which message M' has resulted for the recipient, or to determine for a given recipient's message M' from which transcript M & S have evolved. Similar approaches have been applied to constructions of electronic cash [18, 19].

Blind signatures have been employed extensively in cryptographic constructions of privacy oriented services such as untraceable electronic cash, anonymous voting schemes, and un-linkable credentials.

4. The Proposed blind signature scheme

4.1 Identity Hiding

Knowing the plaintext-ciphertext pairs and the public key would lead to ease the process of breaking the security system by the cryptanalysts. Therefore, hiding the sender’s identity by blind signature technique will make life more difficult for cryptanalysts. This paper suggests a method suitable for group users communication with group manager applications. In this method, the proposed public key for all users is hidden in a trustee

center in order to disguise all users. Then, a general public key is generated that will be used for sending encrypting documents. Therefore, any user will encrypt his or her message using this general public key and sends it to a secretary. This key does not reveal the sender's or receiver's identities.

Only after the identity of the sender is validated by the secretary that is responsible for the database confidentiality, it is accepted, signed be the secretary and sent to the intended manager for his attention. The secretary signs the document blindly, as he or she is only interested in its sender's identity but not its contents. The whole process can be summarized as follows.

Each manager generates two keys, one is private that he or she keeps for himself and one is public, gives to a key distribution center. For example manager 1 generates d_{M1} and e_{M1} respectively. Moreover, a secretary generates two respective keys d_S and e_S too. These keys are sent to the key distribution center, that will generate a general key k_{G1} as $e_{M1}\, e_S$. This key is then sent to trustworthy center, who will be made public.

Any member of the users group can encrypt a document M with key k_{G1} getting the Cryptogram C as

$$C = E_{k_{G1}}(M) \qquad (8)$$

Then, the cryptogram C is sent to the manager together with the user's ID through the secretary. This secretary checks the validity of the ID by directly consulting the database, then he or she signs blindly as

$$S = D_{k_S}(C) \qquad (9)$$

The manager uses his own private key to decrypt the received signed cryptogram. This step will recover the original clear message as follows

$$\begin{aligned} D_{d_{M1}}(S) &= D_{d_{M1}}(D_{k_S}(C)) \\ &= D_{d_{M1}}(D_{k_S}(E_{k_{G1}}(M))) \;\Longrightarrow M \end{aligned} \qquad (10)$$

The suggested scheme in this paper provided a method that gives three basic advantages, i.e. (1) The real public key of the receiver is not revealed publicly thus increasing the difficulties for cryptanalyst to compromise the key used or the algorithm implemented. (2) The secretary checks the validity of the sender's ID and (3) The secretary signs the document blindly, guaranteeing the sender validity and his or her authority for sending the message without knowing the clear content of the message. Figure 2 illustrates the whole security scheme.

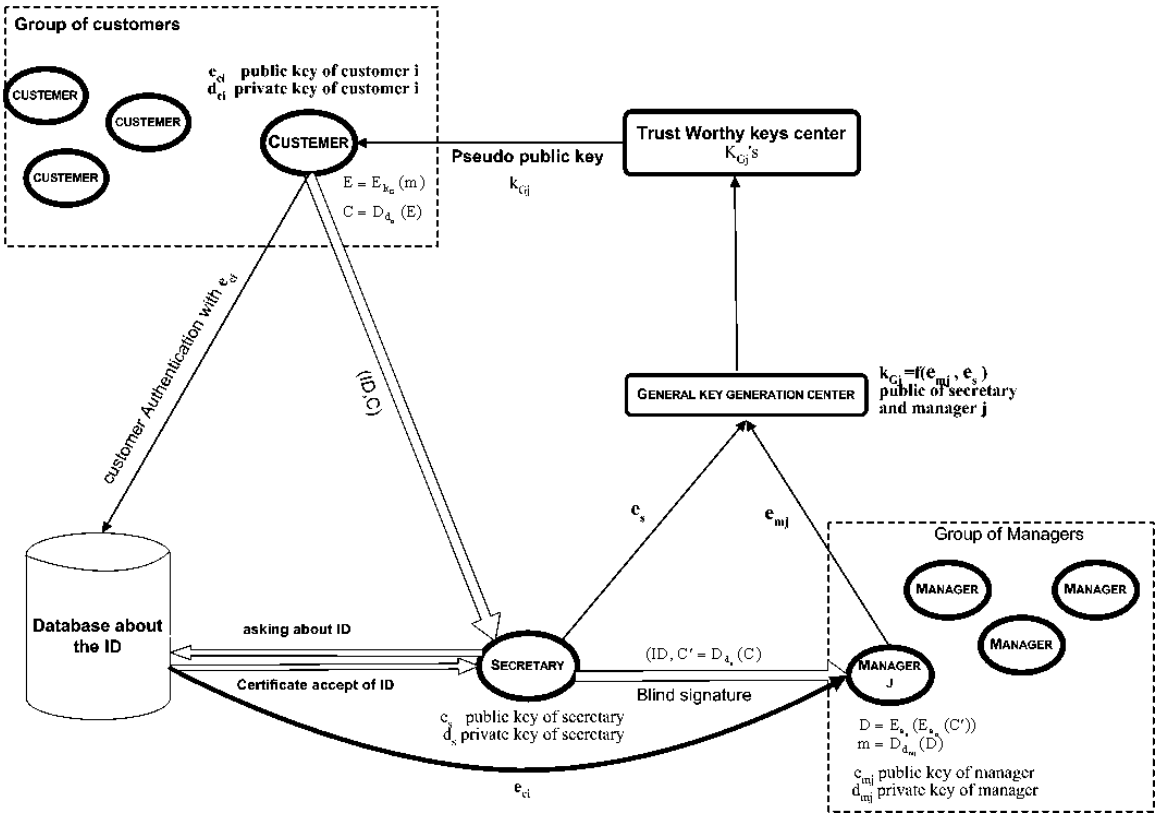

Fig 2. Block diagram of the identity hiding and blind signature.

A forth advantage may also be obtained to check the message integrity. This may be achieved if a message digest is included in the message sent by the customer to the database with access to this database by the manager. Although, this means an addition of extra load to the transmission channel, more reliable communication will be resulted.
This identity hiding and blind signature scheme finds a wide application in many fields, not the least is the following

(1)Banks for depositing money by using the web-site, so that information related to the money and other details will be encrypted under the key K_G which is obtained from a trustworthy data base whose function is providing keys along with account numbers, considered as ID's and passwords used for logging in, when it is necessary for more documentation to the customer.

(2)Commercial companies dealing with permanent dealers and customers having ID's within the sales and purchases services.

(3)Governmental organizations, especially those both with sensitive and confidential information, e.g. those related to national security, military, intelligence and other sensitive organizations.

5. The algorithm

To illustrate the algorithm for the suggested identity hiding scheme, RSA cryptosystem will be used. Two large prime p & q are chosen, then their product N is calculated as N=pq. This product N will be common for the group managers and the secretary, see figure 2.

Let $\phi(N)=(p-1)(q-1)$ and E & D means encryption and decryption algorithms, respectively. For the secretary, the two keys e_S & d_S are selected such that $e_S\ d_S \bmod \phi(N)=1$. Also for each manager j, two keys are selected e_{Mj} & $d_{Mj,}$ such that $e_{Mj}\ d_{Mj} \bmod \phi(N)=1$. Then d keys are kept private and e keys are sent to the key distribution center of the group managers organization. This center calculates new general keys for each manager by $K_{Gj} = e_S\ e_{Mj}$. These keys are sent to a trustworthy key center and made public. They will be used for encrypting messages to be over the communication network. The algorithm proceeds as in the following.

Algorithm

Initialization

{
Send(Mang(j), DC, e_{mj});
Send(Secr, DC, e_s);
DC : $k_G = f(e_{mj}, e_s)$;
}

Customer i

{
Access(Cust(i),TWKC, k_G);
$C = D_{d_{ci}}(E_{k_G}(M))$;
Send(Cust(i), DBC, ID, e_{ci}, customer authentication);
Send(Cust(i), Secr , ID, C);
}

Secretary

{
Access(Secr, DBC, ID, Certif);
DBC : Send(DBC, Secr, Certif);
if (Certif = = false)
{
Send(Secr, Cust(i), Unaccepting);
STOP;
}
else
{
DBC : Send(DBC, Mang(j), eci);
$C` = D_{d_s}(C)$;
Send(Secr, Mang(j), C');
}

Manager j

{
$M = D_{d_{mj}}(E_{e_{ci}}(C'))$;
}}

Notation

Cust(i) : The Customer i.
DC : Distribution Center.
Access(C, S, a, b,…) :Method access the client C to Server S to asking about a, b, …
Secr : The Secretary
Send(S, R, a,b,..) : Method to send a,b,… from the sender S to receiver R.
Mang(j) : The manager j.
DBC :Database about the customers to given Certificate.
TWKC : trust worthy keys center.
S : M : process the method M at Server or client S.

Fig 3. The algorithm for the identity hiding scheme.

At the customer: Any customer who likes to send a message M to manager j of the group. He or she encrypts his or her message with the public key k_{Gj}, relevant to that manager.

$$C = M^{K_{Gj}} \bmod N = M^{e_S e_{Mj}} \bmod N \qquad (11)$$

Then, the customer sends his or her ID together with the encrypted message to the secretary, that validates this ID by consulting the database of the organization in order to accept or reject the message.

At the secretary: If the customer's ID is accepted, then the secretary signs the cipher message by his or her private key d_S as

$$S = C^{d_S} \bmod N = M^{e_S e_{M\,j} d_S} \bmod N$$
$$==> M^{e_{Mj}} \bmod N \qquad (12)$$

This signature S, which is a blind signature is sent to the intended manager.

At the manager: Finally, the manager will use his or her private key d_{Mj} to recover the original message M as

$$S^{d_{Mj}} \bmod N = (M^{e_{Mj}} \bmod N)^{d_{Mj}} \bmod N$$
$$= (M)^{e_{Mj} d_{Mj}} \bmod N ==> M \qquad (13)$$

The whole process is shown in figure 3.

One may summaries the advantages of the customer and manager identities hiding scheme by the following:

(1) The sender will not be able to know the public key (Cryptographer) for the intended receiver (manager).

(2) Each of the receiver and secretary can change their public key individually and this process does not follow any specific rules.

(3) The secretary does not sign any message without knowing its origin, and this gives confidentiality to the receiver (Manager) about the signed message by the secretary.

(4) In this method, the message is both signed and encrypted.

(5) The public keys used by any organization are pseudo keys, and do not reveal any information about the real key.

6. Implementation Example

The suggested algorithm in sections 4 & 5 is practically implemented using RSA technique. The program is written in Java Sun language. The two prime numbers p & q were chosen of 50 digits length each, the public keys for the manager and secretary (e_m & e_s) are of 90 digits length, respectively and public key for the customer (e_c) is of 40 digits length. The private keys d_m, d_c & d_s were calculated. Then a message, M of 200 digits length is encrypted using the general key k_G and sent together with the customer's ID to the secretary as C, it will be signed by the secretary after checking its validity and sent to the manager. The manager, using his or her private key recovers the original message. An example showing the steps for actual keys and message encryption, signing, validation

and message recovery is shown in figure 4. The message block length is taken of the order of 50 digits.

p=22953686867719691230002707821868552601124472329079 **(p and q are of 50 digits each)**
q=307625422503012706920514605395861669272917327549 61

The public key of the manager j, is e_{mj} = 204005728266090048777253207241416669051476369216 501266754813821619984472224780876488344279 (**90 digits)**
and private key,dmj =268923193194521465675527408288861078207056418569768028456339021417853897826305495603551516812225799

The public key of Secretary e_S = 635752334942676003169313626814655695963315290125751655287486460091602385142405742365191277 (**90 digits)**
and the private key d_S = 6 79304729128845707084524237256483902478378090450919845313369915385618453409705785676472587293575 73

The general key kG= emj es mod (ø(N)) = 688387667240002560185075574480900162561967769 355914508026613012428535681491424818116377698967378205533 0

The public key of secretary e_{Ci} = 599283023552414275838685063377325868111 9
and the private key of secretary dCi = 688387667240002560185075574480900162561967769 896737820553303559145080266130124285356814914248181163

The message, M = ***167147222467734852078216952221076085874809964747211172912752992589912196684750549658310084416732550077367495770217142995264827948666809233066409497699870112003149352380375124855230068487109373226251814*** **(200 digit)**
(**The block =50)**

At the Customer: he signs the message using his key d_{Ci}, and encrypts it using k_G.
C= 159110680231558278817649764019245072206635020646518726032763055788994962543179135771672394118550393452788956003246878597850302737371661181219518070759934614636859351055448358204704980720847465262577122008524281372592468223484337468809163837884292427613305066875697825035520510066779244585067058038146577698860071457112418760392989297590566445538243486721425559538132228885462912168335356516908729448707334034071395903403382834434451728413106815088921733129900694473034232171735170551530108264551 1

At the Secretary: he message is signed.
S= 140982419412350238238273315098289697675021142520873308267484574595657765418594085046910709418791772451829776055790559114796677523018419089924693248911264500272027520360901187904366411879523510878077609757102001277169227590446215553873185934379277110428252367285161111424056252002012772756127320134178392075032880200803076190664450613536914231379898710884802074391667497207646521620320675572490085259971557011025027506376082170942493148888138950773547734767779992199896230225414100993554337005689

At the manager: he recovers the original message as
M'= ***167147222467734852078216952221076085874809964747211172912752992589912196684750549658310084416732550077367495770217142995264827948666809233066409497699870112003149352380375124855230068487109373226251814*** ==> M

Fig 4. An example for the implementation or the identity hiding scheme.

7. Conclusions

Mathematical theories behind blind signature prove that it gives more secure systems. While no proof based on true complexity has been found so far, there is considerable evidence that one exists and will be found [20].

Giving access to the public key and/or the sender's identity might help the cryptanalyst to break the system. This paper presented a method for public key hiding, i.e. the public key of the receiver will not be used directly in the encryption process rather a pseudo key will be used. This scheme guarantees reducing the risk of breaking both the encryption algorithm and the public-private key pair. Furthermore, this pseudo public key is generated independent of the sender, i.e. as blind signature is achieved by using another key as well as reduces breaking encryption method.

Blind signature facilitates the sender authenticity and preserve the message privacy. This method is designed and tried on group-users / group-managers environment. It is achieved without the need for the addition random numbers. Also double encryption of the message gives strong security as it travel along the communication network.

Another advantage may also be obtained to check the message integrity. This may be achieved if a message digest is included in the message sent by the customer to the database with access to this database by the manager. Although, this means an addition of extra load to the transmission channel, more reliable communication will be resulted.

References

[1] http://developer.netscape.com/docs.manuals/security/pkin/

[2] Kaeo, M., "Designing Network Security", *Cisco Systems*, 1999.

[3] ANSI X3.106, "American National Standard for Data Encryption Algorithm (AES)", *Americam National Standard Institution*, 1981.

[4] Stalling, W., "Introduction to Cryptography and Network Security", 3rd Ed., *Prentice Hall*, 2003.

[5] "Extracting a 3DES key from an IBM 4758", http://www.cl.cam.ac.uk/~rnc1/descrack/. Last visited on 6 / 7 / 2003.

[6] Lai, X., "On the Design and Security of Block Ciphers", *ETH Series in Information Processing*, Vol. 1, Konstanz: Hartinhg – Gorre Verlag, 1992.

[7] Rivest, R. L., Shamir, A. and Adleman, L. M., "A Method for Obtaining Digital Signatures and Public – Key Cryptosystems", *Communication of ACM*, Vol. 21, No. 2, 1978, PP 120-126.

[8] ElGamal, T., "A Public – Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Trans. On Information* Theory, Vol. IT_31, No. 4, 1985, PP 469-472.

[9] "Proposed Fedral Information Processing Standard for Digital Signature Standard (DSS)", *Fedral Regi*ster, Vol. 56, No. 169, 1991, PP 42980-42982.

[10] Kent, P., "P.G.P Companion for Windows", *Ventana Press*, 1995.

[11] McDysan, D., "VPN Applications Guide", *John Wiley & Sons*, Inc., 2000.

[12] Kosiur, D., "Building and Managing Virtual Privacy Network", *John Wiley & Son*, Inc., 19998.
[13] Diffie, W. and Hellman, M. E., "New Directions in Cryptography", *IEEE Trans. On Information Theory*, Vol. IT-22, No. 6, 1976, PP 644-654.
[14] Chaum, D., "Blind Signatures for Untraceable Systems", *In Advances in Cryptology – Crypto '82*, Springer – Verlag, 1982, PP 199-203.
[15] Marte O. C., "Blind Signatures and Their Applications.
[16] Naccache, and Von Solms, "On Blind Signature and Perfect Crimes", *Computer & Security*, Vol. 11, No. 6, 1992, PP 581-583.
[17] Stadler, M, Piveteau, J. M and Camenisch, L., " Fai Blind Signatures", *Eurocrypt 95*, LNCS 921, Springer – Verlag, 1995, PP 209-219.
[18] Brickell, E. Gemmell, P. and Kravitz, D., "Trustee Based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change", *6th ACM – SIAM Symposium on Discrete Algorithms (SODA)*, 1995, ACM Press, PP457-466.
[19] Radu, C., Govaerts, R. and Vadewalle, J., " Efficient Electronic Cash with resticted Privacy", *Financia Cryptography 97, Springer – Verlag*, 1997, PP 57-69.
[20] Sprague, P., "Blind Signature and Fair Blind Signature", *email: prs@cs.fit.edu*.