Performance Comparison of Efficient Identity Based Signature Schemes

S.Kuzhalvaimozhi, Dr.G.Raghavendra Rao

Abstract—

In a conventional public key crypto system, the participants must verify the certificate prior to use the public key. The main drawback of the certificate in conventional public key system are large storage, large computing time to store and verify each user's public key and the corresponding certificate. Identity based cryptography is the new system which reduces the key management process in conventional public key infrastructures (PKI). Any public information such as the e-mail address, name, etc., can be used as a public key. This resolves the problem of getting the public key of a user and checking the validity of certificate. This paper provides a general idea of the Digital signature based on Identity based cryptography. The various efficient Identity Based Signature schemes are analyzed based various criteria like number of operations required for generation and verifying signature, size of the signature and number of paring operations.

***Index Terms*— Digital Signature, Identity based cryptosystem, Identity based signature, Public key infrastructure, Pairing.**

I. INTRODUCTION

In the traditional Public key infrastructure (PKI), certificates are used to offer a guarantee of the relationship between public keys and the identities that hold the corresponding private keys. This assurance on a public key is delivered in the form of certificate which is granted with a signature by a Certification Authority (CA).

A sender is not able to encrypt a message for a recipient unless the recipient has previously obtained a certificate and has made the certificate available to the sender. The recent development in the cryptography is the Identity Based Cryptography (IBC)[2,8]. The IBC does not need any certificate, as public keys are calculated from public identifiers. Thus the binding between an identity and a public key is direct in IBC, rather than being enabled by a certificate as in conventional public key cryptography. The public key of the signer is actually a type of random string.

The size of an identifier may be smaller compared to the size of a certificate. This provides a considerable advantage in terms of communication cost savings, mostly in applications where multiple certificates require to be transmitted between two nodes.

In 1984 Shamir[1] proposed ID-based encryption and signature schemes to simplify key management procedures in conventional certificate based public key crypto system. Since then, many ID-based encryption and signature schemes have been proposed. The main idea of Identity based cryptosystems is that the identity information of each user works as his/her public key.

The user's public key can be calculated directly from his/her identity (e-mail address, name) rather than being extracted from a certificate issued by a CA[7]. Identity based public key setting can be a good alternative for certificate-based public key setting, particularly when efficient key management and moderate security are required.

The most significant and popular security method in modern cryptography is the Digital Signature. Mainly in online applications, digital signature is the most widely used public key cryptographic method to provide integrity, authentication, and non repudiation. The digital signature scheme based on IBE is the identity-based signature scheme (IBS)[3]. In IBS, the signer Alice first obtains a signing (private) key associated with her identifier information from the Private Key Generator (PKG). She then signs a message using the signing key. The verifier Bob now uses Alice's identifier information to verify Bob's signature. – No needs for Bob to get Alice's certificate. Figure 1 illustrates a schematic outline of an IBS scheme.

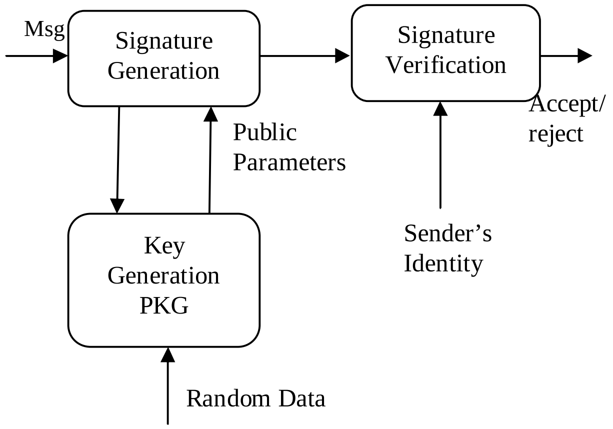

Fig 1: Identity Based Signature

S.Kuzhalvaimozhi, Department of Information Science and Engineering, National Institute of Engineering, Mysore, Karnataka, India.

Dr.G.Raghavendra Rao, Department of Computer Science and Engineering, National Institute of Engineering, Mysore, Karnataka, India.

II. Related Work

In 1984, Adi Shamir[1] introduced the concept of Identity based cryptography. First proposed scheme for identity-based public key cryptography deals with the drawbacks of authenticity of keys in a different way to traditional PKI. In the identity- based signature a trusted third party called the PKG (Private Key Generator) manages the generation and distribution of the users' private keys. This feature significantly reduces the complexity of a cryptography system by removing the need for generating and managing user certificates.

At the time Shamir published his proposal, which he had already determined a way of using the existing RSA function for identity based signature (IBS) scheme but had yet to solve the problem of identity based encryption (IBE). Most of the schemes proposed since 1984 were unsatisfactory because they were too computational intensive and they required tamper resistant hardware or they were not secure if users colluded.

Three IBE solutions were proposed in 2001 by Boneh and Franklin[2] as well as by Cocks and Sakai-Kasahara [4]respectively. The Boneh-Franklin scheme has received much attention owing to the fact that it was the first IBE scheme to have a proof of security in an appropriate model. Boneh and Franklin used the bilinear pairing to realize IBE scheme, many IBE and IBS schemes based on the bilinear pairing have been constructed recently. Al-Riyami and Paterson[5] introduced and made concrete the concept of Certificateless public key cryptography.

After Boneh and Franklin's work, many schemes built from the same computational and architectural primitives, showed how identity-based signature schemes could be. These schemes were all predated by the signature scheme of Hess. All the schemes are similar in terms of operation and implementation, and the schemes of [9,10,11] actually have better security guarantees.

III. Bilinear Pairing

Pairings are bilinear mappings defined over groups wherein the discrete logarithm problem is hard. They are usually instantiated with carefully chosen elliptic curves. For the last couple of years, they have been found to provide plenty of applications in the design of cryptographic protocols. The most salient examples were probably the appearance of tripartite key agreement protocols, identity-based encryption schemes, where any arbitrary public identifier can be used as a public key, and digital signature schemes producing short signatures.

Bilinear pairing is an important primitive for many cryptographic schemes[6,12,13]. Many elegant cryptographic schemes have been formulated utilizing the properties of these bilinear pairings.

- G1 be an additive group of prime order q, generated by p,
- G2 be a multiplicative group with the same order q.

We assume that there is a bilinear map e from G1×G1→ G2 with the following characteristics:

A. Bilinearity: Which means that given elements

A1,A2,A3 є G1 , we have that

e(A1 + A2, A3) = e(A1,A3) × e(A2,A3) and

e(A1, A2 + A3) = e(A1, A2) × e(A1, A3).

In particular, for e(aA1, bA2) = e(A1, A2)ab, a,b ε Z*q where Zp denotes all positive integer which is less than p. Z*q denotes multiplicative group modulo p.

B. Non-degeneracy: Which means that there exists A1, A2 ε G1 such that e(A1, A2) $\neq$ 1G2 , where 1G2 is the identity of G2.

C. Computability: Which means that there exists an efficient algorithm to compute e(A1, A2) A1, A2 ε G1.

The following are some of the properties of pairing:

1) $e(P,0) = e(0,Q) = 1$

2) $e(-P,Q) = e(P,Q)^{-1} = e(P,-Q)$

3) $e([a]P,Q) = e(P,Q)^{a} = e(P,[a]Q)$ for all $a \in \mathbf{Z}$

4) $e([a]P,[b]Q) = e(P,Q)^{ab}$ for all $a,b \in \mathbf{Z}$

Decision Diffie-Hellman is easy: The Decision Diffie-Hellman problem (DDH). Given aP, bP, cP ε G1. If we want to decide whether cP = abP, we can easily determine by checking e(P, cP) = e(aP, bP).

Computational Diffie-Hellman is hard: The Computational Diffie-Hellman problem (CDH). Given P, aP, bP ε G1, if we want to compute abP ε G1, it is assume to be hard.

Since the Decision Diffie-Hellman problem (DDH) in G1 is easy, we cannot use DDH to build our cryptosystems. Instead, the security of our IBE system is based on a variant of the Computational Diffie-Hellman assumption (CDH).

IV. Model of Identity Based Signatures

In Identity Based Signature Scheme (IBS), the sender obtains a private key associated with the unique identity information from the PKG. Then the sender signs a message using the signing key. The verifier uses the sender's identity information to verify the signature. For the verifier it is not required to get the sender's certificate to verify the key.

Identity Based Signatures scheme includes four algorithms:

- *Setup*
- *Extract*
- *Sign*
- *Verify.*

They are used to generate the system parameters, extract the secret key associated the user's identity, sign the message by the secret key and verify the signatures under the public key and the user's identity. In the random oracle model, we say an IBS scheme is existential un forgeable under an adaptive chosen message and identity attack if no polynomial time algorithm has non-negligible probability against a challenger.

1. Setup: The Private Key Generator (PKG), which is a trusted third party, creates its master private and public key pair. The PKG chooses the global secret key, computes the global public key and publishes it with other system parameters.
2. Private Key Extraction: The sender authenticates to the PKG and obtains a private key associated with the identity. PKG verifies the user's identity and computes user's public and private key of the user. The private key should be sent to the user over a secure channel after this phase.
3. Signature Generation: Using the private key and other public parameters, the sender creates a signature on the message M.
4. Signature Verification: Having obtained the signature and the message M from sender, the verifier checks whether the signature is a genuine signature on M using sender's identity and the PKG's public key. If it is, then the receiver accepts the message or otherwise rejects it.

V. Identity Based Signature Schemes

We introduce the major identity based signature schemes based on the integer factorization and bilinear pairing.

A. *Shamir's Identity Based Signature*

Shamir proposed the identity based signature scheme in 1984 based on the integer factorization mechanism. The security of this scheme is based on the computational hardness of the integer factorization problem, i.e given a large positive integer, finding its prime factorization is computationally infeasible.

1) Signing Algorithm:

   Message m
   Private key SID
   Master Public Key (e,n)

   - r ЄR Zn*
   - t=re mod n
   - f= H(t,m)
   - s= SID rf mod n
   - σ=(s,t)

2) Verification Algorithm:

   Using m, ID , Public parameter(e,n) receiver will verify Se=ID . t H(t,m) mod n
   If equal he will accept message or reject it.

B. *Hess's Identity Based Signature*

Hess proposed the identity based signature scheme in 2003. The security of this scheme was proved under CDHP assumption in the random oracle model.
Signing:

- Setup
  - master public key: P
  - master private key: s
  - computes s P
  - PKG generates signer's private key:
    - sQ where Q = H1(ID)
- hash functions: H1 and H2
- sign on m:
- Signature is (h, S)
  - k ЄR Zq*
  - T = ê(sQ, P)k
  - h = H2(m, T)
  - S = (k - h)sQ

verify (h, S):

- T = ê(S, P)ê(Q, sP)h
- h =?= H2(m, T).

C. *Cha-Cheon's Identity Based Signature*

This scheme [9] is completely secure against existential forgery under adaptively chosen message and ID attack in the random oracle model assuming the hardness of CDHP. Signing phase of this scheme is very efficient as it does not require pairing operation as described in [11].

Signing Algorithm:

- key construction
  - master public key: P
  - master private key: s
  - Computes sP
  - signer's private key: sQ where Q = H1(ID)
- hash functions: H1 and H2
- sign on m: Signature is (T, S)
  - r ЄR Zq*
  - T = rQ
  - h = H2(m, T)
  - S = (r + h)sQ

Verify (T, S):

- h = H2(m, T)
- ê(P, S) =?= ê(sP, T + hQ)

D. *Barreto's Identity Based Signature*

This scheme[15] can benefits from the most efficient pairing calculation technique for a larger variety of elliptic curves than previous schemes as described. This identity based signature is faster and significantly more efficient at verification because its verification algorithm requires a single pairing calculation.

Signing Algorithm

- key construction
  - master public key: P, Q, sQ, g = ê(P, Q)
  - master private key: s
  - signer's private key: SID = 1/(H1(ID) +s)P
- hash functions: H1 and H2
- sign on m: Signature is (h, S)
  - x ЄR Zq*
  - r = gx

−h = H2(m, r)

−S = (x + h) SID

verify (h, S):

- h =?= H2(m, ê(S, H1(ID)Q + sQ)g-h) = H2(m, r)

E. Sakai-Ogishi-Kasahara IdentityBased Signature

The Sakai-Ogishi-Kasahara IBS (called SOK-IBS here) that was already proven secure and has a much tighter security proof under the Diffie-Hellman assumption.

Setup

- security parameter k
- PKG chooses groups G1 and G2 of prime order q > 2 k , a generator P of G1,
- master secret key s ∈ Zq ∗
- master public key Ppub = sP.
- H1, H2 : {0, 1} ∗ → G1∗.
- params = G1, G2, e, P, P ˆ pub, H1, H2

Key Generation

- user's identity ID
- PKG computes QID = H1(ID) ∈ G1
- private key of the signer dID = sQID ∈ G1

Sign

- message M
- choose r ЄR Zq
- compute
  - oU = rP ∈ G1
  - oH = H2(ID, M, U) ∈ G1.
  - oV = dID + rH ∈ G1.
- The signature on M is the pair

  σ = <U, V > ∈ G1 × G1.

Verify:

verify a signature σ on a message M for an identity ID,

- verifier uses QID = H1(ID) ∈ G1 and H = H2(ID, M, U) ∈ G1.

accepts the signature if ˆe(P, V) = ˆe(Ppub, QID)ˆe(U, H) and rejects it otherwise.

VI. Performance Comparison of IBS Schemes on Computational Cost

We have used the notations as shown in Table 1 to evaluate the computational cost of Eight identity based signature schemes and the result have been shown in Table 2

Table 1: Notations

P: the pairing operation
M: the multiplication in G
E: the exponentiation in G
H :hash operation in Zn

Table 2: IBS Comparison

Methods	Sign	Verify	Signature size	Pairing
Shamir	2E+1M+1H	2E+1M+1H	640	3
Hess	1P+1E+1A + 2M+1H	2P+1H+1E	320	3
Cha-Cheon	2H+2M+1A	2P+1H+ 1M+1A	320	2
Barreto	2E	>23E	512	1
SOK	2M+1A	3P+1H	1196	1
Zhang & yang	4M+1H+1I	3P+1H	4|G1|	1
Boneh	1EC+1H	2P+1EC+ 1H	2900	2
Paterson	3M+2A+2H	3P+2E+ 1M+2H	1196	1

VII. Conclusion

The above conducted study shows that different digital signature with different key sizes have different performance characteristics are analyzed. The aim of this paper was to answer the question of whether it is feasible to implement digital signature in various applications. Based on the analysis a user can select the method using different criteria less operation, smaller key size or less time taken. Research has resulted in the development of efficient ECC implementations and stronger, faster security protocols. Smaller key size, high performance, lower computational cost, and a relatively fast signature generation are the reasons why we choose ECC as a reliable e-commerce application solution.

References

[1] A. Shamir. Identity-based Cryptosystems and Signature Schemes,*Advances in Cryptology - CRYPTO '84*, LNCS 196, pp. 47-53, 1985.

[2] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing, *Advances in Cryptology - CRYPTO '2001*, LNCS 2139, pp.213-229, 2001.

[3] F. Hess. Efficient Identity based Signature Schemes based on Pairings. *Selected Areas in Cryptography –SAC 2002*, LNCS 2595, pp. 310-324, 2003.

[4] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems Based on Pairings, *The 2000 Symposium on Cryptography and Information Security*, pp. 26-28, 2000.

[5] C. Boyd, W. Mao, and K.G. Paterson. Key Agreemet Using Statically Keyed Authenticators, *Applied Cryptography and Network Security, ACNS 2004*, LNCS 3089, pp. 248-262, 2004.

[6] L. Chen and C. Kudla. Identity Based Authenticated Key Agreement Protocols from Pairings. *Hewlett-Packard Technical Report HPL-2003-25 20030212*, HP Laboratories, 2003.

[7] K. Hoeper and G. Gong. Limitations of Key Escrow in Identity- Based Schemes in Ad Hoc Networks. *Security and Privacy for Emerging Areas in Communication Networks –SecureComm 2005*, submitted for publication.

[8] M. Girault. Self-Certified Public Keys, *Advances in Cryptology-EUROCRYPT '91*, LNCS 547, pp. 490-497, 1991.

[9] J.C. Cha and J.H. Cheon. An identity-based signature from gap Diffie-Hellman groups. Cryptology ePrint Archive, Report 2002/018, 2002. http://eprint.iacr.org/.

[10] F. Hess. Exponent group signature schemes and efficient identity based signature schemes based on pairings. Cryptology ePrint Archive, Report 2002/012, 2002. http://eprint.iacr.org/.

[11] K.G. Paterson. ID-based signatures from pairings on elliptic curves. Electronics Letters,38(18):1025–1026, 2002.

[12] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In The 2000 Sympoium on Cryptography and Information Security, Okinawa, Japan, January 2000.

[13] Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryp-tology - CRYPTO '84, volume 196 of Lecture Notes in Computer Science, pages 47–53. Springer-Verlag, 1984.

[14] Zhang and K. Kim, ID-based Blind Signature and Ring Signature from Pairings, Advances inCryptology – Proceddings of ASIACRYPT 2002,LNCS 2501, pages 533–547, Springer-Verlag, 2002

[15] P. Barreto, H. Kim, B. Lynn, and M. Scott, Efficient Algorithms for Pairing-Based Crypto systems , Advances in Cryptology - Proceedings of CRYPTO 2002, LNCS 2442, pages 354–369, Springer-Verlag, 2002.