A Comparative Study on Various Proxy Signature Scheme

Tinam Sharma[1] DR. Padma Bonde[2]
[1]Scholar [2]Reader
[1]SSTC-SSGI [2]CSVTU

Abstract— A proxy signature scheme is a digital signature scheme which allows an entity, called a original signer, to delegate its signing right to another entity called a proxy signer introduced in 1996 by Mambo et al. It is used in various applications such as mobile agent, e-vote, wireless e-commerce, distributed shared object system etc. From inception several ID based proxy signature schemes and certificate based proxy signature schemes have been discussed.The current paper focuses on a comparative study and analysis of various identity based public key cryptosystem and certificate based public key cryptosystem. This survey is a structured guide to support the current status of both the schemes that is based on their efficiency in terms of communication overhead and security.

Key words: Proxy Signature Schemes

I. INTRODUCTION

Digital signatures are one of the foremost basic concepts of recent cryptography. they provide authentication, integrity and non-repudiation to digital communications, that makes them the most used public key cryptanalytic tool in real applications.A digital signature theme with message recovery could be a signature theme in which the initial message of the signature is not needed to be transmitted along with the signature since it has been appended to the signature and might be recovered according to the verification/message recovery method. It's totally different to an authenticated encryption theme or signcryption theme, since during this theme, the embeded message may be recovered by anyone without the key information. The aim of this type of signatures is to reduce the whole length of the original message and also the appended signature.

A proxy signature protocol permits an entity, known as the designator or original signer, to delegate another entity, known as a proxy signer, to sign messages on its behalf, just in case of say, temporal absence, lack of time or computational power, etc. The delegated proxy signer will compute a proxy signature which will be verified by anyone with access to the initial signer's certified public key. Blaze and Strauss[1] and Dodis and Ivan [2] use the term "proxy signatures," in the context of "proxy cryptography," to explain a distinct primitivewith distinct goals. In a PKI (public key infrastructure)-based cryptosystem, the general public key certificate that is generated and signed by a certificate authority (CA) is needed for authentication of the public keys of the entities, and, as a result, it creates a significant management burden for maintaining and using the public key certificate by developing a worldwide infrastructure.

Initially, of these extensions were introduced for the quality PKI-based framework, wherever every user generates a secret key and publishes the matching public key. In observe, digital certificates linking public keys with identities of users square measure required to implement these systems, and this truth results in some drawbacks in potency and ease. For this reason, the choice framework of identity-based cryptography was introduced by Shamir [3]. the concept is that the general public key of a user are often directly derived from his identity, and so digital certificates square measure avertable. The user obtains his secret key by interacting with some trusty master entity. Shamir already proposed an identity primarily based signature scheme. In contrast, the matter of designing an efficient and secure identity-based encryption theme remained open until [4,5].
Proxy signatures have found various sensible applications, particularly in distributed computing where delegation of rights is quite common. Examples mentioned within the literature include distributed systems [6,7], grid computing [8], mobile agent applications [9, 10], distributed shared object systems [11], international distribution networks [12], and mobile communications [13]. The proxy signature primitive and the initial efficient solution were introduced by Mambo, Usuda and Okamoto [14].

Handwritten signature is a type of identification for an individual a technique is introduced by Md. Itrat Bin Shams [15] where a signature image is first divided (vertical and horizontal) and then information is extracted from individual blocks. Here these data is then compared with the test signature. Signatures are composed of special characters andflourishes and therefore most of the time they will be unclear. Baseline is the imaginary or invisible line, which a signature is assumed to rest on. A baseline is the line on which the letter sits. In our daily life, a baseline must be notional once signing or writing in an unlined sheet of paper. The straightness and direction of the signature can be changeable features during a signature [16].

Fig. 1: Distance Calculation

For verification of signature image after extraction of features from written signature pictures several authors use completely different mathematical formulas. Such as correlation is employed for verification between sample and test signature. Extracted features are used for cluster the signature pictures for verification stage.Features can have to be extract from each sample pictures and check image. Extraction procedures for signature image verification is as follows:

- Signature Height Width Ratio
- Signature Occupancy Ratio
- Distance Ratio Calculation at Boundary
- Compute the length and ratio of adjacency Columns
- Compute the number of Spatial symbols within the signature Image

II. METHODOLOGY

A. A Provably Secure ID-SDVPS Scheme from Bilinear Pairings

This method relies on Identity based strong designated verifier proxy server.In this scheme it is assumed that Alice is the original signer and has the identity IDA, Bob is the proxy signer and has the identity IDB and Cindy is the designated verifier and has the identity IDC. We denote them as IDi, where i 2 ϵ{A, B, C}, and we consider (Qi, Si) to be their public/private key pair. The concepts of the schemes (Huang et al., 2008; Sun et al., 2010; Yoon, 2011) are combined to construct a brand new ID-SDVPS scheme that has robust security within the random oracle model and fewer computational price which is described as follows:

– Step 1: Setup

It takes a security parameter k ϵ Z+ as input and outputs the system's parameter Ω and a pair of master private/ public key (msk, mpk).

– Step 2: Extract

It takes a security parameter k, a system parameter Ωand the master private key msk as input, and it outputs the valid private/public key pair (Si, Ω i) for an entity ID_i.

– Step3: DGen

On input of the system's parameter Ω, the original signer's private key S_i and a warrant m_w, the DGen algorithm outputs a valid delegation W for the proxy signer ID_j.

– Step 4: DVerify

It takes the original signer's public key Q_i and a delegation W as input and outputs accept if W is valid; otherwise, it outputs reject.

– Step 5: PKGen

Given the proxy signer's private key S_j and a delegation W, it outputs a valid proxy private/public key pair (S_P, Q_P).

– Step6: PSGen

It takes the proxy private key S_P, the delegation W, the designated verifier's public key Q_k and a signed message m ϵ {0,1}* as input and generates a proxy signature r for the designated verifier ID_k.

– Step7: PSVerify

This algorithm accepts a message m ϵ {0,1}*, a warrant W, a signature r, the public key pair (Q_i, Q_j) of the original signer and the proxy signer, the designated verifier's private key S_k and returns accept if the signature σ is valid; otherwise, it returns reject.

– Step7: Transcript simulation

This algorithm takes a message m ϵ {0,1}*, a warrant W and the designated verifier's private key S_k to generate a simulated proxy signature r 0, which is identical to the original designated verifier proxy signature r that was generated by the proxy signer.

Several ID-SDVPS schemes based on elliptic curve bilinear pairing have been proposed in recent years; however, they are neither secure against different attacks nor computationally efficient.an efficient ID-SDVPS scheme, which is demonstrated to be provably secure with the hardness assumption of CDH and GBDH problems in the random oracle model against an adaptive chosen message and identity attacks under the different types of adversaries. Additionally, the formal validation of the proposed ID-SDVPS scheme is performed by using an automated validation tool called AVISPA, and the simulation results show that the scheme is unforgeable against active and passive adversaries.

B. Id-Based Ring Signature Scheme (IDBRS)

The concept of ring signature was introduced by Rivest, Shamir and Tauman in [17]. The ring signature allows a user from a set of possible signers to convince the verifier that the author of the signature belongs to the set but identity of the author is not disclosed. The ring signature may be considered to be a simplified group signature which consists of only users without the managers. It protects the anonymity of a signer since the verifier knows only that the signature comes from a member of a ring, but doesn't know exactly who the signer is.

– Step 1: Setup

Let P is a generator of G1; e : G1 × G1 −! G2 is a bilinear pairing. H1 : {0, 1}*→z*q , H2 : {0, 1}*→ G1 and H3 : G2→z*qare cryptographic hash functions. Key Generation Center (KGC) chooses a random number s ϵ Z*q and sets PPub = sP. The KGC publishes the system parameters{G1,G2, e, q, P, PPub,H1,H2,H3} and keeps s as the master key.

– Step 2: Extract

An user submits its identity information IDk to KGC. KGC publishes the public key Qk =H2(IDk) and returns Sk = sQk to the user as his/her private key.

Step 3:Ring Signature Generation

Given a message m to be signed, signer's secret key Sk, and the possible signers' public keys sequence L = (ID1, ID2, · · · , IDr) of all ring members, the signer computes the ring signature as follows.

1) Choose a key: K = H1(m||L).
2) Pick a random glue value: The signer picks a random A ϵ G1 and computes the initialization value: v = ck = e(A, P)k
3) Pick random Ti's: The signer picks a random Ti for all other ring members uniformly and in-dependently from G1, and computes: ci+1 = [e(PPub,H3(ci)Qi).e(Ti, P)]K.
4) Formation of ring: The signer solves the ring equation for yk. When i = k, we get ck+1 = [e(PPub,H3(ck)Qk).e(Tk, P)]K = v. On solving this ring equation we get Tk = A − H3(ck)Sk. Now compute T = Σ Ti.
5) Output the ring signature: The ring signature onmessage m is the tuple (L; c1, c2, · · · , cr; T).

– Step 4: Ring Signature Verification

On receiving the ring signature (L; c1, c2, · · · , cr; T) on message m, the verifier can verify as follows. The verifier computes K = H1(m||L) and checks if $\pi_i c_i$ = [e(P_{Pub},Σ_i(H3(ci)Qi)).e(T, P)]K.

If the equation is satisfied, the verifier accepts the signature as valid otherwise reject

C. Efficient ID-based Proxy Signature Scheme from pairings

A new efficient ID-based proxy signature theme relies on a variation of the ID-based signature theme planned by Barreto et.al [18] in Asiacrypt'05. the strategy for getting

non-public keys from identities may be a simpli¯cation of a technique recommended by Sakai and Kasahara [19].

– Step1: Setup

Takes as input a security parameter *k*, and returns a master keys and system parameters - = (G1;G2; q; ê; P; Ps; Pss; g; gs;H1;H2), where (G1; +) and (G2; ¢) are two cyclic groups of order q, ê: G1 x G1 → G2 is an admissible bilinear map, Ps = sP, Pss = s^2P, g = ê (P; P), gs = ê (Ps; P),
H1 : {0, 1}*→Z^*_q and H2 : {0, 1}*xG1 → Z_q are hash functions.

– Step 2:Extract

Takes as input an identity ID_X ϵ {0, 1}*, computers DX = (H1(IDX) + s)¡1P, and lets DX be the user's secret key.

– Step 3:Delegate

Takes as input the secret key DA, the proxy signer's identity IDB and a warrant m_w, selects a random x ϵ Z*q , computes qB = H1(ID_B), rA = g_s^x .$g^{qBx,}$ hA = H2(m_w,r_A), VA = (x + h_A)D_A, and outputs the delegation $W_{A\to B}$ = (m_w,r_A,V_A).

– step4:DVerify

Once B receives $W_{A\to B}$ = (m_w,r_A,V_A), he computes hA = H2(m_w,rA), qA = H1(IDA), qB = H1(IDB), and accepts the delegation only if
ê ((qA + qB)Ps + qAqBP + Pss; VA) = rA g_s^{hA} . g^{qBhA}

– Step 5: PKgen

If B accepts the delegation WA!B = (m_w,r_A,V_A), he computes the proxy signing key DP as DP = hA .DB -VA, where hA = H2(m_w,r_A).

– Step 6:PSign

The proxy signer can pre-computingξ= ghA(qA¡qB)=rA, where qA = H1(IDA), qB = H1(IDB) and rA is from WA!B. Let DP be the proxy signing key, for a message m, the proxy signer chooses y ϵ Z*q at random and computes rP = ξy, hP = H2(m,rP), VP = (y+hP)DP , and lets (m,T) = (m,rP, VP,mw, rA) be the proxy signature for m.

– Step 7: PVerify

For a proxy signature (m,rP , VP ,mw, rA), a recipient first checks if the proxy signer and the message confirm to mw.Then we compute hP = H2(m, rP), qA = H1(IDA), qB = H1(IDB) and verifies whether
ê((qA + qB)Ps + qAqBP + Pss,VP) = rP $^{ghAhP\,(qA-qB)}$ r_A^{-hP}
If both steps succeed, the proxy signature on behalf of A is valid.

– Step 8:ID

The proxy signer's identity IDB can be revealed by mw.

D. Short and Efficient Certificate-Based Signature

A short and efficient certificate-based signature (CBS) scheme projected by gentry [20] combines the benefit of traditional public key cryptography (PKI) and identity primarily based cryptography, without use of the expensive certificate chain verification method and therefore the removal of key escrow security concern. we tend to need one group component for the signature size and public key respectively. therefore the public info for every user is reduced to simply one cluster part. it's even shorter than the progressive PKI primarily based signature theme, which needs one cluster part for the general public key whereas another cluster part for the certicate.Algorithm is as follows:

– Step 1:Setup.

Select a pairing e : G x G →GT where the order of G is p. Let g be a generator of G. Let H1 : {0,1}*→ G and H2 : {0,1}*→ Zp be two collision resistant cryptographic hash functions. Randomly select α ϵ R Zp and compute g1 = g^{α}. The public parameters param are (e,G,GT, p, g, g1) and the master secret key msk is α.

– Step 2: User Key Generation

User selects a secret value x ϵ Zp as his secret key usk, and computes his public key PK
as Y = g^x

– Step 3: Certify

To construct the certificate for user with public key PK and binary string ID, the CA computes
C = H1(ID; PK) $^{\alpha}$.

– Step 4: Signature

To sign a message m ϵ {0,1}*, the signer with public key PK (and user information ID) , certificate C and secret key x, compute σ= 1\$C^{x+H2(m,ID,PK)}$

– Step 5: Verify

Given a signature σ for a public key PK and user information ID on a message m, a verifier checks whether
e(σ,Y,$g^{H2(m;ID;PK)}$)= e(H1(ID, PK),g1).

III. CONCLUSION

This paper presents the work done by different researchers associated with proxy signature scheme. Specifically the area under review in proxy signature is ID based proxy signature and message encrypted proxy signature.This paper presents a quick review of proxy signature scheme which includes feature extraction,key generation,encryption etc. Experimental results demonstrated in this survey paper that an ID based proxy Signature scheme can over come the disadvantages of other proxy signature scheme.

REFERENCES

[1] M. Blaze and M. Strauss. Atomic proxy crpytography. In Eurocrypt, LNCS, 1998.
[2] Ivan and Y. Dodis. Proxy Cryptography Revisited. NDSS 2003, 2003.
[3] Shamir. Identity-based cryptosystems and signature schemes. *CRYPTO'84*,volume 196 of *LNCS*, pages 47–53, 1985.
[4] D. Boneh and M.K. Franklin. Identity based encryption from the Weil pairing.*SIAM Journal on Computing*, 32(3):586–615, 2003.
[5] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing over elliptic curve (in Japanese). *SCIS 2001*, Jan 2001.
[6] C. Neuman. Proxy based authorization and accounting for distributed systems. In Proceedings of the 13th International Conference on Distributed Computing Systems, pages 283–291, 1993.
[7] Varadharajan, P. Allen, and S. Black. An analysis of the proxy problem in distributed systems. In Proceedings of 1991 IEEE Computer Society Symposium on Research in Security and Privacy, pages 255–275, 1991.
[8] Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A security architecture for computational grids. In CCS, 1998.
[9] H. Kim, J. Baek, B. Lee, and K. Kim. Secret computation with secrets for mobile agent using one-time proxy signature. In Cryptography and Information Security 2001, 2001.

[10] B. Lee, H. Kim, and K. Kim. Strong proxy signature and its applications. In SCIS, 2001.
[11] J. Leiwo, C. Hanle, P. Homburg, and A. S. Tanenbaum. Disallowing unauthorized state changes of distributed shared objects. In SEC, pages 381–390, 2000.
[12] Bakker, M. Steen, and A. S. Tanenbaum. A law-abiding peer-to-peer network for free-software distribution. In IEEE International Symposium on Network Computing and Applications (NCA'01), 2001.
[13] H.-U. Park and L.-Y. Lee. A digital nominative proxy signature scheme for mobile communications. In ICICS 2001,volume 2229 of LNCS, 2001.
[14] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures for delegating signing operation. In CCS). ACM, 1996.
[15] Md. Itrat Bin Shams, "Signature Recognition by Segmentation and Regular Line Detection" TENCON 2007 - 2007 IEEE Region 10 Conference Volume , Issue , Page(s):1 – 4, Oct. 30, 2007- Nov. 2, 2007.
[16] Azlinah Mohamed, Rohayu Yusof, Shuzlina Abdul Rahman, Sofianita Mutalib, "Baseline Extraction Algorithm for Online Signature Recognition", WSEAS TRANSACTIONS on SYSTEMS, Issue 4, Volume 8,ISSN: 1109-2777, April 2009
[17] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Advances in Cryptology, Asiacrypt 2001, LNCS 2248, pp. 552-565, Springer-Verlag, 2001.
[18] P. S. L. M. Barreto, B. Libert, N. McCullagh, J. Quisquater, E±cient and Provably- Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In B. Roy, editor(s), Asiacrypt 2005, LNCS 3788, pages 515-532, Springer-Verlag, 2005.
[19] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054.
[20] C. Gentry. Certi_cate-based encryption and the certi_cate revocation problem. In EUROCRYPT '03,pages 272{293. Springer-Verlag, 2003. LNCS No. 2656.

