A Survey of Identity-Based Cryptography

Joonsang Baek[1] Jan Newmarch[2], Reihaneh Safavi-Naini[1], and Willy Susilo[1]
[1] School of Information Technology and Computer Science, University of Wollongong
{baek, rei, wsusilo}@uow.edu.au
[2] School of Network Computing, Monash University
jan.newmarch@infotech.monash.edu.au

Abstract

In this paper, we survey the state of research on identity-based cryptography. We start from reviewing the basic concepts of identity-based encryption and signature schemes, and subsequently review some important identity-based cryptographic schemes based on the bilinear pairing, a computational primitive widely used to build up various identity-based cryptographic schemes in the current literature. We also survey the cryptographic schemes such as a "certificate-based encryption scheme" and a "public key encryption scheme with keyword search", which were able to be constructed thanks to the successful realization of identity-based encryption. Finally, we discuss how feasible and under what conditions identity-based cryptography may be used in current and future environments and propose some interesting open problems concerning with practical and theoretical aspects of identity-based cryptography.

1 Introduction

In 1984, Shamir [31] proposed a concept of identity-based cryptography. In this new paradigm of cryptography, users' identifier information such as email or IP addresses instead of digital certificates can be used as public key for encryption or signature verification. As a result, identity-based cryptography significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as Public Key Infrastructure (PKI).

Although Shamir [31] easily constructed an identity-based signature (IBS) scheme using the existing RSA [28] function, he was unable to construct an identity-based encryption (IBE) scheme, which became a long-lasting open problem. Only recently in 2001, Shamir's open problem was independently solved by Boneh and Franklin [8] and Cocks [15]. Thanks to their successful realization of identity-based encryption, identity-based cryptography is now flourishing within the research community.

2 Basic Concepts of Identity-Based Encryption and Signature

Basic Concept of IBE. As mentioned earlier, in the IBE scheme, the sender Alice can use the receiver's identifier information which is represented by any string, such as email or IP address, even a digital image [29], to encrypt a message. The receiver Bob, having obtained a private key associated with his identifier information from

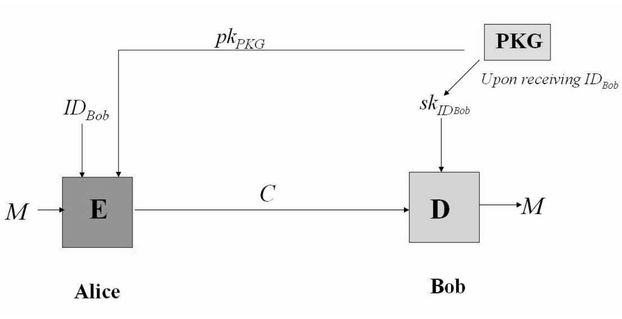

Figure 1: Identity-Based Encryption

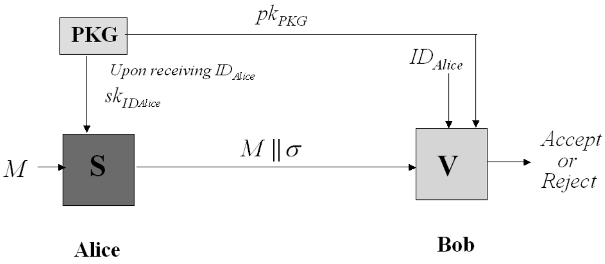

Figure 2: Identity-Based Signature

the trusted third party called the "Private Key Generator (PKG)", can decrypt the ciphertext.

Summing up, we describe an IBE scheme using the following steps. (Figure 1 illustrates a schematic outline of an IBE scheme).

- Setup: The PKG creates its master (private) and public key pair, which we denote by sk_{PKG} and pk_{PKG} respectively. (Note that pk_{PKG} is given to all the interested parties and remains as a constant system parameter for a long period.)

- Private Key Extraction: The receiver Bob authenticates himself to the PKG and obtains a private key $sk_{\texttt{ID}_{Bob}}$ associated with his identity $\texttt{ID}_{Bob}$.

- Encryption: Using Bob's identity $\texttt{ID}_{Bob}$ and the PKG's pk_{PKG}, the sender Alice encrypts her plaintext message M and obtains a ciphertext C.

- Decryption: Upon receiving the ciphertext C from Alice, Bob decrypts it using his private key $sk_{\texttt{ID}_{Bob}}$ to recover the plaintext M.

As a mirror image of the above identity-based encryption, one can consider an identity-based signature (IBS) scheme. In this scheme, the signer Alice first obtains a signing (private) key associated with her identifier information from the 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. More precisely, an IBS scheme can be described using the following steps. (Figure 2 illustrates a schematic outline of an IBS scheme).

- Setup: The Private Key Generator (PKG), which is a trusted third party, creates its master (private) and public key pair, which we denote by sk_{PKG} and pk_{PKG} respectively.

- Private Key Extraction: The signer Alice authenticates herself to the PKG and obtains a private key $sk_{\texttt{ID}_{Alice}}$ associated with her identity $\texttt{ID}_{Alice}$.

- Signature Generation: Using her private key $sk_{\texttt{ID}_{Alice}}$, Alice creates a signature σ on her message M.

- Signature Verification: Having obtained the signature σ and the message M from Alice, the verifier Bob checks whether σ is a genuine signature on M using Alice's identity $\texttt{ID}_{Alice}$ and the PKG's public key pk_{PKG}. If it is, he returns "*Accept*". Otherwise, he returns "*Reject*".

3 Identity-Based Cryptographic Schemes from the Bilinear Pairing

We first review the "admissible bilinear pairing", which is a mathematical primitive that has been playing a central role in current identity-based cryptography since it was used in Boneh and Franklin's identity-based encryption scheme [8]. (Note that differently from Boneh and Franklin, Cocks [15] used a variant of "integer factorization" problem to construct his IBE scheme. However, the scheme is inefficient in that a plaintext message is encrypted bit-by-bit and hence the length of the output ciphertext becomes long. For this reason, in this paper, we focus only on the pairing-based identity-based cryptographic schemes which are more widely used in practice).

Definition of the Bilinear Pairing. The admissible bilinear pairing $\hat{e}$ is defined over two groups of the same prime-order q denoted by $\mathcal{G}$ and $\mathcal{F}$. (By $\mathcal{G}^*$ and $\mathbb{Z}_q^*$, we denote $\mathcal{G} \setminus \{O\}$ where O is the identity element of $\mathcal{G}$, and $\mathbb{Z}_q \setminus \{0\}$ respectively.) We will use an additive notation to describe the operation in $\mathcal{G}$ while we will use a multiplicative notation for the operation in $\mathcal{F}$. In practice, the group $\mathcal{G}$ is implemented using a group of points on certain elliptic curves, each of which has a small MOV exponent [27], and the group $\mathcal{F}$ will be implemented using a subgroup of the multiplicative group of a finite field. The admissible bilinear map, denoted by $\hat{e} : \mathcal{G} \times \mathcal{G} \to \mathcal{F}$, has the following properties.

- Bilinear: $\hat{e}(aR_1, bR_2) = \hat{e}(R_1, R_2)^{ab}$, where $R_1, R_2 \in \mathcal{G}$ and $a, b \in \mathbb{Z}_q^*$.
- Non-degenerate: $\hat{e}$ does not send all pairs of points in $\mathcal{G} \times \mathcal{G}$ to the identity in $\mathcal{F}$. (Hence, if R is a generator of $\mathcal{G}$ then $\hat{e}(R, R)$ is a generator of $\mathcal{F}$.)
- Computable: For all $R_1, R_2 \in \mathcal{G}$, the map $\hat{e}(R_1, R_2)$ is efficiently computable.

Throughout this paper, we will simply use the term "bilinear pairing" to refer to the admissible bilinear pairing defined above.

Bilinear Diffie-Hellman Assumption. The above bilinear pairing gave rise to the following computational problem called "Bilinear Diffie-Hellman (BDH)" problem:

- Given $(\mathcal{G}, q, \hat{e}, P, aP, bP, cP)$ where a, b, and c are chosen at random from $\mathbb{Z}_q^*$, compute $\hat{e}(P, P)^{abc}$.

The BDH assumption means that the above problem is computationally intractable. Note that the security of many identity-based cryptographic schemes in the current literature depends on the BDH assumption (or its variations).

Non-Identity-Based Schemes Based on the Bilinear Pairing. Not only for identity-based cryptographic schemes, the bilinear pairing has been used for constructing other interesting non-identity-based cryptographic schemes. One of them is the surprising "Tripartite Key Agreement" protocol proposed by Joux [23]. Suppose that Alice, Bob, and Chris have private/public key pairs (a, aP), (b, bP), and (a, cP) where $a, b, c \in \mathbb{Z}_q^*$ are chosen at random and $aP, bP, cP \in \mathcal{G}$. Without the bilinear pairing, to share the same key, a number of interactions must be conducted by the three persons. But, if the bilinear pairing is employed, this can be done in *one round*: Alice, Bob, and Chris compute $\hat{e}(bP, cP)^a$, $\hat{e}(aP, cP)^b$, and $\hat{e}(aP, bP)^c$! (It is easy to see that $\hat{e}(bP, cP)^a = \hat{e}(aP, cP)^b = \hat{e}(aP, bP)^c = \hat{e}(P, P)^{abc}$ by the bilinear property of $\hat{e}$).

Other notable cryptographic schemes based on the bilinear pairing include Boneh, Lynn, and Shacham's [11] signature scheme that outputs a very short signature, which was extended into a number of special signature schemes [10]. Based on the short signature proposed by Boneh et al. [11], Boldyreva [6] designed efficient threshold and blind signature schemes.

Boneh and Frankiln's IBE Scheme. We now describe Boneh and Franklin's famous IBE scheme.

In the setup stage, the PKG specifies a group $\mathcal{G}$ generated by $P \in \mathcal{G}^*$ and the bilinear pairing $\hat{e} : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{F}$. It also specifies two hash functions $\mathsf{H}_1 : \{0,1\}^* \rightarrow \mathcal{G}^*$ and $\mathsf{H}_2 : \mathcal{F} \rightarrow \{0,1\}^l$, where l denotes the length of a plaintext. The PKG then picks a master key $s \in \mathbb{Z}_q^*$ at random and computes a public key $P_{\mathrm{PKG}} = sP$. The PKG publishes descriptions of the group $\mathcal{G}$ and $\mathcal{F}$ and the hash functions H_1 and H_2 as well as P_{PKG}. Bob, the receiver, then contacts the PKG to get his private key $D_{\mathtt{ID}} = sQ_{\mathtt{ID}}$ where $Q_{\mathtt{ID}} = \mathsf{H}_1(\mathtt{ID})$. Alice, the sender, can now encrypt her message $M \in \{0,1\}^l$ using Bob's identity $\mathtt{ID}$ by computing $U = rP$ and $V = \mathsf{H}_2(\hat{e}(Q_{\mathtt{ID}}, P_{\mathrm{PKG}})^r) \oplus M$, where r is chosen at random from $\mathbb{Z}_q^*$ and $Q_{\mathtt{ID}} = \mathsf{H}_1(\mathtt{ID})$. The resulting ciphertext $C = (U, V)$ is sent to Bob. Bob decrypts C by computing $M = V \oplus \mathsf{H}_2(\hat{e}(D_{\mathtt{ID}}, U))$.

Note that the above scheme was proven to be secure against chosen plaintext attack in the random oracle model assuming the BDH problem is computationally hard. (The random oracle model means that underlying hash functions used in the scheme are assumed to be ideal random functions [5]). It was also presented in [8] that how the above scheme can be modified into a scheme that prevents chosen ciphertext attack which is stronger than chosen plaintext attack. (Readers are referred to Mao's [25] recent book for an exposition of formal security analysis.)

Hierarchical IBE scheme. One drawback of the IBE scheme is that heavy workloads are imposed on a single PKG. To resolve this problem, Horwitz and Lynn [22] suggested that a hierarchy of PKGs in which the PKGs have to compute private keys only to the entities immediately below them in the hierarchy should be incorporated to a normal IBE scheme. In this hierarchical IBE scheme, which we call a "HIBE" scheme, the users are no longer identified by a single identity, but by a tuple of identities which contains the identity of each of their ancestors in the hierarchy. As an example, Bob's identity in the HIBE system may be represented as $(\mathsf{ID}_{Bob}, \mathsf{ID}_{Company}) = (\mathtt{Bob}, \mathtt{cryptworld.com})$.

Similarly to the case of the design and realization of an IBE scheme, Horwitz and Lynn could not have a fully functional HIBE scheme. Shortly after Lynn et al's proposal, Gentry and Silverberg [21], however, realized a fully-function HIBE scheme that allows a general n-level hierarchy using Boneh and Franklin's IBE scheme.

Other Extensions of the IBE scheme. One of the extensions of an IBE scheme is to give a "threshold decryption" feature to it. In Baek and Zheng's [4] identity-based threshold decryption scheme, a user who obtained a private key associated his identity can distribute the key into a number of decryption servers using a variant of Shamir's secret sharing scheme [30]. The receiver sends the ciphertext to each of the decryption servers to get a "decryption share". If the number of the decryption shares that the receiver holds reaches some "threshold", he will be able to recover the whole plaintext.

Chen, Harrison, Soldera, and Smart [17] illustrated how multiple PKGs/identities in Boneh and Franklin's IBE scheme can be applied to the real world situations. Subsequently, Smart [33] extended the work of [17] to apply IBE schemes to access controls.

Cha and Cheon's IBS Scheme. Below, we describe Cha and Cheon's [16] IBS scheme which is based on the bilinear pairing. (Note that an IBS scheme was already constructed when Shamir [31] proposed the concept of identity-based cryptography in 1984. However, since

Boneh and Franklin used the bilinear pairing to realize IBE scheme, many IBS schemes based on the bilinear pairing have been constructed recently). In the setup stage, the PKG specifies a group $\mathcal{G}$ generated by $P \in \mathcal{G}^*$ and the Bilinear map $\hat{e} : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{F}$. It also specifies two hash functions $\mathsf{H}_1 : \{0,1\}^* \rightarrow \mathcal{G}^*$ and $\mathsf{H}_2 : \{0,1\}^* \times \mathcal{G} \rightarrow \mathbb{Z}_q^*$. The PKG then picks a master key s uniformly at random from $\mathbb{Z}_q^*$ and computes a public key $P_{\mathrm{PKG}} = sP$. The PKG publishes descriptions of the group $\mathcal{G}$ and $\mathcal{F}$, the public key P_{PKG}, and the hash functions H_1 and H_2. Alice, the signer, then contacts the PKG to get his private key $D_{\mathtt{ID}} = sQ_{\mathtt{ID}}$ where $Q_{\mathtt{ID}} = \mathsf{H}_1(\mathtt{ID})$. Alice can create a signature on a message M by computing $U = rQ_{\mathtt{ID}}$ and $V = (r + h)D_{\mathtt{ID}}$, where r is chosen at random from $\mathbb{Z}_q^*$ and $h = \mathsf{H}_2(M, U)$. The verifier Bob can verify the validity of Alice's signature (U, V) by checking whether $\hat{e}(P, V) = \hat{e}(P_{PKG}, U + hQ_{\mathtt{ID}})$.

Note that the above scheme was shown to be secure against chosen message attack in the random oracle model.

Other IBS Schemes and Extensions. Hess [19] also constructed IBS schemes based on the bilinear pairing. Zhang and Kim [35] constructed identity-based blind signature and ring signature schemes. (Roughly speaking, a blind signature scheme is to create a valid signature without having the signer seeing the message that he signs, which may be needed in electronic commerce application. A ring signature scheme is to provide "signer ambiguity" in such a way that the verifier does know one of the a group members singed a message but does not know exactly who signed it). Another notable work on IBS scheme includes Ateniese and Medeiros's [1] identity-based Chameleon signature scheme. (The distinguishing characteristic of chameleon signatures is that they are non-transferable, with only the designated recipient capable of asserting its validity). Their scheme takes advantage of the general identity-based cryptography that the owner of a public key does not necessarily need to retrieve the associated secret key.

In addition, there is a series of work on identity-based signcryption schemes which provide property of IBE and IBS at the same time. Readers are referred to the papers of Boyen [13], Malone-Lee [26], and Libert and Quisquater [24].

4 Other Non-Identity-Based Cryptographic Schemes Related to IBE

Certificate-Based Encryption Scheme. The main motivation for a "certificate-based encryption (CBE)" scheme is to provide a "implicit certification" of public and private key pairs in normal public key cryptography. In a CBE scheme, to decrypt a ciphertext, a user needs to hold his private key and an up-to-date *certificate* from the Certification Authority (CA). Without the certificate, the user is unable to decrypt the ciphertext. This implicit certification is especially useful in public key encryption as the sender of a message does not have to obtain a "certification status information" which checks whether the intended receiver's certificate has been revoked or not.

Formally, an CBE scheme can be described in the following steps. (Note that)

- CA Setup: The CA creates its private and public key pair, which we denote by sk_{CA} and pk_{CA} respectively.
- User Setup: The receiver Bob (a user) creates his private and public key pair, which we denote by sk_{Bob} and pk_{Bob} respectively.
- Certificate Update: The receiver Bob brings his public key pk_{Bob} to the CA and requests a certificate. Upon receiving Bob's request, the CA takes its private key sk_{CA}

and Bob's public key pk_{Bob} to create a certificate. It returns the corresponding certificate $\mathtt{Cert}_{Bob}$ to Bob.

- Encryption: Using the CA's public key pk_{CA} and Bob's public key pk_{Bob}, the sender Alice encrypts her plaintext message M and obtains a ciphertext C.
- Decryption: Upon receiving the ciphertext C from Alice, Bob decrypts it using his private key sk_{Bob} and the certificate $\mathtt{Cert}_{Bob}$ to recover the plaintext M.

Gentry's Scheme. We now describe Gentry's CBE scheme as described in [20]. In the CA setup stage, the CA specifies a group $\mathcal{G}$ generated by $P \in \mathcal{G}^*$ and the Bilinear map $\hat{e} : \mathcal{G} \times \mathcal{G} \to \mathcal{F}$. It also specifies two hash functions $\mathsf{H}_1 : \{0,1\}^* \to \mathcal{G}^*$ and $\mathsf{H}_2 : \mathcal{F} \to \{0,1\}^l$, where l denotes the length of a plaintext. The CA then picks a master key s uniformly at random from $\mathbb{Z}_q^*$ and computes a public key $Y_{\text{CA}} = sP$. The CA publishes descriptions of the group $\mathcal{G}$ and $\mathcal{F}$ and the hash functions H_1 and H_2. Suppose that Bob, the receiver, has a public and private key pair $(x, Q_{Bob} = xP)$, where $x \in \mathbb{Z}_q^*$ is chosen at random. Suppose also that Bob has sent his identifier information $\mathtt{BobsInfo}$ which contains his public key Q_{Bob} to the CA and obtained a certificate $\mathtt{Cert}_{Bob} = s\mathsf{H}(\mathtt{Bobsinfo}, Y_{CA},)$. Alice, the sender, can now encrypt her message $M \in \{0,1\}^l$ using $\mathtt{BobsInfo}$ by computing $U = rP$ and $V = \mathsf{H}_2(\hat{e}(Y_{CA}, \mathsf{H}(\mathtt{BobsInfo}, Y_{CA}))^r$ $\hat{e}(Q_{Bob}, \mathsf{H}(\mathtt{BobsInfo}))^r) \oplus M$, where $r \in \mathbb{Z}_q^*$ is chosen at random. The resulting ciphertext $C = (U, V)$ is sent to Bob. Bob decrypts C by computing $M = V \oplus \mathsf{H}_2(\hat{e}(U, s\mathsf{H}(\mathtt{Bobsinfo}, Y_{CA}) + x\mathsf{H}(\mathtt{BobsInfo})))$.

Public Key Encryption with Keyword Search. More recently, Boneh, Di Crescenzo, R. Ostrovsky, and G. Persiano [12] proposed a public key encryption scheme with keyword search (PEKS). Suppose that Bob sends an email to Alice. To protect the privacy of the contents, Bob encrypted the body of the email and some keyword such as "urgent" using Alice's public key. In this case, however, the email gateway such as IMAP or POP server cannot read the keyword and hence cannot make a decision as to whether the email should be forwarded to Bob with high priority. The PEKS scheme is to enable Alice to give the gateway the ability called "trapdoor" to test whether "urgent" is a keyword of the email in such a way that the email gateway and other possible attackers do not learn anything about the body of the email.

In [12], the PEKS scheme is constructed using the similar technique used in Boneh and Franklin's IBE scheme. Suppose that Alice publishes her public key sP where $s \in \mathbb{Z}_q^*$ is a private key chosen at random. Bob encrypts his message Musing any ElGamal [18]-like public key encryption scheme and creates an encryption of a keyword W by computing $(U, V) = (rP, \mathsf{H}_2(\hat{e}(\mathsf{H}_1(W), sP)^r))$ where H_1 and H_2 are hash functions. When Alice sends a trapdoor $T_w = s\mathsf{H}_1(W)$ to trapdoor, the email gateway can check whether $\hat{e}(T_w, U) = V$ and retrieve the email accordingly.

5 Implementation and applications of IBE

By the group of people including Boneh and Franklin [9], the IBE scheme designed in [8], which they call "Stanford IBE system", was implemented under Debian GNU/Linux. (The source code is available at `http : //crypto.stanford.edu/ibe/download.html`).

Shamus Software [32] also developed a cryptographic library called "MIRACL" that includes Boneh and Franklin's IBE scheme.

Both of Stanford and Shamus's library were developed using C/C++. To our knowledge, there has been no Java implementation of IBE in the public domain.

The notable real world applications of IBE include the IBE email system developed by Voltage Security [34], which provides plug-ins for Outlook, pine, hotmail, and Yahoo. Also, researchers from Hewlett Packard Lab in Bristol, UK [14] developed a health care information system that facilitates an IBE capability.

6 Discussion and Open Problems

Key Escrow Problem. Unfortunately, all identity-based cryptographic schemes have inherent weakness, a "key escrow" property. Recall that in IBE and IBS schemes, the PKG issues private keys for user using its master secret key. As a result, the PKG is able to decrypt or sign any messages. In terms of encryption, this property might be useful in some situations where user's privacy can possibly be limited, for example, due to the involvement in the crime, the user's message should be opened by a court order. However, in terms of signature, this key escrow property is not desirable at all since the "non-repudiation" property is one of the essential requirement of digital signature schemes. (Non-repudiation means that only an entity which possesses a signing key can create a valid signature).

As a countermeasure for the above key escrow problem, Boneh and Franklin [8] suggested that the master secret key of the PKG be distributed using Shamir's [30] secret sharing technique into a number of PKGs. The user then obtains partial private key shares associated with his identity from the multiple PKGs and reconstruct a whole private key. But this "multiple PKG" method impose heavy loads on users since they should authenticate themselves to the multiple PKGs, which takes big communication and computational cost.

As a result, the use of identity-based cryptography may be limited to the environment where the PKG is unconditionally trusted, for example, inside of a company or a particular organization. Hence, a big question here is: Is it possible to construct an *efficient* IBE or IBS scheme that does suffer from the key escrow problem?

Revocation Problem. In non-identity-based cryptography, the revocation of the public key is a big problem in that users who want encrypt messages or verify signatures should first check whether the concerning public keys have been revoked or not. To do this, current PKI requires to maintain Certificate Revocation List (CRL). Management of CRLs may be one of the factors that slows down the deployment of PKI. In identity-based schemes, this problem no longer exists as any identities can be served as public keys. However, another kind of revocation problem occurs in identity-based cryptography. Suppose that Bob wants others to use his email address to encrypt messages. But, suppose that the private key associated with Bob's email address has been compromised, so he cannot use his email address as a public key any more. Does he have to obtain new email address?

As a solution for this problem, Boneh and Franklin [8] suggested that one should attach a time period to a string which is to be used as a public key in IBE schemes. For example. Bob publishes `bob@crytworld.com||June,2004` as a public key. Then a private key associated with this identity will be valid only during June. However, this does not give a complete solution as the format of time periods needs to defined and should be informed to the senders. Also, if the time period should not be too short or too long, which makes security policy management complicated. Hence, a question here is: Is there any method other than Boneh and Franklin's to solve this escrow problem in identity-based cryptography?

Other Open Problems. Identity-based cryptographic schemes proposed so far in the literature can be categorized into two classes: "Pairing-based schemes" and "Factoring-based schemes". The latter mainly refers to the IBE scheme proposed by Cocks [15]. However, because of efficiency, the former "Pairing-based schemes" have been focused on by many cryptographers. Recently, cryptographic schemes that have somewhat different structures than the schemes in [8, 11, 16, 19] have been proposed by Zhang, Safavi-Naini, and Susilo [36], and Boneh and Boyen [7]. Even though these schemes still use the bilinear pairing, they turn out to be more efficient than previous schemes. (Note that although the techniques for speeding up the bilinear pairing computation have been developed by Barreto et al. [2, 11], the computational cost for the pairing computation is still expensive compared to a single or double exponentiation in the finite field.)

Yet, we do not know whether it is possible to construct especially IBE schemes which are not based on the pairing but are more efficient than Cocks' IBE scheme.

7 Concluding Remarks

In this paper, we survey the state of the art of identity-based cryptography. As discussed throughout the paper, there are pros and cons of using identity-based cryptography. From the authors' point of view, defining context of pieces of identifier information that will be used as public key in identity-based cryptography and management of them are important next steps that cryptographers and security engineers should elaborate on.

References

[1] G. Ateniese and B. Medeiros,*Identity-based Chameleon Hash and Applications*, Financial Cryptography – Proceedings of FC 2004, LNCS, Springer-Verlag, to appear.

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

[3] P. Barreto, B. Lynn, and M. Scott, *On the Selection of Pairing-Friendly Groups*, Selected Areas in Cryptography – SAC 2003, LNCS 3006, pages. 17–25, Springer-Verlag, 2004.

[4] J. Baek and Y. Zheng, *Identity-Based Threshold Decryption*, Public Key Cryptography – Proceedings of PKC 2004, LNCS 2947, pages 262-276, Springer-Verlag, 2004.

[5] M. Bellare and P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, Proceedings of the First ACM Conference on Computer and Communications Security 1993, pages 62–73.

[6] A. Boldyreva, *Efficient Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-group Signature Scheme*, Public Key Cryptography – Proceedings of PKC 2003, LNCS 2567, pages 31–46, Springer-Verlag 2003.

[7] D. Boneh and X. Boyen, *Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles*, Advances in Cryptology - Proceedings of EUROCRYPT 2004, LNCS 3027, pages 223–238, Springer-Verlag, 2004.

[8] D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Proceedings of CRYPTO 2001, LNCS 2139, pages 213–229, Springer-Verlag, 2001.

[9] http://crypto.stanford.edu/ibe/

[10] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, Advances in Cryptology - Proceedings of EUROCRYPT 2001, LNCS 2656, pages 416–432, Springer-Verlag, 2003.

[11] D. Boneh, B. Lynn, and H. Shacham, *Short Signatures from the Weil Pairing*, Advances in Cryptology - Proceedings of ASIACRYPT 2001, LNCS 2248, pages 566–582, Springer-Verlag, 2001.

[12] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, *Public Key Encryption with Keyword Search*, Advances in Cryptology - Proceedings of EUROCRYPT 2004, LNCS 3027, pages 506–522, Springer-Verlag, 2004.

[13] X. Boyen, *Multipurpose Identity-Based Signcryption: A Swiss Army Knife for Identity-Based Cryptography*, Advances in Cryptology - Proceedings of CRYPTO 2003, LNCS 2729, pages 382–398, Springer-Verlag, 2003.

[14] M. Casassa Mont, P. Bramhall, C. R. Dalton, and K. Harrison, *A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology in a Health Care Trial*, Hewlett-Packard Laboratories, technical report HPL-2003-21, 2003.

[15] C. Cocks, *An Identity Based Encryption Scheme Based on Quadratic Residues*, Cryptography and Coding - Institute of Mathematics and Its Applications International Conference on Cryptography and Coding – Proceedings of IMA 2001, LNCS 2260, pages 360–363, Springer-Verlag, 2001.

[16] J. Cha and J. Cheon, *An Identity-Based Signature from Diffie-Hellman Groups*, Public Key Cryptography – Proceedings of PKC 2003, LNCS 2567, pages 18–30, Springer-Verlag, 2003.

[17] L. Chen, K. Harrison, D. Soldera and N. P. Smart: *Applications of Multiple Trust Authorities in Pairing Based Cryptosysems*, Proceedings of InfraSec 2002, LNCS 2437, pages 260–275, Springer-Verlag, 2002.

[18] T. ElGamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Trans. Info. Theory, 31, 1985, pages 469–472.

[19] F. Hess, *Efficient Identity Based Signature Schemes Based on Pairings*, Selected Areas in Cryptography – Proceedings of SAC 2002, LNCS 2595, pages 310–324, Springer-Verlag, 2002.

[20] C. Gentry, *Certificate-Based Encryption and the Certificate Revocation Problem*, Proceedings of EUROCRYPT 2003, LNCS 2656, Springer-Verlag 2003, pages 272–293.

[21] C. Gentry and A. Silverberg, *Hierarchical ID-Based Cryptography*, Proceedings of ASIACRYPT 2002, LNCS 2501, Springer-Verlag 2002, pages 548–566.

[22] J. Horwitz and B. Lynn, *Toward Hierarchical Identity-Based Encryption*, Proceedings of EUROCRYPT 2002, LNCS 2332, Springer-Verlag 2002, pages 466–481.

[23] A. Joux, *One Round Protocol for Tripartite Diffie-Hellman*, Algorithmic Number Theory Symposium – Proceedings of ANTS 2002, LNCS 1838, pages 385–394, Springer-Verlag, 2000.

[24] B. Libert, J. Quisquater, *New identity based signcryption schemes based on pairings*, IEEE Information Theory Workshop, 2003. (See also Cryptology ePrint Archive, Report 2003/023).

[25] W. Mao, *Modern Cryptography: Theory & Practice*, Prentice Hall, 2004.

[26] J. Malone-Lee, *Identity-Based Signcryption*, IACR ePrint Archive, Report 2002/098. (http://eprint.iacr.org/).

[27] A. J. Menezes, T. Okamoto, and S. A. Vanstone: *Reducing Elliptic Curve Logarithms to a Finite Field*, IEEE Tran. on Info. Theory, Vol. 31, pages 1639–1646, IEEE, 1993.

[28] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21 (2), pages 120–126, 1978.

[29] A. Sahai and B. Waters *Fuzzy Identity Based Encryption*, IACR ePrint Archive, Report 2004/086. (http://eprint.iacr.org/).

[30] A. Shamir, *How to Share a Secret*, Communications of the ACM, Vol. 22, 1979, pages 612–613.

[31] A. Shamir, *Identity-based Cryptosystems and Signature Schemes*, Proceedings of CRYPTO '84, LNCS 196, pages 47–53, Springer-Verlag, 1984.

[32] http://indigo.ie/ mscott/

[33] N. P. Smart: *Access Control Using Pairing Based Cryptography*, Proceedings of Topics in Cryptology-CT-RSA 2003, LNCS 2612, Springer-Verlag 2003, pages 111–121.

[34] http://www.identicrypt.com/

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

[36] F. Zhang, R. Safavi-Naini, W. Susilo, *An Efficient Signature Scheme from Bilinear Pairings and Its Applications*, Public Key Cryptography – Proceedings of PKC 2004, LNCS 2947, pages. 262–276, Springer-Verlag, 2004.