5-2008

Some Implementation Issues for Security Services based on IBE

Göran Pulkkis
Arcada University of Applied Sciences, goran.pulkkis@arcada.fi

Kaj Grahn
Arcada University of Applied Sciences, kaj.grahn@arcada.fi

Jonny Karlsson
Arcada University of Applied Sciences, jonny.karlsson@arcada.fi

70F. Some Implementation Issues for Security Services based on IBE

Göran Pulkkis
Arcada University of Applied Sciences
goran.pulkkis@arcada.fi

Kaj Grahn
Arcada University of Applied Sciences
kaj.grahn@arcada.fi

Jonny Karlsson
Arcada University of Applied Sciences
jonny.karlsson@arcada.fi

Abstract

Identity Based Encryption (IBE) is a public key cryptosystem where a unique identity string, such as an e-mail address, can be used as a public key. IBE is simpler than the traditional PKI since certificates are not needed. An IBE scheme is usually based on pairing of discrete points on elliptic curves. An IBE scheme can also be based on quadratic residuosity. This paper presents an overview of these IBE schemes and surveys present IBE based security services. Private key management is described in detail with protocols to authenticate users of Private Key Generation Authorities (PKG), to protect submission of generated private keys, and to avoid the key escrow problem. In the security service survey IBE implementations for smartcards, for smart phones, for security services in mobile networking, for security services in health care information systems, for secure web services, and for grid network security are presented. Also the performance of IBE schemes is estimated.

Keywords

IBE, identity based encryption, pairing, key escrow, threshold cryptography, PKI, and security service

1. Introduction

The traditional Public Key Infrastructure (PKI) provides strong security but has turned out to be difficult to use for an average user. Furthermore, PKI causes, especially in mobile devices, a high load on the computational power and the bandwidth. Identity Based Encryption (IBE) is a public key cryptosystem where an arbitrary identity string is a valid public key. Public key certificates and certificate revocation lists (CRLs) are therefore not needed. Computationally costly certificate and CRL management is avoided.

IBE concept was first introduced in (Shamir, 1984). The first practical IBE scheme proposed in (Boneh & Franklin 2001) was followed by vast research on IBE. A security flaw in the Boneh & Franklin scheme has been removed (Galindo, 2005), several variants of these schemes have been proposed (Boneh & Boyen 2004; Gentry, 2006; Al-Riyami & Paterson 2003; Sahai & Waters, 2007), IBE signature schemes have been proposed (Cha & Cheon, 2002; IBE, 2007), a different practical IBE scheme has been proposed (Cocks, 2001), IETF standardization of IBE has started

(Appenzeller et al. 2007), and IBE based security services have been integrated in commercial security products (Voltage, 2007; NoreTech, 2004; Gemplus, 2005).

Authentication, protected data communication, stored data protection, and non-repudiation signatures are examples of security services, which can be implemented with IBE. Requirements for authentication services are IBE based signing, signature verification, encryption and decryption. Requirements for protected data communication and stored data protection are IBE based encryption and decryption. Requirements for non-repudiation signatures are generation and distribution of private user keys without key escrow, IBE based signing, and IBE based signature verification.

2. IBE Requirements for Security Services

An IBE scheme consists of four algorithms (Boneh & Franklin 2003):

- **Setup** – A master private key and public IBE parameters are generated by a Private Key Generation Authority (PKG)
- **Extract** – The private user key associated with an arbitrary public key string is generated with the master private key
- **Encrypt** with the public user key
- **Decrypt** with the associated private user key.

An IBE scheme can be based on an operation called pairing defined for a pair of discrete elliptic curve points or on quadratic residuosity. Elliptic Curve Public Key Cryptosystems are described in detail for example in (Menezes, 1994).

Software and/or hardware for IBE and a PKG are required for security service implementations. Two open source software libraries for pairing implementations are presently available (Identity, 2007; PBC, 2007). Software implementations of quadratic residuosity are supported by number theoretic functions in the GMP library (GMP, 2007).

Secure private user key generation and distribution requires

- authentication of legitimate PKG users
- protected data communication between the PKG and authenticated users.

Three methods have hitherto been used to preserve some benefit of IBE cryptosystems without introducing full key escrow by default:

- Threshold techniques to distribute the secret master key
- Embedment of a user generated component in a private key issued by a PKG
- Use of an Accountable Authority Identity based Encryption (A-IBE) scheme for which the existence of multiple private keys for the same identity string can be proved and detected.

2.1 Pairing

Let G_1 and G_2 be two groups of prime order q. We assume that G_1 is an additive group, G_2 is a multiplicative group and the discrete logarithm problem is hard in both groups. A bilinear mapping (pairing) e: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

- Bilinearity. For all $P,Q \in G_1$ and $R,S \in G_2$, $e(P+Q,R)=e(P,R)\cdot e(Q,R)$ and $e(P,R+S)=e(P,R)\cdot e(P,S)$
- Non-degeneracy. For all generators $P \in G_1$, e(P,P) is a generator of G_2.

Four pairing types have hitherto been defined: Weil, Tate, Eta or ηT, and ATE pairing (Boneh & Franklin 2001; Gailbraith et al. 2002; Hess et al., 2006)

2.2 Quadratic Residuosity

The Jacobi symbol (b/N) for two integers b and N is defined by (b/N)=0 if N divides b, (b/N)=1 if b is a square mod N, and (b/N)=-1 otherwise. For a given b and N odd such that (b/N)= 1, then the Quadratic Residuosity problem is to find an x for which $b = x^2 \bmod N$. This problem can be solved efficiently only if the prime factors of N are known. The Quadratic Residuosity problem is believed to be computationally hard for unknown prime factors of N. (Cocks, 2001)

2.3 Identity based Encryption and Decryption Schemes

An identity string as such is a public key in an IBE scheme without a random oracle. An IBE scheme with a random oracle uses a hash of an identity string as a public key. In a hierarchical IBE scheme the identities are organized in a hierarchy tree (Gentry & Silverberg 2002). A hierarchical scheme is a generalization of identity based encryption. A fuzzy IBE scheme (Sahai & Waters 2007) allows an error tolerance in the identity when attempting to decrypt a message. An exact replica of the identity is not required to allow decryption. A fuzzy IBE scheme example is to use a measurement of a human biometric feature as an identity, which can change from one measurement to another. Characteristics of some IBE schemes are summarized in Table 1.

2.4 Authentication of Legitimate PKG Users

For authentication of legitimate PKG users, a publicly available user registration database maintained by the PKG is proposed in (Kumar, 2006) for a pairing based IBE scheme:

- A user U_{ID}, where ID is an identity string used as a user public key, chooses a nonce r_{ID} in the finite field defined by q and submits $\langle ID,(r_{ID}^{-1} \bmod q)\cdot P\rangle$ to the PKG
- The PKG verifies user credentials and registers the user by storing $\langle ID,(r_{ID}^{-1} \bmod q)\cdot P\rangle$ in the database
- The PKG issues a proof of registration $prf_{ID} = s\cdot H(ID||(r_{ID}^{-1} \bmod q)\cdot P)$ to the user.

A registered user requests a private key by submitting $\langle ID, r_{ID}\cdot P\rangle$ to the PKG. The PKG fetches $r_{ID}^{-1} \bmod q$ corresponding to ID from the database and authenticates the user by checking if $e(r_{ID}\cdot P,(r_{ID}^{-1} \bmod q)\cdot P)$ equals e(P,P).

2.5 Protected Private Key Submission

The private key of an authenticated user U_{ID} can be submitted by a PKG using an existing secure connection. If no secure connection exists, then the blinding technique proposed in (Kumar, 2006) can be used for a pairing based IBE cryptosystem. The PKG chooses a nonce x in the finite field defined by q, calculates the blinded private key $W= s\cdot Q_{ID}+x\cdot P$, $V=x\cdot(r_{ID}^{-1} \bmod q)\cdot P$ and submits $\langle W,V\rangle$ to the authenticated user. On receiving $\langle W,V\rangle$ the user U_{ID} unblinds the private key by calculating $s\cdot Q_{ID}=W- r_{ID}\cdot V$. The correctness of the received blinded private key is

verified by user U_{ID}, if $e(s \cdot Q_{ID}, P)$ equals $e(Q_{ID}, s \cdot P)$. The security of blinding is relies on the hardness to solve the Elliptic Discrete Logarithmic Problem.

Proposed in	(Boneh & Franklin 2003)	(Boneh & Boyen 2004)	(Cocks, 2001)
Based on	pairing	pairing	quadratic residuosity
Random oracle	yes	no	yes
Private master key	PKG chooses random $s \epsilon Z_q^*$	PKG chooses random $(x,y) \epsilon Z_q^*$	PKG chooses random primes (p, q), where p mod 4=q mod 4=3
Public IBE Parameters	prime q, G_1, G_2, pairing e, a generator point P of G_1, public master key $P_{pub}=s \cdot P$, integer n, hash functions $H_1:\{0,1\}^* \rightarrow G_1$, $H_2: G_2 \rightarrow \{0,1\}^n$	prime q, G_1, G_2, pairing e, a generator point P of G_1, public master key $(x \cdot P, y \cdot P)$	public master key $n=p \cdot q$, hash function H: $H(ID_{user})$ is integer i for which $(i/n)=1$ or $(-i/n)=1$
Private user key	$s_{user}=s \cdot H_1(ID_{user})$	(r, K) where $r \epsilon Z_q^*$ is random and $K=P/(ID_{user}+x+r \cdot y)$.	s_{user}=square root mod n of i or of n-i
Encrypt	encrypted message M is (U,V) where $U=r \cdot P$, $V=M \oplus H_2(e(H_1(ID_{user}),P_{pub})^r))$, and $r \epsilon Z_q^*$ is random	encrypted message $M \epsilon G_2$ is C=(X,Y,Z) where $X=ID_{user} \cdot t \cdot P+t \cdot x \cdot P$, $Y=t \cdot y \cdot P$, $Z=e(P,P)^t \cdot M)$, and $t \epsilon Z_q^*$ is random	For each message bit $b \epsilon \{+1,-1\}$ is picked random $\{t,t'\} \epsilon Z_n^*$ for which $(t/n)=(t'/n)=b$. Encryption of b is $(c_1,c_2)= ((t+(i/t)) \bmod n, (t'+(-i/t')) \bmod n)$
Decrypt	$M= V \oplus H_2(e(s_{user},U))$	$M = Z/e(X + r \cdot Y, K)$	For each b: if $(i/n)=1$ then $b=((2 \cdot s_{user}+c_1)/n)$ if $(-i/n)=1$ then $b=((2 \cdot s_{user}+c_2)/n)$

Table 1: Characteristics of some IBE schemes

2.6 Private Keys without Key Escrow Feature

Three trust levels are defined in (Girault, 1991) for a Trusted Third Party (TTP), which generates private keys in IBE:

- **Level I.** The TTP knows or can easily compute the private keys of users and can therefore impersonate any user at any time without being detected. The key escrow problem is thus unresolved.

- **Level II.** The TTP does not know or cannot easily compute the private keys of users. However, the TTP can still impersonate a user by generating a false public key without being detected.
- **Level III.** The TTP does not know or cannot easily compute the private keys of users. Moreover, a proof method exists with which a false public key for a user can be revealed. Thus the TTP cannot impersonate a user by generating a false public key.

For role based IBE security services in an organization trust level I is acceptable, if the organization acts as the TTP. Trust level I is even necessary for a role, which can be transferred from one person to another person. Example of role based security services are

- authentication for using computing, networking, and information resources
- protected storage of information associated with the role.

However, for non-repudiation IBE based signature services only trust level III is acceptable.

2.6.1 Distribution of a Secret Master Key across Multiple Key Issuing Authorities

In some proposals to distribute the secret master key multiple PKGs are used to generate private user key shares. The public master key of each PKG must be included in the public IBE parameters. A user requesting a private key constructs the private key from a subset of these shares with a threshold technique using Lagrange multipliers (Gemmell,1997). In this approach to avoid key escrow, proposed for example in (Boneh & Franklin 2003; Paterson, 2002; Hess, 2003), trust level III is obtained if at least one of the PKGs, which are selected by a user requesting a private key, is honest. However, the user must be registered at each PKG and each PKG must independently check and authenticate the user identity.

Another approach to distribute the secret master key is to use only one PKG and multiple Key Privacy Authorities (KPAs). A private user key issued by the PKG is then combined with the private shares of the KPAs selected by a user requesting a private key. The cost of user authentication is reduced, since only one PKG authenticates the user. Some distributed private key issuing protocols based on this approach have however been shown to obtain only trust level I in (Kumar et al. 2006), where another proposed distributed private key issuing protocol based on one PKG and multiple KPAs is proved to fulfill the requirements of trust level III. The protocol proposed in (Kumar et al. 2006) for pairing based IBE cryptosystems is a (t, n) threshold protocol with secure distribution of generated private user key shares. The (t, n) threshold property means distributed generation of a private user key with one PKG and n Key Privacy Authorities (KPA), of which at most $t<n$ are allowed to be dishonest. The distribution of generated private keys is protected by the blinding technique described in section 2.5.

2.6.2 Embedment of a User Generated Component in a Private Key

Embedding a user generated component in the private key issued by a PKG eliminates the key escrow problem, but a fundamental advantage of IBE is lost. Encryption with a user identity string and public IBE parameters is not possible since also the public key component associated with the user generated private key component is needed. However, some public key management advantage of IBE in comparison with a pure PKI cryptosystem is still preserved. Certificate-Based Encryption (CBE) and Certificateless Public Key Cryptography (CL-PKC) are two slightly different implementations of this approach.

In CBE, introduced in (Gentry, 2003), the IBE component of the private user key is time-dependent and is used as an implicit decryption certificate, which the PKG can deliver without protection. To get the IBE component of the private key, a user must deliver both an identity string and the public key component associated with the self-generated private key component. Certificate management is simple, since certificates are IBE generated. Only certificate validity times must be checked. There are no certification chains and no certificate revocation lists with associated management as in PKI. However, the PKG must renew a certificate before its validity time expires. In (Gentry, 2003) a CBE implementation based on the IBE scheme in (Boneh & Franklin 2003) is described.

CL-PKC, introduced in (Al-Riyami & Paterson 2003), is closely related to CBE. The difference is that private user key generation starts with generation of the IBE component, which depends only on the user identity string and must be delivered by the PKG through a secure communication channel. The full private user key is obtained by combining the IBE component with a user secret. The associated public key is derived by combining this user secret with the public IBE parameters. No certificate for the public user key is needed, since the trust in the user identity is derived from the generation of the IBE component of the private key. A private user key can even be derived afterwards from an identity string, since the public user key is independent of this string. In (Al-Riyami & Paterson 2003) a CL-PKC implementation based on the IBE scheme in (Boneh & Franklin 2003) is described.

2.6.3 Accountable Authority Identity based Encryption (A-IBE)

Key escrow in IBE means that a PKG can decrypt all information encrypted using an ID string in combination with the public IBE parameters of the PKG. A malicious PKG can also distribute copies of issued private keys to third parties.

In (Goyal, 2007) is introduced a private key issuing scheme called Accountable Authority Identity based Encryption (A-IBE). The probability to generate an exact copy of an issued private key for the same identity string is negligible for an A-IBE scheme. In an A-IBE scheme there is only one PKG with a secret master key, but there is still a super-polynomial number of possible private keys corresponding to every identity string. A user requesting a private key for an identity string will get one of all possible private keys. The PKG doesn't know which one of these possible private keys will be issued to the user, because the selection is based on private user data. A malicious PKG can of course generate another private key for the same identity string. Also this private key is a valid decryption key, but it will most probably be different from the private key issued to the user. If the PKG delivers a second private key to a third party, then the authentic user can by comparing the keys prove that the second private key is different from the authentic private key.

In the A-IBE scheme introduced in (Goyal, 2007), the set of possible private keys for an identity string consists of a super-polynomial number of key families. The family of a private key issued for an identity string by a PKG to a user depends on private user data. If another private key is issued for the same identity string without access to this private data, then the probability is negligible that both private keys belong to the same key family. The A-IBE scheme is thus an IBE scheme extended with the algorithm Trace, which outputs a family number for an inputted private key.

Two pairing based A-IBE implementations are in (Goyal, 2007) described and proved to have the required security properties.

3. Survey of Implemented and Proposed Security Services

In this section both commercial and non-commercial IBE based security services are presented.

3.1 Secure E-mail

Voltage SecureMail was the first commercial IBE providing e-mail signing and encryption (Voltage, 2007). Figure 1 illustrates how a user (Alice) can send IBE encrypted e-mail to another user (Bob). Bob is assumed to receive his first encrypted e-mail. In step 1, Alice encrypts the e-mail message using Bob's e-mail address, "bob@b.com", as the public key. When Bob receives the encrypted e-mail, he contacts and authenticates to the PKG (step 2). In step 3, after successful authentication, the PKG sends to Bob his private key needed in the e-mail message decryption.

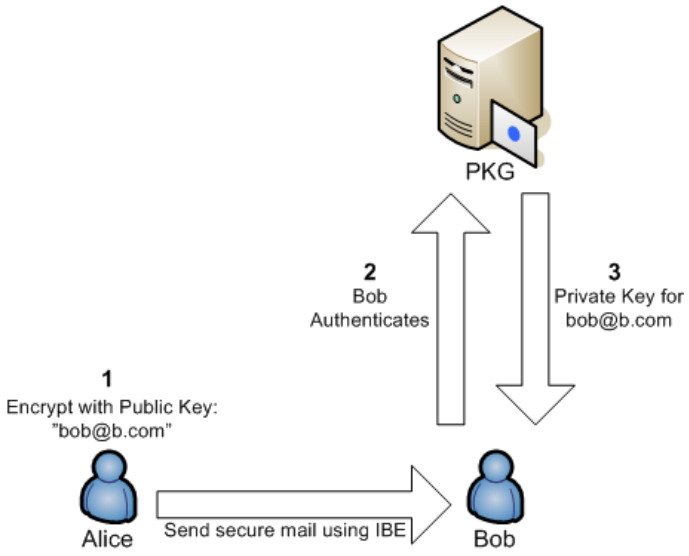

Figure 1: Sending secure mail using IBE**.**

3.2 Smartcard and Smart Phone Implementations

Smartcards can be used for secure private key storage and are currently common in traditional PKI environments. Gemplus has developed a prototype smart card performing IBE based encryption/decryption. This smartcard called Smart IBE, implements the whole Boneh-Franklin protocol. The entire pairing computation is performed on the smartcard. With Smart IBE, a user can e.g. send an encrypted SMS message using the recipients phone number as public key. (Gemplus, 2005)

NoreTech (NoreTech, 2004) has developed prototype implementations for Symbian OS and Microsoft Smartphone OS based mobile phones (McCullagh, 2005). The prototype implementations include toolkits and e-mail solutions based on recent IBE techniques.

3.3 Authentication and Key Agreement for Mobility Protocols

3.3.1 Mobile IPv4

In (Lee et. al., 2003) a Mobile IP authentication protocol using IBE is proposed. In Mobile IP, a Mobile Node (MN) located in a foreign network often needs to use resources provided by the foreign domain. An Authentication Authorization and Accounting (AAA) infrastructure provided by protocols such as RADIUS or Diameter is commonly used to verify the user's credentials and for billing. The entities in this IBE environment are the MN, the HA, and the AAA server in the MN's home network (AAAH). All nodes involved in the Mobile IP and AAA environment must be able to calculate IBE operations. AAAH is a PKG for the MNs. Network Access Identifiers (NAI) are used as IDs. Hence, the HA and the MN has private keys corresponding to their NAIs.

The MN and its HA performs mutual authentication through the FA and the AAAH. The authentication exchange is shown in Figure 2 where:

- ID = Identity. In this proposal NAI is used as ID
- S_{ID} = Private key corresponding to ID
- aaah@ = NAI of AAAH
- ha@ = NAI of HA
- mn@ = NAI of MN
- M_ = Message
- <<M>>S_{ID} = Signature of M with private key S_{ID}
- {M}ID = Encryption of M with ID.

3.3.2 Mobile IPv6

In Mobile IPv6 (Johnson et al. 2004), mutual authentication between a mobile node and its home agent is obligatory and normally uses IPSec (Internet Protocol Security). IKE (Internet Key Exchange) (Kaufman, 2005) is currently the only key agreement protocol in IPSec. Authentication in IKE is presently based on shared secrets, X.509 certificates, or EAP (Extensible Authentication Protocol) but could be modified to use IBE instead of certificates.

The Return Routability (RR) procedure is the standardised solution for securing communication between a mobile node and a correspondent node. This solution is however lightweight and vulnerable. To the RR procedure based on PKI have therefore been proposed alternatives (Vogt & Arkko 2007; Dupont & Combes 2007; Bao et al. 2007), which could be modified to use IBE instead of certificates.

3.3.3 SIP

An extension, providing identity-based authentication and key agreement, for the Session Initiation Protocol (SIP) is proposed in (Ring et. al. 2006). SIP Secure (SIPS) is a HTTP Secure (HTTPS) like protocol providing end to end security and certificate-based user authentication in SIP. In the proposal, a strong IBE based user authentication mechanism is presented which can

be implemented without changing the HTTP authentication semantics. A user's SIP identity, user@domain, is used as public key.

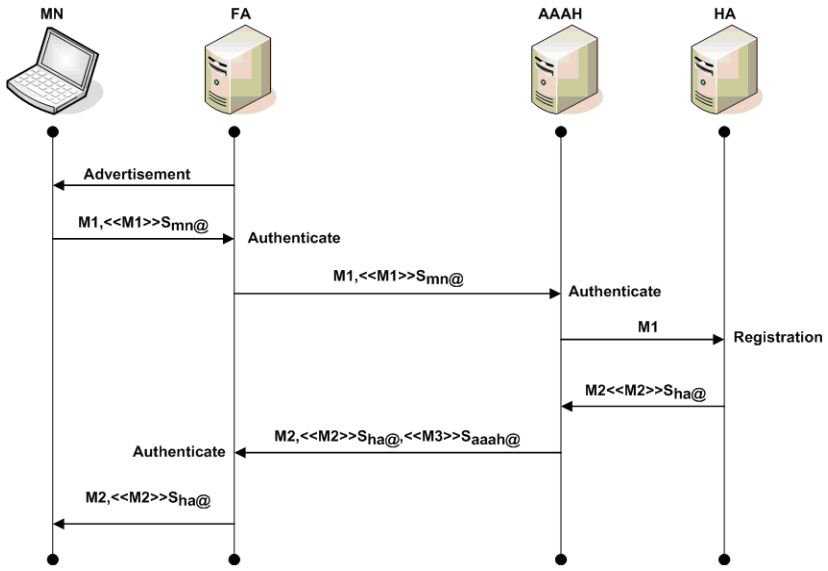

Figure 2: Proposed mutual Mobile IP authentication scheme based on IBE.

3.4 Health Care Information Systems

In (Mont et al. 2003) is presented an innovative IBE based solution to role based secure messaging. Confidential e-mails are encrypted using textual strings as public keys. These strings describe the disclosure policies (terms and conditions) under which the content of an e-mail can be disclosed, specifically a list of roles. A user can for example send a confidential e-mail to any consultant by using "Consultant" as a public key. The solution has been fully implemented and is currently used in a trial environment (a European health service organization) with Microsoft Outlook 2000 and an IBE Add-in as e-mail client. A web based HTTPS protected Trust Authority (TA) Service generates private user keys. A protected Microsoft SQL Server database contains up-to-date role lists and associations of people's identities to their current roles..

3.5 Secure Web Services

Proposals for how IBE may be used to simplify web security services are presented in (Crampton et al. 2007). Various ways of using IBE in public key distribution, access control, and securing XML (Extensible Markup Language) messages are discussed. A suite of key management services for the deployment of IBE in web services, called ID-XKMS (Identity – XML Key Management Specification), is also proposed.

3.6 Grid Security

In (Wei Lim, 2006) is proposed

- a fully identity-based key infrastructure for a grid, IKIG (Identity based Key Infrastructure for Grid),

- an alternative identity based approach, DKIG (Dynamic Key Infrastructure for Grid)
- a new password based protocol using IBE keys.

The idea of IKIG is to replace the current security services provided by GSI (Grid Security Infrastructure) in the Globus Toolkit (Globus, 2007) with some selected properties of Hierarchical Identity-Based Cryptography (HIBC). GSI is based on a PKI with X.509 certificates. DKIG is intended to solve the key escrow problem by combining IBE and the current PKI approach. Each user publishes a fixed parameter with a standard X.509 certificate. Even though X.509 certificates are involved, DKIG is still more lightweight than GSI since the derivation of both long-term and proxy credentials on-the-fly is enabled only for a fixed certificate. The password based protocol is a TLS-like IBE protocol for securing interactions between users and credential storage systems, such as MyProxy (MyProxy, 2007).

4. Performance of IBE Schemes

IBE offers functional advantages over conventional public key methods, but the computational costs or data communication costs are higher.

4.1 Pairing based IBE Schemes

IBE operation performance depends on the required number and the execution times of the following costly operations:

- pairing.
- field exponentiation (integer exponentiation in a finite field)
- point multiplication (integer multiplication of a discrete elliptic curve point in a finite field)

Encryption or decryption requires one pairing and one point multiplication. Encryption also requires one field exponentiation. As a comparison, only one field exponentiation is required in RSA encryption or decryption. However, for equal information security, the field size in RSA is about seven times the group size in IBE. Field exponentiation is therefore significantly more expensive for RSA. Execution time measurements on a 3 GHZ Pentium IV computer are shown in Table 2. To provide the same information security, 1024 bit RSA keys and an IBE group size of about 160 bit are used. IBE encryption/decryption is measured to be more than twice as expensive as RSA encryption.

The execution time of pairing on a 3 GHZ Pentium computer can however be reduced with two decades with a hardware accelerator. In (Beuchat et al. 2007) is described a 150 MHz FPGA based accelerator for $GF(3^{97})$ with a pairing time of about 30 μs.

4.2 IBE Schemes Based on Quadratic Residuosity

Encryption and decryption is computationally very cheap in comparison with both pairing and RSA, since required operations (hashing, modulo inverses of integers, and calculation of Jacobi symbols) are fast. However, data communication is expensive. Since each encrypted bit must be represented by two 1024 bit integers to achieve 1024 bit RSA security, only about 0.05% of the available bandwidth is utilized.

	GF(2^{379}) ηT pairing	GF(p) Tate pairing	GF(p)Ate pairing
Pairing	3.88	2.91	3.10
Point multiplication	1.82	3.08	1.17
Field exponentiation	1.14	0.54	0.62
RSA decryption	1.92		

Table 2: Execution times in milliseconds on a 3GHz Pentium IV computer (Scott, 2007).

5. Conclusions

Identity Based Encryption (IBE) is a very important area in cryptology research. The first concrete IBE system based on pairing of discrete points on elliptic curves was proposed in (Boneh & Franklin, 2001). IBE schemes based on quadratic residuosity have also been proposed. The implementation of IBE in security services is still in an early stage, but many proposals have already been presented. IBE software has been developed and is available also as open source software. Commercial security software with security services implemented with IBE is available and IETF standardization of IBE has started.

A key issue in the implementation of security services is private key management. For secure distribution of private keys generated by a PKG over unprotected communication channels, blinding techniques based on the elliptic curve cryptography and pairing operations have been proposed and implemented.

Key escrow in IBE is a consequence of the requirement that all private user keys must be created from the same master key in a PKG. Key escrow can be avoided by a proper use of threshold cryptography when private user keys are issued. However, the required distributed PKG architecture adds significant complexity to an IBE scheme.

The most important advantage of IBE is that management of public key certificates and certificate revocation lists is not needed, since a public user key is an identity string. This is especially an advantage for mobile computing devices with limited bandwidth and limited computational power. However, the computational costs of the actual cryptographic operations are higher in IBE than in traditional public key methods.

References

Al-Riyami, S. and K. Paterson, K. (2003) Certificateless Public Key Cryptography, In Advances in Cryptology - Asiacrypt'03, LNCS 2894, Springer-Verlag, pp. 452-473.

Appenzeller, G., Martin, L., and Schertler, M. (2007) Identity-based Encryption Architecture, IETF Internet Draft

Bao, F., Deng, R., Qiu, Y., and Zhou, J. (2007) Certificate Based Binding Update Protocol (CBU), IETF Internet Draft.

Beuchat, J.-L., Shirase, M., Takagi, T., and Okamoto, E. (2007) An Algorithm for the η_T Pairing Calculation in Characteristic Three and its Hardware Implementation, in Kornerup, P. and

Muller, J.-M. (Eds), *Proceedings of the 18th IEEE Symposium on Computer Arithmetic*, 97-104, IEEE Computer Society.

Boneh, D. and Boyen, X. (2004) *Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles*. In Advances in Cryptology - Eurocrypt'04, LNCS 3027, Springer-Verlag, pp. 223-238

Boneh D., Franklin M. (2001). *Identity-Based Encryption from the Weil Pairing*, in Proceedings of Crypto 2001, LNCS 2139, Springer-Verlag, pages 213-29

Boneh D., Franklin M. (2003). *Identity-Based Encryption from the Weil Pairing*, SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615

Cha, J.C., and Cheon, J.H. (2002) *An Identity-Based Signature from Gap Diffie-Hellman Groups,* in Cryptology ePrint Artchive, Retrieved March 11th, 2008, from http://eprint.iacr.org/2002/018

Cocks, C. (2001) *An Identity based Encryption Scheme based on Quadratic Residues.* Eight IMA International Conference on Cryptography and Coding, Dec. 2001, Royal Agricultural College, Cirencester, UK

Crampton, J., Wei Lim, H., and Paterson, K. G. (2007) What can identity-based cryptography offer to web services? in Proceedings of the 2007 ACM workshop on Secure web services. Fairfax, Virginia, USA. PP. 26 - 36

Dupont, F. and Combes, J. –M. (2007) Using IPSec between Mobile and Correspondent IPv6 Nodes, IETF Internet Draft

Galbraith, S. D., Harrison, K., and Soldera, D. (2002). *Implementing the Tate pairing*, HP Labs Technical Reports HPL-2002-23, Retrieved March 11th, 2008, from http://www.hpl.hp.com/techreports/2002/HPL-2002-23.pdf

Galindo D. (2005) *Boneh-Franklin Identity Based Encryption Revisited*. In Automata, Languages and Programming, LNCS 3580, Springer-Verlag, pp. 791-802.

Gemmell, P. (1997). *An Introduction to Threshold Cryptography,* in CryptoBytes, a technical newsletter of RSA Laboratories, Vol. 2, No. 7, Retrieved March 11th, 2008, from ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto2n3.pdf

Gemplus. (2005). Gemplus develops the world's first Identity-Based Encryption for smart cards. Gemplus press release, Retrieved March 11th, 2008, from http://www.gemalto.com/press/index.html

Gentry, C. (2003) *Certificate-Based Encryption and the Certificate Revocation Problem*, In Advances in Cryptology- Eurocrypt'03, LNCS 547, Springer-Verlag, pp.272-293

Gentry, C. (2006) *Practical identity-based encryption without random oracles*, in Advances in Cryptology – Eurocrypt'06, LNCS 4004, Springer-Verlag, pp. 445-464

Gentry, C. and Silverberg, A. (2002) *Hierarchical ID-based Cryptography*, in Advances in Cryptology – ASIACRRYPT'02, LNCS 2501, Springer-Verlag, pp. 548-566

Girault, M. (1991) *Self-certified public keys,* in EUROCRYPT 1991, LNCS 547, Springer-Verlag, pp. 490-497

Globus Toolkit Homepage (2007) Retrieved March 11th, 2008, from http://www.globus.org/toolkit/

GMP web pages (2007). Retrieved March 11th, 2008, from http://gmplib.org/

Goyal, V. (2007) *Reducing Trust in the PKG in Identity Based Cryptosystems*, in Advances in Cryptology - CRYPTO 2007, LNCS 547, Springer-Verlag, pp. 490-497

Hess, F. (2003) *Efficient Identity Based Signature Schemes Based on Pairings*, in Selected Areas in Cryptography-SAC'02, LNCS 2595, Springer-Verlag, 310-324

Hess, F., Smart, N., and Vercauteren, F. (2006). The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, 52(10), pp. 4595–4602. October 2006

IBE Secure Email (2007) Stanford University, Retrieved March 11th, 2008, from http://crypto.stanford.edu/ibe/

Identity Based Encryption JCE Provider. (2007). National University of Ireland, Retrieved March 11th, 2008 from http://www.crypto.cs.nuim.ie/software/eyebee/

Johnson, D., Perkins, C., and Arkko, J. (2004) Mobility Support in IPv6, RFC 3775

Kaufman, C. (2005) Internet Key Exchange (IKEv2) Protocol, RFC 4306

Kumar, K.P., Shailaja, G., and Saxena, A (2006). *Secure and Efficient Threshold Key Issuing Protocol for ID-based Cryptosystems,* Cryptology ePrint Archive, Report 2006/245, Retrieved March 11th, 2008, from http://eprint.iacr.org/2006/245.pdf

Lee, B-G., Choi, D.-H., Kim, H-G., Sohn, S.-W., and Park, K-H (2003) Mobile IP and WLAN with AAA Authentication Protocol using Identity-based Cryptography, in Proceedings of the 10th International Conference on Telecommunications, ICT'2003, Tahiti, Papeete, French Polynesia, February 23 – March 1, 2003, ISBN 0-7803-7661-7, Volume 1, pp. 597-603

McCullagh, N. (2005) Securing E-Mail with Identity-Based Encryption, in IT Pro, Volume 7, Issue 3, May 2005, IEEE Educational Activities Department, ISSN: 1520-9202, pp. 64-63

Menezes, A.J. (1994) *Elliptic Curve Public Key Cryptosystems,* USA: Kluwer Academic Publishers. ISBN: 0-792-39368-6

Mont, M. C., Bramhall, P, Dalton, C. R., and Harrison K. (2003) A Flexible Role-based Secure Messaging Service Exploiting IBE Technology in a Health Care Trial, White paper, Hewlett Packard, McAfee.

MyProxy Credential Management Service (2007) Retrieved March 11th, 2008, from http://grid.ncsa.uiuc.edu/myproxy/

NoreTech. (2004) Noretech: Identity Based Encryption. Retrieved March 11th, 2008, from http://www.noretech.com/

Paterson, K. (2002) *Cryptography from Pairings: a snap shot of current research*, Information Security Technical Report, Vol. 7(3), 41-54, 2002

PBC library (2007) Stanford University, Retrieved March 11th, 2008 from http://crypto.stanford.edu/pbc/

Ring, J., Choo, K-K C, Foo, E., and Looi, M. (2006) A New Authentication Mechanism and key Agreement Protocol for SIP Using Identity-based Cryptography, in Proceedings of AusCERT Asia Pacific Information Technology Security Conference 2006, Gold Coast, Australia

Sahai A. and Waters B. (2007) *Fuzzy Identity-Based Encryption,* E-print 2004/086, Retrieved March 11th, 2008, from http://eprint.iacr.org/2004/086.pdf

Scott, M. (2007) Implementing Cryptographic Pairings, in Takagi, T., Okamoto, Tat., Okamoto, E., and Okamoto, Tak. (Eds.) *Pairing-Based Cryptography:* Proceedings of First International Conference, Pairing 2007, Tokyo, Japan, July 2-4, 2007**,** 177-196, Springer-Verlag: LNCS. 4575.

Shamir, A. (1984) *Identity-based cryptosystems and signature schemes,* in Advances in Cryptology - Crypto'84, LNCS 196*,* Springer-Verlag, pp. 47-53

Vogt, C. and Arkko, J. (2007) A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization, RFC 4651

Voltage Security (2007) Retrieved March 11th, 2008, from http://www.voltage.com

Wei Lim, H. (2006) On the Application of Identity-Based Cryptography in Grid Security, Doctoral Thesis. Department of Mathematics Royal Holloway, University of London