CHAPTER X

Cryptography from Pairings

by K.G. Paterson

X.1. Introduction

This chapter presents a survey of positive applications of pairings in cryptography. We assume the reader has a basic understanding of concepts from cryptography such as public key encryption, digital signatures, and key exchange protocols. A solid grounding in the general area of cryptography can be obtained by reading [**218**].

We will attempt to show how pairings (as described in Chapter IX) have been used to construct a wide range of cryptographic schemes, protocols and infrastructures supporting the use of public key cryptography. Recent years have seen an explosion of interest in this topic, inspired mostly by three key contributions: Sakai, Ohgishi and Kasahara's early and much overlooked work introducing pairing-based key agreement and signature schemes [**260**]; Joux's three party key agreement protocol as presented in [**167**]; and Boneh and Franklin's identity-based encryption (IBE) scheme built from pairings [**36**]. The work of Verheul [**305**] has also been influential because it eases the cryptographic application of pairings. We will give detailed descriptions of these works as the chapter unfolds. To comprehend the rate of increase of research in this area, note that the bibliography of an earlier survey [**250**] written in mid-2002 contains 28 items, while, at the time of writing in early 2004, Barreto's website [**14**] lists over 100 research papers.[1]

Thus a survey such as this cannot hope to comprehensively cover all of the pairing-based cryptographic research that has been produced. Instead, we focus on presenting the small number of schemes that we consider to be the high points in the area and which are likely to have a significant impact on future research. We provide brief notes on most of the remaining literature, and omit some work entirely. We do not emphasise the technical details of security proofs, but we do choose to focus on schemes that are supported by such proofs.

[1] A second source for papers on cryptography from pairings is the IACR preprint server at `http://eprint.iacr.org`. Another survey on pairings and cryptography by Joux [**168**] covers roughly the same topics as this and the previous chapter.

X.1.1. Chapter Plan. In the next two sections, we introduce the work of Sakai *et al.* [**260**], Joux [**167**] and Boneh and Franklin [**36**]. Then in Section X.4, we consider various types of signature schemes derived from pairings. Section X.5 is concerned with further developments of the IBE scheme of [**36**] in the areas of hierarchical identity-based cryptography, intrusion-resilient cryptography and related topics. Section X.6 considers how the key agreement protocols of [**260, 167**] have been extended. In the penultimate section, Section X.7, we look more closely at identity-based cryptography and examine the impact that pairings have had on infrastructures supporting the use of public key cryptography. We also look at a variety of trials and implementations of pairing-based cryptography. We draw to a close with a look towards the future in Section X.8.

X.1.2. Pairings as Black Boxes. In this chapter, we will largely treat pairings as "black boxes", by which we mean that we will not be particularly interested in how the pairings can be selected, computed and so on. Rather we will treat them as abstract mappings on groups. Naturally, Chapter IX is the place to look for the details on these issues. The reason to do this is so that we can concentrate on the general cryptographic principles behind the schemes and systems we study, without being distracted by the implementation details. It does occasionally help to look more closely at the pairings, however. For one thing, the availability of easily computable pairings over suitably "compact" groups and curves is key to the utility of some of the pairing-based proposals that we study. And of course, the real-world security of any proposal will depend critically on the actual curves and pairings selected to implement that proposal. It would be inappropriate in a chapter on applications in cryptography to completely ignore these issues of efficiency and security. So we will "open the box" whenever necessary.

Let us do so now, in order to re-iterate some notation from the previous chapter and to establish some of the basics for this chapter. We recall the basic properties of a pairing $e : G_1 \times G_2 \to G_3$ from Section IX.1. In brief, e is a bilinear and non-degenerate map and will be derived from a Tate or Weil pairing on an elliptic curve $E(\mathbb{F}_q)$. In cryptographic applications of pairings, it is usually more convenient to work with a single subgroup G_1 of $E(\mathbb{F}_q)$ having prime order r and generator P as input to the pairing, instead of two groups G_1 and G_2. For this reason, many of the schemes and systems we study were originally proposed in the context of a "self-pairing" as described in Section IX.7. To ensure that the cryptographic schemes are not completely trivial, it is then important that $e(P, P) \neq 1$. The distortion maps of Verheul [**305**] are particularly helpful in ensuring that these conditions can be met for supersingular curves.

As in Section IX.7.3, we assume that $E(\mathbb{F}_q)$ is a supersingular elliptic curve with $r|\#E(\mathbb{F}_q)$ for some prime r. We write $k > 1$ for the embedding degree for E and r, and assume that $E(\mathbb{F}_{q^k})$ has no points of order r^2. As usual, we write $e(Q,R) = \langle Q,R\rangle_r^{(q^k-1)/r} \in \mathbb{F}_{q^k}$ for $Q \in E(\mathbb{F}_q)[r]$ and $R \in E(\mathbb{F}_{q^k})$. We then let φ denote a non-rational endomorphism of E (a distortion map). Suitable maps φ are defined in Table IX.1. We put $G_1 = \langle P\rangle$ where P is any non-zero point in $E(\mathbb{F}_q)[r]$ and $G_3 = \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$. We then write $\hat{e}$ for the map from $G_1 \times G_1$ to G_3 defined by:

$$\hat{e}(Q,R) = e(Q,\varphi(R)).$$

The function $\hat{e}$ is called a *modified* pairing. As a consequence of its derivation from the pairing e and distortion map φ, it has the following properties:

Bilinearity: For all $Q, Q', R, R' \in G_1$, we have

$$\hat{e}(Q+Q',R) = \hat{e}(Q,R)\cdot\hat{e}(Q',R)$$

and

$$\hat{e}(Q,R+R') = \hat{e}(Q,R)\cdot\hat{e}(Q,R').$$

Symmetry: For all $Q, R \in G_1$, we have

$$\hat{e}(Q,R) = \hat{e}(R,Q).$$

Non-degeneracy: We have

$$\hat{e}(P,P) \neq 1.$$

Hence we have: $\hat{e}(Q,P) \neq 1$ for all $Q \in G_1$, $Q \neq \mathcal{O}$ and $\hat{e}(P,R) \neq 1$ for all $R \in G_1$, $R \neq \mathcal{O}$.

Although our notation inherited from the previous chapter suggests that the map $\hat{e}$ must be derived from the Tate pairing, this need not be the case. The Weil pairing can also be used. However, as Chapter IX spells out, the Tate pairing is usually a better choice from an implementation perspective.

Relying on distortion maps in this way limits us to using supersingular curves. There may be good implementation or security reasons for working with curves other than these, again as Chapter IX makes clear. (In particular, special purpose algorithms [**2, 3, 82, 169**] can be applied to solve the discrete logarithm problem in $\mathbb{F}_{q^k}$ when E is one of the supersingular curves over a field of characteristic 2 or 3 in Table IX.1. This may mean that larger parameters than at first appears must be chosen to obtain required security levels.) Most of the cryptographic schemes that were originally defined in the self-pairing setting can be adapted to operate with ordinary curves and unmodified pairings, at the cost of some minor inconvenience (and sometimes a loss of bandwidth efficiency). We will encounter situations where ordinary curves are in fact to be preferred. Moreover, we will present some schemes using the language of self-pairings that were originally defined using unmodified pairings. We will note in the text where this is the case.

We can summarise the above digression into some of the technicalities of pairings as follows. By carefully selecting an elliptic curve $E(\mathbb{F}_q)$, we can obtain a symmetric, bilinear map $\hat{e} : G_1 \times G_1 \to G_3$ with the property that $\hat{e}(P,P) \neq 1$. Here, P of prime order r on $E(\mathbb{F}_q)$ generates G_1 and

G_3 is a subgroup of $\mathbb{F}_{q^k}$ for some small k. When parameters $\langle G_1, G_3, \hat{e}\rangle$ are appropriately selected, we also have the following properties:

Efficiency: The computation of $\hat{e}$ can be made relatively efficient (equivalent perhaps to a few point multiplications on $E(\mathbb{F}_q)$). Elements of G_1 and G_3 have relatively compact descriptions as bit-strings, and arithmetic in these groups can be efficiently implemented.

Security: The bilinear-Diffie–Hellman problem and the decision-bilinear-Diffie–Hellman problem are both computationally hard.[2]

X.2. Key Distribution Schemes

In this section, we review the work of Sakai *et al.* [**260**] and Joux [**167**] on key distribution schemes built from pairings. These papers paved the way for Boneh and Franklin's identity-based encryption scheme, the subject of Section X.3. Note that both papers considered only unmodified pairings. We have translated their schemes into the self-pairing setting in our presentation.

X.2.1. Identity-Based Non-Interactive Key Distribution. Key distribution is one of the most basic problems in cryptography. For example, frequently refreshed, random keys are needed for symmetric encryption algorithms and MACs to create confidential and integrity-protected channels. Consider the situation of two parties A and B who want to compute a shared key K_{AB} but cannot afford to engage in a Diffie–Hellman protocol (perhaps one of them is initially offline, or they cannot afford the communications overhead of an interactive protocol).

Sakai *et al.* [**260**] proposed a pairing-based solution to this problem of constructing a non-interactive key distribution scheme (NIKDS). An important and interesting feature of their solution is its identity-based nature. The notion of identity-based cryptography dates back to work of Shamir [**270**]. Shamir's vision was to do away with public keys and the clumsy certificates for those public keys, and instead build cryptographic schemes and protocols in which entities' public keys could be derived from their identities (or other identifying information) alone. In place of a Certification Authority (CA), Shamir envisaged a Trusted Authority (TA) who would be responsible for issuance of private keys and maintenance of system parameters. Whilst Shamir was able to construct an identity-based signature scheme in [**270**], and identity-based NIKDS followed from a variety of authors (see [**218**, p. 587]), the problem of constructing a truly practical and provably secure identity-based encryption scheme remained an open problem until the advent of pairing-based cryptography. As we shall see in Section X.3, the work of

[2]Note that these problems are defined in Section IX.11.3 for unmodified pairings. We will define the BDH problem for modified pairings below, after which the definition of the DBDH problem should be obvious.

Sakai *et al.* [**260**] can be regarded as being pivotal in Boneh and Franklin's solution of this problem.

Sakai *et al.* make use of a TA who chooses and makes public the *system parameters* of the form $\langle G_1, G_3, \hat{e}\rangle$ (with properties as in Section X.1.2) along with a cryptographic hash function

$$H_1 : \{0,1\}^* \to G_1$$

mapping binary strings of arbitrary length onto elements of G_1. We briefly indicate in Section X.3.1 below how such a hash function can be constructed. The TA also selects but keeps secret a master secret $s \in \mathbb{Z}_r^*$. The TA interacts with A and B, providing each of them with a private key over a confidential and authenticated channel. These private keys depend on s and the individuals' identities: the TA computes as A's secret the value $S_A = [s]Q_A$ where $Q_A = H_1(\mathtt{ID}_A) \in G_1$ is a publicly computable function of A's identity. Likewise, the TA gives B the value $S_B = [s]Q_B$ where $Q_B = H_1(\mathtt{ID}_B)$. Because of its role in distributing private keys, the TA is also known as a Private Key Generator (PKG) in these kinds of applications.

Now, with this keying infrastructure in place, consider the equalities:

$$\hat{e}(S_A, Q_B) = \hat{e}([s]Q_A, Q_B) = \hat{e}(Q_A, Q_B)^s = \hat{e}(Q_A, [s]Q_B) = \hat{e}(Q_A, S_B)$$

where we have made use of the bilinearity of $\hat{e}$. On the one hand, A has the secret S_A and can compute $Q_B = H_1(\mathtt{ID}_B)$ using the public hash function H_1. On the other hand, B can compute Q_A and has the secret S_B. Thus both parties can compute the value $K_{AB} = \hat{e}(Q_A, Q_B)^s$, and provided they know each others' identifying information, can do so without any interaction at all. A key suitable for use in cryptographic applications can be derived from K_{AB} by appropriate use of a key derivation function.

A closely related version of this procedure was rediscovered somewhat later by Dupont and Enge [**101**]. Their scheme works in the unmodified setting and requires that each entity receive two private key components (one in each group G_1 and G_2). The security proof in [**101**] is easily adapted to the self-pairing setting. The adapted proof models the hash function H_1 as a random oracle and allows the adversary the power to obtain the private keys of arbitrary entities (except, of course, the keys of entities A and B).

The proof shows that the above procedure generates a key $\hat{e}(Q_A, Q_B)$ which cannot be computed by an adversary, provided that the (modified) bilinear-Diffie–Hellman problem (BDH problem) is hard. This problem can be stated informally as follows (c.f. the definition in Section IX.11.3):

Bilinear-Diffie–Hellman problem (BDH problem): given P, $P_1 = [a]P$, $P_2 = [b]P$ and $P_3 = [c]P$ in G_1 with a, b and c selected uniformly at random from $\mathbb{Z}_r^*$, compute

$$\hat{e}(P, P)^{abc}.$$

One implication of the security proof is that the scheme is *collusion resistant*: no coalition of entities excluding A and B can join together and compromise the key K_{AB}. Notice, however, that the TA can generate A and B's common key for itself – the scheme enjoys (or suffers from, depending on one's point of view and the application in mind) key escrow. For this reason, A and B must trust the TA not to eavesdrop on communications encrypted by this key, and not to disclose the key to other parties. In particular, they must trust the TA to adequately check claimants' identities before issuing them with private keys.

For the purpose of comparison, consider the following alternative traditional (i.e. certificate-based) means of realizing a NIKDS. A CA publishes system parameters $\langle E(\mathbb{F}_q), P\rangle$ where P on E is of prime order r. A chooses a private value a, calculates the public value $q_A = [a]P$ and obtains a certificate on $\mathtt{ID}_A$ and q_A from a Certification Authority (CA). Entity B does the same with his value b. Now A can compute a common key as follows: A fetches B's certificate and verifies that it is valid by checking the CA's signature. Now A can combine his secret a with B's value $[b]P$ to obtain $[ab]P$. This value constitutes the common key. Here, A and B have simply engaged in a non-interactive version of the ECDH protocol. The complexity with this approach comes from the need for A to obtain B's certificate, verify its correctness and check its revocation status, and vice versa. These checks require the use of a public key infrastructure (PKI). In contrast, with the identity-based scheme of [**260**], all A needs is B's identity string $\mathtt{ID}_B$ and the public parameters of the TA.[3] This could be B's e-mail or IP address, or any other string which identifies B uniquely within the context of the system. The trust in public values does not come from certificates, but is rather produced implicitly through A's trust in the TA's private key issuance procedures.

At this point, the reader would be justified in asking: why do A and B simply not use the key K_{AB} as the basis for deriving an encryption key? Moreover, if they do, why does the combination of Sakai *et al.*'s identity-based NIKDS with this encryption not constitute an identity-based encryption scheme? There are two parts to the answer to this latter question. First of all, the key they agree is *static*, whereas a dynamic message key would be preferable. Secondly, and more importantly, both A and B must have registered ahead of time and have received their private keys before they can communicate in this way. A true public key encryption scheme would not require the *encrypting* party to register and obtain such a key.

X.2.2. Three Party Key Distribution. Around the same time that Sakai *et al.* proposed their two-party NIKDS, Joux [**167**] put forward a three party

[3]The revocation issue for the identity-based approach also requires careful consideration. We shall return to this topic in Section X.7, where we take a closer look at identity-based systems.

key agreement protocol with the novel feature that only one (broadcast) message per participant is required to achieve key agreement. Thus only one round of communication is needed to establish a shared key. This contrasts sharply with the two rounds that are needed if a naive extension of the (Elliptic Curve) Diffie–Hellman protocol is used. We sketch Joux's protocol. First of all, it is assumed that the three parties have agreed in advance on system parameters $\langle G_1, G_3, \hat{e}, P\rangle$. Then entity A selects $a \in \mathbb{Z}_r^*$ uniformly at random and broadcasts ephemeral value $[a]P$ to entities B and C. Entity B (respectively C) selects b (resp. c) in the same way and broadcasts $[b]P$ (resp. $[c]P$) to the other entities. Now by bilinearity we have:

$$\hat{e}([b]P, [c]P)^a = \hat{e}([a]P, [c]P)^b = \hat{e}([a]P, [b]P)^c$$

so that each party, using its private value and the two public values, can calculate the common value

$$K_{ABC} = \hat{e}(P, P)^{abc} \in G_3.$$

This value can be used as keying material to derive session keys. On the other hand, an adversary who only sees the broadcast messages $[a]P$, $[b]P$, $[c]P$ is left with an instance of the BDH problem to solve in order to calculate K_{ABC}. This last statement can be formalised to construct a security proof relating the security of this protocol against *passive* adversaries to the hardness of the (modified) BDH problem. The protocol is vulnerable to an extension of the classic man-in-the-middle attack conducted by an active adversary. We will return to this issue in Section X.6 below.

Note the importance of the fact that $\hat{e}(P, P) \neq 1$ here. Without this condition, K_{ABC} could trivially equal $1 \in G_3$. Joux's protocol was originally stated in the context of an unmodified pairing and required each participant to broadcast a pair of independent points of the form $[a]P, [a]Q$ in order to avoid degeneracy in the pairing computation. Using modified pairings limits the range of curves for which the protocol can be realised but decreases its bandwidth requirements. This point was first observed by Verheul [**305**].

X.3. Identity-Based Encryption

As we have discussed above, the construction of a workable and provably secure identity-based encryption (IBE) scheme was, until recently, an open problem dating back to Shamir's 1984 paper [**270**]. Two solutions appeared in rapid succession in early 2001 – the pairing-based approach of Boneh and Franklin [**36**] (appearing in an extended version as [**37**]) and Cocks' scheme based on the Quadratic Residuosity problem [**79**]. It has since become apparent that Cocks' scheme was discovered some years earlier but remained unpublished until 2001, when the circulation of Boneh and Franklin's scheme prompted its disclosure.[4] We do not discuss Cocks' scheme any further here, but recommend that the interested reader consult [**79**] for the details.

X.3.1. The Basic Scheme of Boneh and Franklin. We first discuss the scheme `BasicIdent` of [**37**]. This basic IBE scheme is useful as a teaching tool, but is not suited for practical use (because its security guarantees are too weak for most applications). We will study the full scheme `FullIdent` of [**37**] in Section X.3.3. The IBE scheme `BasicIdent` makes use of essentially the same keying infrastructure as was introduced above in describing the NIKDS of Sakai *et al.*. The TA (or PKG) publishes system parameters $\langle G_1, G_3, \hat{e}\rangle$. In addition, the PKG publishes a generator P for G_1, together with the point $Q_0 = [s]P$, where, as before, $s \in \mathbb{Z}_r^*$ is a master secret. Note that Q_0 is denoted by P_{pub} in [**37**]. Descriptions of cryptographic hash functions

$$H_1 : \{0,1\}^* \rightarrow G_1, \quad H_2 : G_3 \rightarrow \{0,1\}^n$$

are also made public. Here, n will be the bit-length of plaintext messages. So the complete set of system parameters is:

$$\langle G_1, G_3, \hat{e}, P, Q_0, n, H_1, H_2\rangle.$$

As in the scheme of [**260**], each entity A must be given a copy of its private key $S_A = [s]Q_A = [s]H_1(\mathtt{ID}_A)$ over a secure channel.

With this set of parameters and keys in place, `BasicIdent` encryption proceeds as follows. To encrypt an n-bit plaintext M for entity A with identity $\mathtt{ID}_A$, entity B computes $Q_A = H_1(\mathtt{ID}_A)$, selects $t \in \mathbb{Z}_r^*$ uniformly at random and computes the ciphertext as:

$$C = \langle [t]P, M \oplus H_2(\hat{e}(Q_A, Q_0)^t)\rangle \in G_1 \times \{0,1\}^n.$$

To decrypt a received ciphertext $C = \langle U, V\rangle$ in the scheme `BasicIdent`, entity A computes

$$M' = V \oplus H_2(\hat{e}(S_A, U))$$

using its private key $S_A = [s]Q_A$.

To see that encryption and decryption are inverse operations, note that (by bilinearity)

$$\hat{e}(Q_A, Q_0)^t = \hat{e}(Q_A, P)^{st} = \hat{e}([s]Q_A, [t]P) = \hat{e}(S_A, U).$$

On the one hand, the encryption mask $H_2(\hat{e}(Q_A, Q_0)^t)$ that is computed by entity B is the same as that computed by A, namely $H_2(\hat{e}([s]Q_A, U))$. On the other hand, the computation of the encryption mask by an eavesdropper (informally) requires the computation of $\hat{e}(Q_A, Q_0)^t$ from the values P, Q_A, Q_0 and $U = [t]P$. This task is clearly related to solving the (modified) BDH problem.

[4]Very recently, it has come to our attention that Sakai, Ohgishi and Kasahara proposed an IBE scheme using pairings in May 2000. Their paper was published in Japanese in the proceedings of the 2001 Symposium on Cryptography and Information Security, January 2001; an English version is available from the authors.

Notice that encryption and decryption each require one pairing computation, but that the cost of this can be spread over many encryptions if the encrypting party repeatedly sends messages to the same entity. A small number of other operations are also needed by each entity (dominated by hashing and exponentiation in G_1 and G_3). Ciphertexts are relatively compact: they are equal in size to the plaintext plus the number of bits needed to represent an element of G_1.

The definition of the hash function H_1 mapping arbitrary strings onto elements of G_1 requires care; a detailed exposition is beyond the scope of this survey. The reader is referred to [**37**, Sections 4.3 and 5.2] for the details of one approach that works for a particular class of curves and to [**40**, Section 3.3] for a less elegant method which works for general curves.

X.3.2. Relationship to Earlier Work. It is instructive to examine how this basic identity-based encryption scheme relates to earlier work. There are (at least) two different ways to do so.

Writing $Q_A = [a]P$ for some $a \in \mathbb{Z}_r^*$, we see that the value $\hat{e}(Q_A, Q_0)^t$ appearing in `BasicIdent` is equal to $\hat{e}(P, P)^{ast}$. Thus it is formally equal to the shared value that would be agreed in an instance of Joux's protocol in which the ephemeral values "broadcast" by the entities were $Q_A = [a]P$, $Q_0 = [s]P$ and $U = [t]P$. In the encryption scheme, only U is actually transmitted; the other values are static in the scheme and made available to B through the system parameters and hashing of A's identity. One can think of $Q_0 = [s]P$ as being the ephemeral value from a "dummy" entity here. Entity A gets the value U from B and is given the ability to compute $\hat{e}(P, P)^{ast}$ when the PKG gives it the value $[s]Q_A = [sa]P$. Thus Boneh and Franklin's IBE scheme can be regarded as a rather strange instance of Joux's protocol.

Perhaps a more profitable way to understand the scheme is to compare it to ElGamal encryption . In a variant of textbook ElGamal, an entity A has a private key $x_A \in \mathbb{Z}_r^*$ and a public key $y_A = g^{x_A}$. To encrypt a message for A, entity B selects $t \in \mathbb{Z}_r^*$ uniformly at random and computes the ciphertext as:

$$C = \langle g^t, M \oplus H_2({y_A}^t) \rangle$$

while to decrypt $C = \langle U, V \rangle$, entity A computes

$$M' = V \oplus H_2(U^{x_A}).$$

Thus one can regard the basic IBE scheme of Boneh and Franklin as being an adaptation of ElGamal encryption in which $\hat{e}(Q_A, Q_0)$, computed from system parameters and A's identity, replaces the public key y_A.

We have already noted the similarities in keying infrastructures used by Boneh and Franklin's IBE scheme and in the NIKDS of Sakai *et al.* [**260**]. The above discussion shows a relationship between Boneh and Franklin's IBE scheme and Joux's protocol [**167**]. However, it would be wrong to leave the impression that Boneh and Franklin's scheme is just a simple development of ideas in these earlier papers. Prior to Boneh and Franklin's work, Joux's protocol was merely an interesting curiosity, and the work of [**260**] almost unknown to the wider community. It was Boneh and Franklin's work that quickly led to a wider realization that pairings could be a very useful constructive cryptographic tool and the spate of research that followed.

X.3.3. Security of Identity-Based Encryption. Boneh and Franklin provide in [**37**] a variant of `BasicIdent` named `FullIdent` which offers stronger security guarantees. In particular, the security of `FullIdent` can be related to the hardness of the BDH problem in a model that naturally extends the widely-accepted IND-CCA2 model for public key encryption (see Definition III.4) to the identity-based setting. We present the scheme `FullIdent` below, outline the security model introduced in [**37**] and then discuss the security of `FullIdent` in this model.

In general, an IBE scheme can be defined by four algorithms, with functions as suggested by their names: `Setup`, `(Private Key) Extract`, `Encrypt` and `Decrypt`. For the scheme `FullIdent`, these operate as follows:

`Setup:` This algorithm takes as input a security parameter ℓ and outputs the system parameters:

$$\texttt{params} = \langle G_1, G_3, \hat{e}, n, P, Q_0, H_1, H_2, H_3, H_4 \rangle.$$

Here G_1, G_3 and $\hat{e}$ are the usual objects[5], n is the bit-length of plaintexts, P generates G_1 and $Q_0 = [s]P$ where s is the scheme's master secret. Hash functions H_1 and H_2 are as above, while $H_3 : \{0,1\}^{2n} \to \mathbb{Z}_r^*$ and $H_4 : \{0,1\}^n \to \{0,1\}^n$ are additional hash functions. In principle, all of these parameters may depend on ℓ.

`Extract:` This algorithm takes as input an identity string `ID` and returns the corresponding private key $[s]H_1(\texttt{ID})$.

`Encrypt:` To encrypt the plaintext $M \in \{0,1\}^n$ for entity A with identity $\texttt{ID}_A$, perform the following steps:

1. Compute $Q_A = H_1(\texttt{ID}_A) \in G_1$.
2. Choose a random $\sigma \in \{0,1\}^n$.
3. Set $t = H_3(\sigma, M)$.
4. Compute and output the ciphertext:

$$C = \langle [t]P, \sigma \oplus H_2(\hat{e}(Q_A, Q_0)^t), M \oplus H_4(\sigma) \rangle \in G_1 \times \{0,1\}^{2n}.$$

`Decrypt:` Suppose $C = \langle U, V, W \rangle \in G_1 \times \{0,1\}^{2n}$ is a ciphertext encrypted for A. To decrypt C using the private key $[s]Q_A$:

1. Compute $\sigma' := V \oplus H_2(\hat{e}([s]Q_A, U))$.

[5]Boneh and Franklin make use of a subsidiary instance generating algorithm $\mathcal{IG}$ to produce the parameters $\langle G_1, G_3, \hat{e} \rangle$ (possibly probabilistically) from input ℓ, the security parameter.

2. Compute $M' := W \oplus H_4(\sigma')$.
3. Set $t' = H_3(\sigma', M')$ and test if $U = [t']P$. If not, reject the ciphertext.
4. Otherwise, output M' as the decryption of C.

The reader should compare `FullIdent` with the basic scheme above. When C is a valid encryption of M, it is quite easy to see that decrypting C will result in an output $M' = M$. The value $H_2(e(Q_A, Q_0)^t)$ is still used as an encryption mask, but now it encrypts a string σ rather than the plaintext itself. The string σ is subsequently used to form an encryption key $H_4(\sigma)$ to mask the plaintext. The encryption process also now derives t by hashing rather than by random choice; this provides the decryption algorithm with a checking facility to reject ciphertexts that are not of the correct form.

In fact, the scheme `FullIdent` is obtained from the basic scheme of the previous section by applying the Fujisaki-Okamoto hybridization technique [**119**]. It is this technique that ensures `FullIdent` meets the strong security definition in the model developed by Boneh and Franklin in [**37**]. In that model, an adversary $\mathcal{A}$ plays against a challenger $\mathcal{C}$ in the following game:

IND-ID-CCA Security Game: The game runs in five steps:

Setup: $\mathcal{C}$ runs algorithm `Setup` on input some value ℓ, gives $\mathcal{A}$ the system parameters `params` and keeps the master secret s to itself.

Phase 1: $\mathcal{A}$ issues a series of queries, each of which is either an `Extract` query on an identity, in which case $\mathcal{C}$ responds with the appropriate private key, or a `Decrypt` query on an identity/ciphertext combination, in which case $\mathcal{C}$ responds with an appropriate plaintext (or possibly a fail message).

Challenge: Once $\mathcal{A}$ decides to end Phase 1, it selects two plaintexts M_0, M_1 and an identity $\texttt{ID}_{\text{ch}}$ on which it wishes to be challenged. We insist that $\texttt{ID}_{\text{ch}}$ not be the subject of an earlier `Extract` query. Challenger $\mathcal{C}$ then chooses b at random from $\{0, 1\}$ and runs algorithm `Encrypt` on M_b and $\texttt{ID}_{\text{ch}}$ to obtain the challenge ciphertext C^*; $\mathcal{C}$ then gives C^* to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ issues another series of queries as in Phase 1, with the restriction that no `Extract` query be on $\texttt{ID}_{\text{ch}}$ and that no `Decrypt` query be on the combination $\langle \texttt{ID}_{\text{ch}}, C^* \rangle$. $\mathcal{C}$ responds to these as before.

Guess: Finally, $\mathcal{A}$ outputs a guess b' and wins the game if $b' = b$.

Adversary $\mathcal{A}$'s advantage is defined to be $\text{Adv}(\mathcal{A}) := 2|\Pr[b' = b] - \frac{1}{2}|$, where the probability is measured over any random bits used by $\mathcal{C}$ (for example, in the `Setup` algorithm) and $\mathcal{A}$ (for example, in choosing ciphertexts and identities to attack). An IBE scheme is said to be semantically secure against adaptive chosen ciphertext attack (IND-ID-CCA secure) if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the above game. Here, non-negligiblity is defined in terms of the security parameter ℓ

used in the Setup algorithm.[6] This model and definition of security extends the by-now-standard IND-CCA2 notion of security for public key encryption: it allows the adversary to access private keys of arbitrary entities (except the challenge identity, of course) as well as giving the adversary access to a decryption oracle. It also allows the adversary to choose the public key on which it is to be challenged and automatically captures attacks involving colluding entities.

It is proved in [**37**] that the scheme FullIdent is IND-ID-CCA secure in the Random Oracle model, provided that there is no polynomially bounded algorithm having a non-negligible advantage in solving the BDH problem. Here, parameters $\langle G_1, G_2, \hat{e}\rangle$ for the BDH problem are assumed to be generated with the same distribution as by the Setup algorithm of FullIdent.

The proof of security for FullIdent proceeds in several stages. First it is shown, via a fairly standard simulation argument, that an adversary who can break FullIdent (in the sense of winning the IND-ID-CCA security game) can be used to produce an adversary that breaks a related standard public key encryption scheme in an IND-CCA2 game. Then results of [**119**] are invoked to relate the IND-CCA2 security of the public key scheme to the security of a simpler public key encryption scheme BasicPub, but in a much weaker attack model (one without decryption queries). Finally, it can be shown directly that an adversary breaking BasicPub can be used to construct an algorithm to solve instances of the BDH problem. For details of these steps, see [**37**, Lemma 4.3, Lemma 4.6 and Theorem 4.5].[7] The security analysis in [**37**] depends in a crucial way on the replacement of hash functions H_1, H_2, H_3 and H_4 by random oracles. At the time of writing, it is still an open problem to produce an IBE scheme that is provably secure in Boneh and Franklin's security model, but without modelling any hash functions as random oracles. The composition of a sequence of security reductions also yields a fairly loose relationship between the security of FullIdent and the hardness of the BDH problem. Tightening this relationship seems to be a difficult challenge.

This concludes our description of the identity-based encryption scheme of Boneh and Franklin [**37**]. The paper [**37**] contains much else of interest besides, and we recommend it be read in detail by every reader who has more than a passing interest in the subject.

X.3.4. Further Encryption Schemes. In [**305**], Verheul showed how pairings can be used to build a scheme supporting both non-repudiable signatures and escrowable public key encryption using only a single public key.

[6] A function f of ℓ is said to be *negligible* if, for any polynomial $p(\ell)$, there exists ℓ_0 such that, for all $\ell > \ell_0$, $f(\ell) < 1/p(\ell)$. Naturally, a function is said to be *non-negligible* if it is not negligible.

[7] But note that the proof of Lemma 4.6 in [**37**] requires a small repair: when $coin_i = 1$, the values b_i should be set to equal 1, so that the ciphertexts C_i' do not always fail the consistency check in the decryption algorithm of $\mathtt{BasicPub}^{hy}$.

The main idea of Verheul's scheme is as follows. As usual, we have system parameters $\langle G_1, G_3, \hat{e}\rangle$ with G_1 of prime order r generated by point P. An entity A chooses as its private signing key $x_A \in \mathbb{Z}_r^*$; the corresponding public key used for both encryption and signatures is $y_A = \hat{e}(P,P)^{x_A} \in G_3$. A CA then issues A with a certificate on the value y_A (the scheme is not identity-based). Any discrete logarithm based digital signature algorithm employing the values $g = \hat{e}(P,P)$, x_A and $y_A = g^{x_A}$ can be used. To encrypt a message $M \in \{0,1\}^n$ for A, the sender generates a random $t \in \mathbb{Z}_r^*$ and computes the ciphertext:

$$C = \langle [t]P, M \oplus H_2((y_A)^t)\rangle.$$

Here, as before, $H_2 : G_3 \to \{0,1\}^n$ is a cryptographic hash function. To decrypt $C = \langle U, V\rangle$, entity A computes

$$M' = V \oplus H_2(\hat{e}(P,U)^{x_A}).$$

Notice the similarity of this encryption scheme to that in Section X.3.2. The escrow service is supported as follows. Ahead of time, A sends to the escrow agent the value $Y_A = [x_A]P$. The escrow agent can then calculate the value $\hat{e}(P,U)^{x_A}$ for itself using its knowledge of Y_A and bilinearity:

$$\hat{e}(Y_A, U) = \hat{e}([x_A]P, U) = \hat{e}(P,U)^{x_A}.$$

Note that A does not give up its private signing key x_A to the escrow agent. Thus A's signatures remain non-repudiable. Verheul's scheme currently lacks a formal security proof. Such a proof would show that the same public key can safely be used for both signature and encryption.

Verheul's scheme may be described as providing a non-global escrow: entity A must choose to send the value Y_A to the escrow agent in order that the agent may recover plaintexts. Boneh and Franklin in [**37**, Section 7] gave yet another variant of pairing-based ElGamal encryption that provides escrow yet does not require interaction between escrow agent and users. For this reason, they described their scheme as providing global escrow. Their scheme works as follows. The system parameters, chosen by the escrow agent are $\langle G_1, G_3, \hat{e}, P, Q_0, n, H_2\rangle$. These are all defined as for the basic IBE scheme in Section X.3.1. In particular, $Q_0 = [s]P$ where s is a master secret. An entity A's key-pair is of the form $\langle x_A, Y_A = [x_A]P\rangle$. Thus A's public key is identical to the escrowed key in Verheul's scheme, and A's private key is the same in the two schemes. Now to encrypt $M \in \{0,1\}^n$ for A, the sender generates a random $t \in \mathbb{Z}_r^*$ and computes the ciphertext:

$$C = \langle [t]P, M \oplus H_2(\hat{e}(Y_A, Q_0)^t)\rangle.$$

To decrypt $C = \langle U, V\rangle$, entity A computes

$$M' = V \oplus H_2(\hat{e}([x_A]Q_0, U))$$

while the escrow agent computes

$$M' = V \oplus H_2(\hat{e}([s]Y_A, U)).$$

It is straightforward to see that (by bilinearity) both decryption algorithms produce the plaintext M. It is claimed in [**37**] that the security of this scheme rests on the hardness of the BDH problem. To see informally why this is so, note that to decrypt, an adversary must compute the value $\hat{e}(P, P)^{stx_A}$ given the values $Q_0 = [s]P$, $U = [t]P$ and $Y_A = [x_A]P$.

Lynn [**207**] has shown how to combine ideas from the IBE scheme of [**37**] and the NIKDS of [**260**] to produce an *authenticated identity-based encryption scheme*. In this scheme, a recipient A can check which entity sent any particular ciphertext. Simplifying slightly, this ability is provided by using the NIKDS key $\hat{e}(Q_A, Q_B)^s$ in place of the value $\hat{e}(Q_A, Q_0)^r$ in the Boneh-Franklin IBE scheme. This approach cannot yield a non-repudiation service, since A itself could have prepared any authenticated ciphertext purported to be from B.

We will report on the hierarchical identity-based encryption scheme of Gentry and Silverberg [**135**] and related work in Section X.5.

X.4. Signature Schemes

In this section, we outline how pairings have been used to build signature schemes of various kinds. Our coverage includes identity-based signature and signcryption schemes, standard (i.e. not identity-based) signature schemes and a variety of special-purpose signature schemes.

X.4.1. Identity-based Signature Schemes. Not long after the appearance of Boneh and Franklin's IBE scheme, a rash of identity-based signature (IBS) schemes appeared [**58, 148, 149, 249**]. Sakai *et al.*'s paper [**260**] also contains an IBS; another IBS scheme appears in [**319**]. Since IBS schemes have been known since Shamir's original work on identity-based cryptography in [**270**], the main reason to be interested in these new schemes is that they can make use of the same keying infrastructure as the IBE scheme of [**37**]. Being identity-based, and hence having built in escrow of private keys, none of the schemes can offer a true non-repudiation service. The schemes offer a variety of trade-offs in terms of their computational requirements on signer and verifier, and signature sizes. The scheme of [**58**] enjoys a security proof in a model that extends the standard adaptive chosen message attack model for (normal) signature schemes of [**137**] to the identity-based setting. The proof is in the random oracle model and relates the scheme's security to the hardness of the computational Diffie–Hellman problem (CDH problem) in G_1 using the Forking Lemma methodology [**253**]. The first IBS scheme of [**148**] also has a security proof; the second scheme in [**148**] was broken in [**71**].

To give a flavour of how these various IBS schemes operate, we present a version of the scheme of Cha and Cheon [**58**] here. An IBS scheme is defined by four algorithms: `Setup`, `Extract`, `Sign` and `Verify`. For the scheme of [**58**], these operate as follows:

`Setup:` This algorithm takes as input a security parameter ℓ and outputs the system parameters:

$$\mathtt{params} = \langle G_1, G_3, \hat{e}, P, Q_0, H_1, H_2 \rangle.$$

Here G_1, G_3, $\hat{e}$, P and $Q_0 = [s]P$ are as usual; s is the scheme's master secret. The hash function $H_1 : \{0,1\}^* \to G_1$ is as in Boneh and Franklin's IBE scheme, while $H_2 : \{0,1\}^* \times G_1 \to \mathbb{Z}_r$ is a second hash function.

`Extract:` This algorithm takes as input an identity `ID` and returns the corresponding private key $S_{\mathtt{ID}} = [s]H_1(\mathtt{ID})$. Notice that this key is identical to the private key in the IBE scheme of Boneh and Franklin [**37**].[8]

`Sign:` To sign a message $M \in \{0,1\}^*$, entity A with identity $\mathtt{ID}_A$ and private key $S_A = [s]H_1(\mathtt{ID}_A)$ chooses a random $t \in \mathbb{Z}_r$ and outputs a signature $\sigma = \langle U, V \rangle$ where $U = [t]H_1(\mathtt{ID}_A)$, $h = H_2(M, U)$ and $V = [t+h]S_A$.

`Verify:` To verify a signature $\sigma = \langle U, V \rangle$ on a message M for identity $\mathtt{ID}_A$, an entity simply checks whether the equation

$$\hat{e}(Q_0, U + hQ_A) = \hat{e}(P, V)$$

holds.

It is a simple exercise to show that the above IBS scheme is sound (signatures created using `Sign` will verify correctly using `Verify`).

The IBS scheme of [**58**] was originally presented in the context of any gap Diffie–Hellman group. Informally speaking, these are groups in which the CDH problem is hard but the DDH problem is easy, a notion first formalised in [**240**] and further explored in [**170**]. The signature generation algorithm uses the private key D_A to create Diffie–Hellman tuples, while the signature verification algorithm amounts to deciding whether $\langle P, Q_0, U + hQ_A, V \rangle$ is a valid Diffie–Hellman tuple. Since all the realizations of such gap groups currently known use pairings on elliptic curves, we have preferred a presentation using pairings.

X.4.2. Short Signatures. In [**40, 41**], Boneh, Lynn and Shacham used pairings to construct a (normal) signature scheme in which the signatures are rather short: for example, one version of their scheme has signatures that are approximately 170 bits in length whilst offering security comparable to that of 320-bit DSA signatures.

A simplified version of this BLS scheme can be described using modified pairings though (for reasons which will be discussed below) this does not lead to the preferred instantiation. This is essentially the approach taken in [**40**]. We will begin with this approach for ease of presentation.

[8] It is generally good cryptographic practice to use different keys for different functions. If this is required here, then a separate master secret could be used for the IBS scheme, or the identity string `ID` could be replaced by the string `ID`||"Sig" where "||" denotes concatenation of strings.

As usual, we work with system parameters $\langle G_1, G_3, \hat{e}\rangle$ and assume P of prime order r generates G_1. We also need a hash function $H : \{0,1\}^* \to G_1$. A user's private key is a value x selected at random from $\mathbb{Z}_r$, and the matching public key is $[x]P \in G_1$. The signature on a message $M \in \{0,1\}^*$ is simply $\sigma = [x]H(M) \in G_1$. To verify a purported signature σ on message M, the verifier checks that the 4-tuple:

$$\langle P, [x]P, H(M), \sigma\rangle$$

is a Diffie–Hellman tuple. This can be done by checking that the equation:

$$\hat{e}(\sigma, P) = \hat{e}(H(M), [x]P)$$

holds.

As with the IBS scheme of [**58**], this signature scheme exploits the fact that the signer can create Diffie–Hellman tuples in G_1 using knowledge of the private key x, while the verifier can check signatures using the fact that the DDH problem is easy in G_1, thanks to the presence of the pairing $\hat{e}$. The scheme is very closely related to the undeniable signature scheme of Chaum and van Antwerpen [**62, 63**]. That scheme has an identical signing procedure (except for a change of notation), but the confirmation (or denial of a signature) is via a zero-knowledge protocol in which the signer proves (or disproves) that the tuple is a Diffie–Hellman tuple. One can view the scheme of [**40**] as being the result of replacing the confirmation and denial protocols by a pairing computation. This makes the signatures verifiable without the aid of the signer, thus converting the undeniable signature scheme into a standard one. Of course, the BLS construction works more generally in the setting of gap Diffie–Hellman groups; the observation that signature schemes could be constructed from gap problems was made in [**240**, Section 4.1], though without a specific (standard) scheme being presented. The scheme of [**40**] can also be viewed in another way. As is noted in [**37**], Naor has pointed out that any IBE scheme can be used to construct a signature scheme as follows: the private signing key is the master key for the IBE scheme, the public verification key is the set of public parameters of the IBE scheme, and the signature on a message M is simply the private key for "identity" M in the IBE scheme. To verify a signature, the verifier can encrypt a random string and check that the signature (viewed as a decryption key) properly decrypts the result. In the special case of the IBE scheme of Boneh and Franklin, the signature for message M would be the IBE private key $[s]H_1(M)$. This is simply a BLS signature on M. The BLS scheme replaces the trial encryption/decryption with a more efficient procedure, but it is otherwise the signature scheme that can be derived from the Boneh-Franklin IBE scheme using Naor's construction.

It is not difficult to show that the BLS signature scheme is secure (in the usual chosen message attack model of [**137**], and regarding H as a random oracle) provided the CDH problem is hard in G_1.

A signature in this scheme consists of a single element of G_1 (as does the public key). Thus short signatures will result whenever G_1 can be arranged to have a compact representation. Using point compression, elements of G_1 can be represented using roughly $\lceil \log_2 q \rceil$ bits if G_1 is a subgroup of $E(\mathbb{F}_q)$.[9] So in order to obtain signatures that are as short as possible, it is desirable to make q as small as possible whilst keeping the ECDHP in G_1 (a subgroup of $E(\mathbb{F}_q)$) hard enough to make the scheme secure. However, one must bear in mind that, because of the presence of the pairing $\hat{e}$, the ECDLP in $E(\mathbb{F}_q)$ can be translated via the MOV reduction into the DLP in $\mathbb{F}_{q^k}$, where k is the embedding degree of $E(\mathbb{F}_q)$. Thus the security of the scheme not only rests on the difficulty of solving the ECDHP in $E(\mathbb{F}_q)$, but also on the hardness of the DLP in $\mathbb{F}_{q^k}$.

At first sight, it seems that Table IX.1 gives a pair of characteristic 3 supersingular curves E_1, E_2 which are fit for purpose.[10] When ℓ is odd, the curves have embedding degree 6, so the MOV reduction translates the ECDLP on $E_i(\mathbb{F}_{3^\ell})$ into the DLP in $\mathbb{F}_{3^{6\ell}}$, a relatively large finite field. Thus it should be possible to select a moderate sized ℓ and obtain short, secure signatures. For example, according to [**41**, Table 2], taking $\ell = 121$, one can obtain a signature size of 192 bits for a group G_1 of size about 2^{155}, while the MOV reduction yields a DLP in $\mathbb{F}_{3^{726}}$, a field of size roughly 2^{1151}. This set of parameters would therefore appear to offer about 80 bits of security.[11]

However, as is pointed out in [**41**], Coppersmith's discrete logarithm algorithm [**82**], although specifically designed for fields of characteristic 2, also applies to fields of small characteristic and is more efficient than general purpose discrete logarithm algorithms. The function field sieve as developed in [**2, 3, 169**] is also applicable and has better asymptotic performance than Coppersmith's algorithm for fields of characteristic 3. But it is currently unclear by how much these algorithms reduce the security offered by BLS signatures for particular curves defined over fields of characteristic 3. For example, it may well be that the algorithm reduces the security level below the supposed 80 bits for the parameters in the paragraph above. The conclusion of [**41**] is that in order to obtain security similar to that offered by DSA, curves $E_i(\mathbb{F}_{3^\ell})$ where $3^{6\ell}$ is much greater than 1024 bits in size are needed. Similar security considerations apply when using the same curves in other cryptographic applications. In the current context, this results in much longer signatures, running counter to the whole rationale for the BLS scheme. The problem of constructing signatures that are simultaneously short and secure should provide motivation for a detailed study of the performance of the

[9] A modified verification equation is then needed to handle the fact that two elements of G_1 are represented by each $x \in \mathbb{F}_q$.

[10] These curves are named E^+, E^- in [**40**].

[11] This choice of parameters was not present in the original version [**40**] because of the threat of Weil descent attacks; according to [**41**], the work of Diem in [**97**] shows Weil descent to be ineffective for $\ell = 121$.

function field sieve in characteristic 3. Some estimates for the size of factor bases arising in the function field sieve for fields of small characteristic can be found in [**141**].

In [**41**], Boneh, Lynn and Shacham explain how ordinary (non-supersingular) curves and unmodified pairings can be used to remedy the situation. Assume now we have a triple of groups G_1, G_2, G_3 and a pairing $e : G_1 \times G_2 \to G_3$. For $i = 1, 2$, let P_i of prime order r generate G_i. A user's private key is still a value $x \in \mathbb{Z}_r$, but now the matching public key is $[x]P_2 \in G_2$. The signature on a message $M \in \{0,1\}^*$ is still $\sigma = [x]H(M) \in G_1$. To verify a purported signature σ on message M, the verifier now checks that

$$\langle P_2, [x]P_2, H(M), \sigma \rangle$$

is a valid co-Diffie–Hellman tuple, that is a tuple in which the second pair of elements (in G_1) are related by the same multiple as the first pair (in G_2). This can be done using the pairing e by checking that the equation:

$$e(\sigma, P_2) = e(H(M), [x]P_2)$$

holds. The security of this scheme rests on the hardness of the co-CDH problem, a variant of the CDH problem appropriate to the situation where two groups G_1 and G_2 are in play. The security proof has an interesting twist, in that the existence of an efficiently computable isomorphism $\psi : G_2 \to G_1$ is required to make the proof work.

Boneh, Lynn and Shacham [**40**] show how groups and pairings suitable for use with this scheme can be obtained from MNT curves (see Section IX.15.1) and how ψ can be constructed using the trace map. They report an example curve $E(\mathbb{F}_q)$ where q is a 168-bit prime and where the embedding degree is 6. The curve has an order that is divisible by a 166-bit prime r; using appropriate subgroups of $E(\mathbb{F}_q)$ and $E(\mathbb{F}_{q^6})$ for G_1 and G_2, one can obtain a scheme with 168 bit signatures where the best currently known algorithm for the co-CDH problem requires either a generic discrete logarithm algorithm using around 2^{83} computational steps or taking a discrete logarithm in a 1008-bit field of large characteristic (where Coppersmith's algorithm and the function field sieve are ineffective). Unfortunately, the public key, being a point on $E(\mathbb{F}_{q^6})$, is no longer short, an issue that may limit the wider applicability of this scheme.

The above discussion gives a clear example where unmodified pairings should be used in preference to modified pairings for reasons of efficiency and security.

X.4.3. Further Signature Schemes. We provide brief references to a selection of the other relevant literature.

Libert and Quisquater developed an identity-based undeniable signature scheme in [**201**]. Pairings were used to construct a variety of proxy signaturechemes by Zhang *et al.* in [**326**]. Identity-based blind signatures and ring signatures were considered by Zhang and Kim in [**322, 324**], but the schemes presented lack a full security analysis. Herranz and Sáez [**147**] used the Forking Lemma methodology to build provably secure identity-based ring signatures from pairings.

Thanks mainly to their simple algebraic structure, BLS signatures have been productively exploited by a number of authors. Boldyreva [**31**] showed how to adapt the scheme of [**40**] to produce provably secure threshold signatures, multisignatures and blind signatures. The blinding capability of BLS signatures was also noted by Verheul in [**306**]. In the same paper, Verheul also considered the use of pairings to construct self-blindable credential certificates. Steinfeld *et al.* [**292**] extended the BLS signature scheme to obtain a new primitive, universal designated-verifier signatures. Boneh *et al.* [**38**] also used BLS signatures as a basis to produce an aggregate signature scheme (in which multiple signatures can be combined to form a single, short, verifiable signature), a verifiably encrypted signature scheme (with applications to fair exchange and optimistic contract signing), and a ring signature scheme. In turn, Boldyreva *et al.* [**32**] used the aggregate signature scheme of [**38**] to construct efficient proxy signature schemes. See also [**151**] for an attack on and repair of the verifiably encrypted signature scheme of [**38**], and [**85**] for a result relating the complexity assumption that was used to establish security for the aggregate signature scheme in [**38**] to the CDH problem.

Recently, Libert and Quisquater and Quisquater [**202**] modified the BLS signature scheme to produce a particularly efficient *signcryption* scheme, that is, a scheme in which signature and encryption are combined into a single "monolithic" operation. An alternative scheme of Malone-Lee [**210**] has a security proof in a multi-user model and offers ciphertexts that are even shorter than in the scheme of [**202**]. Malone-Lee's scheme is not based on BLS signatures, but does use pairings as a tool in the security proofs.

Zhang *et al.* [**328**] modified the BLS signature scheme to obtain a more efficient signature scheme that does not require the use of a special hash function (i.e. one that outputs elements of G_1). The scheme is provably secure in the random oracle model, but its security is based on the hardness of the non-standard k-weak CDH problem that was introduced in [**227**]. Zhang *et al.* [**327**] adapted the scheme of [**328**] to obtain a verifiably encrypted signature scheme, also based on pairings, but more efficient than the scheme of [**38**].

Boneh, Mironov and Shoup [**42**] used pairings to construct a tree-based signature scheme whose security can be proved in the standard model (i.e. without the use of random oracles), based on the hardness of the CDH problem. A much more efficient scheme, also secure in the standard model, was presented in [**34**]. Here, the security relies on the hardness of another non-standard problem, the Strong Diffie–Hellman problem. This problem is related to the k-weak CDH problem of [**227**].

X.4.4. Identity-Based Signcryption. A number of authors have considered combining signature and encryption functions in a single identity-based scheme. The first attempt appears to be that of Malone-Lee [**209**], who provided an identity-based signcryption scheme. Unfortunately, the computational costs of the signcryption and matching un-signcryption operations in [**209**] are not much less than the sum of the costs of the encryption/decryption and signature/verification algorithms of [**37**] and [**58**] (say). On the other hand, the scheme's ciphertexts are a little shorter than they would be in the case of a simple "sign then encrypt" scheme. In contrast to the scheme of Lynn [**207**], Malone-Lee's scheme offers non-repudiation: an entity A can present a message and ciphertext to a judge who can then verify that they originated from another entity B. However, as is pointed out in [**200**], this property means that Malone-Lee's scheme cannot be semantically secure.[12] An identity-based signcryption scheme which does not suffer from this weakness was presented by Libert and Quisquater in [**200**]. The scheme uses pairings, is roughly as efficient as the scheme of [**209**] and has security that depends on the hardness of the decision-bilinear-Diffie–Hellman problem (defined in Section IX.11.3 for unmodified pairings). This scheme also allows non-repudiation, but the origin of ciphertexts can be verified by third parties without knowledge of the underlying plaintext. This last feature may be a positive or negative one depending on the intended application.

A two-layer approach to combining identity-based signature and encryption was taken by Boyen in [**45**]. The resulting mechanism, called an IBSE scheme, has comparable efficiency but stronger security guarantees than the earlier work of [**200, 209**]. As well as providing the usual properties of confidentiality and non-repudiation, the pairing-based scheme of Boyen in [**45**] offers ciphertext unlinkability (allowing the sender to disavow creating a ciphertext), ciphertext authentication (allowing the recipient to be convinced that the ciphertext and signed message it contains were prepared by the same entity) and ciphertext anonymity (making the identification of legitimate sender and recipient impossible for any entity not in possession of the recipient's decryption key, in contrast to the scheme of [**200**]). These properties are not available from single-layer signcryption schemes and a major contribution of [**45**] is to identify and formalise these properties. The security of Boyen's IBSE scheme depends on the hardness of the BDH problem. An examination of the scheme shows that it builds on the NIKDS of Sakai *et al.* [**260**], with the key $\hat{e}(Q_A, Q_B)^s$ once again being at the heart of the matter. Chen and Malone-Lee [**68**] have recently proposed an identity-based signcryption scheme that is secure in the model of [**45**], but more efficient than Boyen's IBSE scheme.

[12] The adversary, when presented with a challenge ciphertext C^* which encrypts one of M_0, M_1, can simply attempt to verify both pairs M_0, C^* and M_1, C^*; a correct verification reveals which plaintext M_b was encrypted.

X.5. Hierarchical Identity-Based Cryptography and Related Topics

Identity-based cryptography as we have described it so far in this chapter involves a single trusted authority, the PKG, who carries out all the work of registering users and distributing private keys. Public key infrastructures (PKIs) supporting "classical" public key cryptography allow many levels of trusted authority through the use of certificates and certificate chains. A hierarchy of CAs topped by a root CA can spread the workload and simplify the deployment of systems relying on public key cryptography. The first attempt to mimic the traditional PKI hierarchy in the identity-based setting was due to Horowitz and Lynn [**156**]. Their scheme is restricted to two levels of hierarchy and has limited collusion resistance. A more successful attempt was made soon after by Gentry and Silverberg [**135**]. Their solution, which extends the IBE scheme of Boneh and Franklin in a very natural way, has led other researchers to develop further interesting cryptographic schemes. In this section, we outline the contribution of Gentry and Silverberg in [**135**] and then give a brief overview of the subsequent research.

X.5.1. The Basic Scheme of Gentry and Silverberg. The basic hierarchical identity-based encryption (HIBE[13]) scheme of [**135**] associates each entity with a level in the hierarchy, with the root authority being at level 0. An entity at level t is defined by its tuple of identities $\langle \mathtt{ID}_1, \mathtt{ID}_2, \dots, \mathtt{ID}_t \rangle$. This entity has as superior entities the root authority (or root PKG) together with the $t-1$ entities whose identities are $\langle \mathtt{ID}_1, \mathtt{ID}_2, \dots, \mathtt{ID}_i \rangle$, $1 \le i < t$. An entity at level t will have a secret $s_t \in \mathbb{Z}_r^*$, just like the PKG in the Boneh-Franklin IBE scheme. As we describe below, this secret will be used by an entity at level t to produce private keys for its children at level $t+1$.

The scheme `BasicHIBE`[14] is defined by five algorithms:

`Root Setup`, `Lower-level Setup`,
`(Private Key) Extract`, `Encrypt` and `Decrypt`.

These operate as follows:

`Root Setup`**:** To set up the root authority at level 0, this algorithm takes as input a security parameter ℓ and outputs the system parameters:

$$\mathtt{params} = \langle G_1, G_3, \hat{e}, n, P_0, Q_0, H_1, H_2 \rangle.$$

Here G_1, G_3, $\hat{e}$, n (the bit-length of plaintexts) and hash functions H_1 and H_2 are just as in the Boneh-Franklin scheme. We write P_0 for an arbitrary

[13] This is a perhaps more natural acronym than "HIDE" as used by Gentry and Silverberg, albeit one that does not have the same neat connotation of secrecy. It also enables us to use the acronym HIBS for the matching concept of a hierarchical identity-based signature scheme. It can be no bad thing to mention at least one Scottish football team in this chapter.

[14] `BasicHIDE` in [**135**]

generator of G_1 and $Q_0 = [s_0]P_0$ where $s_0 \in \mathbb{Z}_r^*$ is the root authority's secret value. Apart from these minor changes of notation, this procedure is identical to the `Setup` procedure of the scheme `BasicIdent` in [**37**].

`Lower-level Setup`: An entity at level t in the hierarchy is initialised simply by selecting for itself a secret value $s_t \in \mathbb{Z}_r^*$.

`Extract`: Consider a level t entity $\mathcal{E}_t$ with identity tuple $\langle \mathtt{ID}_1, \mathtt{ID}_2, \ldots, \mathtt{ID}_t \rangle$. This entity's parent (having identity $\langle \mathtt{ID}_1, \mathtt{ID}_2, \ldots, \mathtt{ID}_{t-1} \rangle$) performs the following steps:

1. Compute $P_t = H_1(\mathtt{ID}_1, \mathtt{ID}_2, \ldots, \mathtt{ID}_t) \in G_1$.
2. Set $S_t = S_{t-1} + s_t P_t \in G_1$ and give the private key S_t to entity $\mathcal{E}_t$ over a secure channel. (When $t = 1$, we set $S_0 = 1_{G_1}$.)
3. Give $\mathcal{E}_t$ the values $Q_i = s_i P_0$, $1 \leq i < t$.

Notice that, by induction, we have $S_t = \sum_{i=1}^{t} s_{i-1} P_i$.

`Encrypt`: To encrypt plaintext $M \in \{0,1\}^n$ for an entity with identity tuple $\langle \mathtt{ID}_1, \mathtt{ID}_2, \ldots, \mathtt{ID}_t \rangle$, perform the following steps:

1. Compute $P_i = H_1(\mathtt{ID}_1, \mathtt{ID}_2, \ldots, \mathtt{ID}_i) \in G_1$ for $1 \leq i \leq t$.
2. Choose a random $w \in \mathbb{Z}_r^*$.
3. Compute and output the ciphertext:

$$C = \langle [w]P_0, [w]P_2, \ldots [w]P_t, M \oplus H_2(\hat{e}(P_1, Q_0)^w) \rangle \in G_1^t \times \{0,1\}^n.$$

Notice that in order to encrypt a message for an entity, the sender needs only know the parameters of the root PKG along with the identity tuple of the intended recipient, and not any parameters associated with intermediate entities. Note too that the omission of the value $[w]P_1$ from the ciphertext is deliberate (if it were included, then an eavesdropper could decrypt C by calculating the mask $H_2(\hat{e}([w]P_1, Q_0)))$.

`Decrypt`: Suppose $C = \langle U_0, U_2, \ldots, U_t, V \rangle \in G_1^t \times \{0,1\}^n$ is a ciphertext encrypted for an entity $\langle \mathtt{ID}_1, \mathtt{ID}_2, \ldots, \mathtt{ID}_t \rangle$. To decrypt C using the private key S_t, the recipient computes

$$M' = V \oplus H_2 \left(\hat{e}(S_t, U_0) \cdot \prod_{i=2}^{t} \hat{e}(Q_{i-1}, U_i)^{-1} \right).$$

To see that decryption works properly, consider the following chain of equalities, established using the bilinearity of $\hat{e}$:

$$\begin{aligned}
\hat{e}(S_t, U_0) \cdot \prod_{i=2}^{t} \hat{e}(Q_{i-1}, U_i)^{-1} &= \hat{e}(\sum_{i=1}^{t} [s_{i-1}]P_i, [w]P_0) \cdot \prod_{i=2}^{t} \hat{e}([s_{i-1}]P_0, [w]P_i)^{-1} \\
&= \hat{e}(\sum_{i=1}^{t} [s_{i-1}]P_i, [w]P_0) \cdot \prod_{i=2}^{t} \hat{e}(-[s_{i-1}]P_i, [w]P_0) \\
&= \hat{e}(\sum_{i=1}^{t} [s_{i-1}]P_i, [w]P_0) \cdot \hat{e}(-\sum_{i=2}^{t} [s_{i-1}]P_i, [w]P_0) \\
&= \hat{e}([s_0]P_1, [w]P_0) \\
&= \hat{e}(P_1, [s_0]P_0)^w \\
&= \hat{e}(P_1, Q_0)^w.
\end{aligned}$$

A few comments on this scheme are in order. Firstly, note that encryption only requires one pairing computation, and this needs only to be computed once to enable communication with any entity registered in the hierarchy. On the other hand, t pairing computations are required for every decryption. It would be interesting to find hierarchical schemes with an alternative balance between the costs of encryption and decryption. Secondly, notice how the length of ciphertexts grows with t – this seems inescapable in a hierarchical system. Thirdly, note that the scheme has a strong in-built escrow, in that any ancestor of an entity can decrypt ciphertexts intended for that entity: an ancestor at level j can use the equation

$$M' = V \oplus H_2\left(\hat{e}(S_j, U_0) \cdot \prod_{i=2}^{j} \hat{e}(Q_{i-1}, U_i)^{-1}\right)$$

to decrypt a message encrypted for a child at level t.

X.5.2. Extensions of the Basic Scheme. In [**135**], Gentry and Silverberg also showed how to use the techniques of Fujisaki-Okamoto [**119**] to produce a strengthened encryption scheme which is secure against chosen-ciphertext attackers in the random oracle model, provided that the BDH problem is hard. The security model adopted in [**135**] is sufficiently strong to capture collusions of entities attempting to compromise the private keys of their ancestors. This is because it allows the adversary to extract the private keys of entities at any level in the hierarchy and to adaptively select the identity on which it wishes to be challenged.

Naor's idea for turning an IBE scheme into a signature scheme was exploited in [**135**] to produce a hierarchical identity-based signature (HIBS) scheme. The security of this scheme depends on the hardness of the CDH problem in G_1. Gentry and Silverberg also considered how the NIKDS of Sakai *et al.* can be used to reduce the amount of computation needed for encryption between two parties who are "near" to one another in the hierarchy. The resulting scheme also enjoys shorter ciphertexts. A number of other variants on this theme are also explored in [**135**].

X.5.3. Related Topics. Canetti, Halevi and Katz [**52**] built upon the work of [**135**] to produce the first non-trivial forward-secure public-key encryption (FS-PKE) scheme. In a FS-PKE scheme, a user has a fixed public key but a private key which evolves over time; such a scheme should then have the property that a compromise of the user's private key at time t does not affect the security of messages encrypted during earlier time periods (though clearly no security can be guaranteed after time t).

The scheme in [**52**] makes use of a basic primitive called a binary tree encryption (BTE) scheme. A BTE scheme consists of a single "master" public key, a binary tree of private keys together with encryption and decryption algorithms and a routine which computes the private keys of the children of a node from the private key at that node. The encryption algorithm takes as input the public key and the label of a node. A selective-node chosen-ciphertext attack (SN-CCA) against a BTE scheme goes roughly as follows. The adversary selects a target node to attack in the challenge phase in advance. The adversary is then given the private keys for a certain set of nodes. This set consists of all the children of the target together with all the siblings of the target's ancestors. This is the maximal set of private keys which the adversary can be given without enabling the trivial computation of the private key of the target node. The adversary's job is then to distinguish ciphertexts encrypted under the public key and target node, given access to a decryption oracle.

Canetti, Halevi and Katz show how a BTE scheme secure against SN-CCA attacks can be constructed from a simplification of the HIBE scheme of [**135**]. They then show how any SN-CCA secure BTE scheme can be used in a simple construction to obtain an encryption scheme that is forward-secure in a natural adaptation of the standard IND-CCA2 model for public key encryption. The trick is to traverse the tree of the BTE in a pre-order traversal, with the key at the t-th node in the traversal determining how the private key in the forward-secure scheme is updated at time t. The security definition for a BTE scheme quickly converts into the desired forward security. Combining their constructions, the authors of [**52**] obtain an efficient, forward-secure encryption scheme whose security rests of the hardness of the BDH problem in the random oracle model.

A BTE scheme secure in the SN-CCA sense, but without requiring random oracles, is also constructed in [**52**]. The construction uses $O(\ell)$-wise independent hash functions and the security of the resulting BTE scheme depends on the hardness of the DBDH problem rather than the BDH problem. However the construction gives a completely impractical scheme because of its reliance on non-interactive zero-knowledge proofs. As an interesting aside, Canetti, Halevi and Katz go on to show how a HIBE scheme can be constructed from a BTE scheme, though with a weaker security model than is considered in [**135**]. A corollary of this result is the construction of an IBE scheme (and a HIBE scheme) that is secure in the standard model (i.e. without the use of random oracles) assuming the hardness of the DBDH problem, though only for an adversary who specifies in advance which identity he will attack. Again the scheme will be impractical if it is to be secure against chosen-ciphertext attacks.

One issue that the proofs of security in [**52**] have in common with those of [**37, 135**] (and indeed many papers in the area) is that the security reductions are not particularly tight. For example, a factor of $1/N$ is introduced in [**52**, Proof of Theorem 4], where N is the number of time periods supported by the FS-PKE scheme. It seems to be a challenging problem to produce results tightly relating the security of the schemes to the hardness of some underlying computational problems.

Canetti, Halevi and Katz [**53**] have shown a surprising connection between IBE and chosen-ciphertext security for (normal) public key encryption. They give a construction for an IND-CCA2 secure scheme of the latter type from a weakly-secure IBE scheme and a strongly unforgeable one-time signature scheme. Here, the IBE scheme need only be secure against chosen-plaintext attacks by selective-ID adversaries, that is, adversaries who specify in advance which identity they will attack in the challenge phase. The twist needed to make the construction work is to interpret the public key of the signature scheme as an identity in the IBE scheme, for which the decrypting party holds the master secret. Since a weakly-secure IBE scheme can be constructed in the standard model, the results of [**53**] yield a new IND-CCA2 secure public key encryption scheme whose security does not rely on the random oracle assumption.

Boneh and Boyen [**33**] provided new and efficient constructions for a HIBE scheme and an IBE scheme using pairings. Both schemes are secure in the standard model, against selective-ID, chosen plaintext attackers. The HIBE scheme is secure given that the DBDH problem is hard. It can be converted into a selective-ID, chosen-ciphertext secure HIBE scheme using the method of [**53**]; the resulting scheme is efficient. The security of the new IBE scheme in [**33**] depends on the hardness of a new problem, the decision bilinear Diffie–Hellman Inversion problem (DBDHI problem), which is related to a decisional version of the k-weak CDH problem of [**227**]. This scheme is also closely related to the signature scheme of [**34**]. Unfortunately, no efficient conversion to a chosen-ciphertext secure scheme is currently known. However, by combining this scheme with ideas in [**53**] and the signature scheme of [**34**], one obtains a reasonably efficient public key encryption scheme that is IND-CCA2 secure in the standard model.

Forward secure encryption is perhaps the most basic form of what might be called "key updating cryptography." Here the general approach is to have an evolving private key which may or may not be updated with the help of second entity called a base or helper. Several other papers use pairings to address problems in this area. Of particular note is the work of Bellare and Palacio in [**22**] and of Dodis *et al.* in [**100**]. In the former paper, the authors construct a strongly key-insulated encryption scheme from the IBE scheme of Boneh and Franklin. Such a scheme allows a user to cooperate with a helper to refresh his private key; the scheme remains secure even if the user's private key is corrupted in up to some threshold number of time periods, and even if the helper is compromised (so long as the user's key then is not). Bellare and Palacio also provide an equivalence result in [**22**, Theorem 4.1], relating the existence of a secure IBE scheme to that of a secure strongly key-insulated encryption scheme. Dodis *et al.* [**100**] work with an even stronger security model, in which the base can also be frequently corrupted, and construct an intrusion-resilient public key encryption scheme from the forward-secure scheme of [**52**].

Yum and Lee [**321**] have explored similar concepts in the context of signatures, using the IBS scheme of [**58**] to obtain efficient key updating signature schemes.

X.6. More Key Agreement Protocols

Alongside encryption and signatures, key agreement is one of the fundamental cryptographic primitives. As we have already seen in Section X.2, pairings were used early on to construct key agreement schemes and protocols. In this section, we examine how this area has developed since the foundational work of [**260, 167**].

X.6.1. Two party Key Agreement Protocols. The NIKDS of Sakai *et al.* [**260**] allows two parties to non-interactively agree the identity-based key $K_{AB} = \hat{e}(Q_A, Q_B)^s$ after they have registered with the same TA and obtained their respective private keys $S_A = [s]Q_A$, $S_B = [s]Q_B$. However, the key K_{AB} is a static one, while many applications require a fresh key for each communications session.

Smart [**286**] was the first author to consider how pairings could be used to develop identity-based, authenticated key agreement protocols. His protocol uses the same keying infrastructure as the IBE scheme of Boneh and Franklin. In particular, system parameters $\langle G_1, G_3, \hat{e}, P, Q_0 = [s]P, H_1\rangle$ are pre-established and entities A, B possess private keys $S_A = [s]Q_A$, $S_B = [s]Q_B$. Here, $Q_A = H_1(\mathtt{ID}_A)$ where $\mathtt{ID}_A$ is the identity string of A. Q_B is defined similarly. In Smart's protocol, A and B exchange ephemeral values $T_A = [a]P$ and $T_B = [b]P$, where a, b are selected at random from $\mathbb{Z}_r^*$. Notice that these are identical to the messages exchanged in a straightforward

Diffie–Hellman protocol for the group G_1. Entity A then computes:

$$K_A = \hat{e}([a]Q_B, Q_0) \cdot \hat{e}(S_A, T_B)$$

while entity B computes:

$$K_B = \hat{e}([b]Q_A, Q_0) \cdot \hat{e}(S_B, T_A).$$

It is an easy exercise to show that

$$K_A = K_B = \hat{e}([a]Q_B + [b]Q_A, [s]P)$$

so that this common value can be used as the basis of a shared session key. The bandwidth requirements of the protocol are moderate, being one element of G_1 per participant. A version of the basic protocol offering key confirmation is also considered in [**286**]: this service ensures that each entity gets a guarantee that the other entity actually has calculated the shared key. While no attacks have been found on this protocol to date, no formal security analysis has been given either.

Smart's protocol requires two pairing computations per participant. An alternative protocol was given by Chen and Kudla in [**67**]. In their protocol, A and B exchange ephemeral values $W_A = [a]Q_A$ and $W_B = [b]Q_B$ and compute the keys

$$K_A = \hat{e}(S_A, W_B + [a]Q_B), \quad K_B = \hat{e}(W_A + [b]Q_A, S_B).$$

Now $K_A = K_B = \hat{e}(Q_A, Q_B)^{s(a+b)}$ can be computed using just one pairing operation. A useful security model that is applicable for this type of protocol is the extension of the Bellare-Rogaway model [**24**] to the public key setting that was developed by Blake-Wilson *et al.* in [**27, 28**]. It is proved in [**66**] that the above protocol is a secure authenticated key agreement in this model, provided the BDH problem is hard. The original proof of this result published in [**67**] is flawed, and a strong restriction on adversarial behaviour is needed provide the corrected version in [**66**]. Chen and Kudla also consider modifications of their protocol which provide forward secrecy, anti-escrow features and support for multiple TAs.

Other authors have also tried to adapt Smart's protocol. Shim's attempt [**275**] was shown to be vulnerable to a man-in-the-middle attack in [**296**]. Yi's protocol [**320**] halves the bandwidth required by Smart's protocol using a form of point compression.

An alternative approach to identity-based key agreement was taken by Boyd *et al.* in [**44**]. In this work the non-interactively agreed key $K_{AB} = \hat{e}(Q_A, Q_B)^s$ of Sakai *et al.* is used as the key to a MAC algorithm to provide authentication of the messages in a Diffie–Hellman key exchange. The resulting protocol is provably secure in the model developed in [**21, 54**] and has the interesting privacy feature of providing deniable authentication: since either party could have computed all the messages in a protocol run, both parties can also deny having taken part in the protocol. The authors of [**44**] also considered the use of identity-based encryption as a session key transport mechanism. Related uses of the key $\hat{e}(Q_A, Q_B)^s$ in "secret handshake" key agreement protocols were also explored in [**12**], where the integration of these protocols into the SSL/TLS protocol suite was also studied.

X.6.2. Multi-party Key Agreement Protocols. In this section we discuss how Joux's protocol [**167**] has inspired new protocols for multi-party key agreement.

Recall that in Joux's protocol, the key agreed between three parties is equal to $\hat{e}(P, P)^{abc}$ when the ephemeral broadcast values are $[a]P$, $[b]P$ and $[c]P$. We have noted in Section X.2.2 that this protocol is vulnerable to man-in-the middle attacks because it is not authenticated. An obvious way to enhance the security of the protocol is to add signatures to the ephemeral values. A number of efficient, signature-free approaches to securing Joux's protocol were described in [**6**]. It was also shown in [**6**], perhaps surprisingly, that an authenticated version of Joux's protocol has no benefit over a simple extension of the Diffie–Hellman protocol when three party, authenticated protocols with confirmation are considered in a non-broadcast environment: any secure protocol will require at least six messages in this context. Galbraith *et al.* [**124**] have studied the bit security of the BDH problem; their results can be applied to Protocols of [**6**] and [**286**] to show that it is secure to use a finite-field trace operation to derive a session key from the raw key material exchanged in these protocols.

Shim's attacks [**274**] on the protocols of [**6**] show that adding authentication to three-party protocols is a delicate business. Zhang and Liu [**325**] developed identity-based, authenticated versions of Joux's protocol.[15] Nalla and Reddy [**236**] also put forward identity-based, three party key agreement protocol, but these were all broken in [**70, 273**]. Meanwhile, Shim's proposal for a three-party protocol [**276**] was broken in [**296**].[16]

Protocols for more than three parties, using Joux's protocol and its derivatives as a building block, have been considered by several authors [**105, 258, 13**]. Lack of space prevents their detailed consideration here. For attacks on some other schemes which attempted to mimic the Burmester-Desmedt protocol of [**50**], see [**323**].

X.7. Applications and Infrastructures

It should be apparent that one of the major uses of pairings has been in developing identity-based cryptographic primitives. So far, we have said little about what identity-based public key cryptography (ID-PKC) has to offer in

[15]Note that there is no real benefit in deriving eight different keys from a single key exchange by algebraic manipulations as in [**325**]: a simple key derivation function based on hashing suffices.

[16]Even though the protocol defined in [**276**] does not actually make mathematical sense! For it involves an exponentiation of an element $\hat{e}(P, P)$ in G_3 to a power that is a product of an element in $\mathbb{Z}_r^*$ and an element in G_3.

comparison to more traditional forms of public key cryptography. We rectify this in the first part of this section. We go on to study how pairings have been used to develop new architectures supporting the deployment of public key cryptography. Then in the third part, we outline a variety of recent work in which pairings have been put into practice, either in trials of identity-based technology or in on-paper proposals outside the immediate confines of cryptography.

X.7.1. Further Development of Identity-based Systems. We introduced the concepts of identity-based encryption (IBE) and, more generally, ID-PKC in Sections X.2.1 and X.3, portraying them as being useful alternatives to traditional PKIs. Here we explore in a little more detail why this is the case, and critically examine some of the problems inherent in identity-based approaches.

X.7.1.1. Identity-based Systems Versus Traditional PKIs. Recall that in an identity-based system, a TA is responsible for issuing private keys to the correct users. This TA in effect replaces the CA in a traditional PKI, but the roles of TA and CA are somewhat different. The CA in a traditional PKI does not usually know users' private keys, but rather issues certificates which assert a binding between identities and public keys. The TA in an identity-based system is responsible for checking that applicants do have the claimed identity and then issuing the corresponding private key. Thus identity-based systems automatically have a key escrow facility. Whether this is a good thing or not will depend on the particular application at hand. It will certainly be a useful feature in many "corporate" deployment scenarios, where the recovery of encrypted files and e-mail may well be important should an employee leave the organisation, say. However, escrow can complicate the issue of non-repudiation of signatures. For example, an important piece of EU legislation [**EU 1999**] requires that the signing key be under the sole control of the signing party in order that a signature be recognised as an "advanced electronic signature". Thus traditional signatures supported by a PKI are likely to be more useful than identity-based signatures in practice.

Note that, in both ID-PKC and traditional PKI, it is important to authenticate applicants before issuing valuable data (private keys in the former, certificates in the latter). So some additional authentication mechanism is needed at the time of registration/key issuance. Both systems also require that any system parameters (e.g. a root certificate or a TA's public parameters) are authentically available to users. However, with ID-PKC, there is an additional requirement: the private keys must be delivered over confidential and authentic channels to the intended recipients. Again this seems to point towards the enterprise as being a fruitful deployment area for ID-PKC

– for example, one could use a company's internal mail system and personnel database to distribute keys and control registration for low-to-medium security applications.

The particular IBE scheme of Boneh and Franklin [**37**] supports multiple TAs and split private keys in a very natural way. This goes some way to addressing escrow concerns. For example, suppose two TAs share parameters $\langle G_1, G_3, \hat{e}, P\rangle$ but have master secrets $s_1, s_2 \in \mathbb{Z}_r^*$ and public values $Q_1 = [s_1]P$, $Q_2 = [s_2]P$. Then a user A with identity string $\mathtt{ID}_A$ can form his private key as the sum $[s_1]Q_A + [s_2]Q_A = [s_1 + s_2]Q_A$ of the private keys obtained from each TA. To encrypt to A, ciphertexts of the form

$$\langle [t]P, M \oplus H_2(\hat{e}(Q_A, Q_1 + Q_2)^t)\rangle$$

can be used. More generally, a k-out-of-n escrow capability can be established – see [**37**] for details. Such a facility is also supported by many other ID-based schemes developed post-Boneh-Franklin.

The ability to make use of multiple TAs was exploited in [**65**] to create cryptographic communities of interest. Here, each TA represents a particular group (e.g. the group of all people having the same citizenship, profession or name); a sum of keys from different groups creates intersections of groups all of whose members can calculate the same private key.

Another point of comparison for traditional public key and ID-PKC systems is the issue of revocation. Whenever a certificate in a traditional system expires (perhaps because the end of its validity period is reached or because of a private key compromise), this fact must be communicated to the parties relying on the certificates. There is the same requirement for timely transmission of revocation information in an ID-PKC system too. It has been suggested by many authors that in ID-PKC, one can simply attach a validity period to identities, for example "john.smith || 2004", so that public keys automatically expire. However such a system is no longer purely identity-based, and one must still find a way to deal with keys that become compromised before the end of their expiry period.

A deeper comparison of revocation and many other issues for ID-PKC and traditional PKIs is made in [**251**]. Whether ID-PKC really has something to offer over traditional PKIs and even symmetric systems very much depends on the application context, on what is to be secured and on what constraints there are on the solutions that can be adopted. It is certainly not the case that an identity-based approach will be the correct one in every circumstance.

X.7.1.2. Cryptographic Workflows. An apparently innocuous feature of IBE is that when encrypting a message for entity A, the sender can choose the identity string $\mathtt{ID}_A$ used in the encryption process. Only if A has the matching private key $[s]Q_A = [s]H_1(\mathtt{ID}_A)$ will he be able to decrypt the message. Naturally, in many situations, it is most convenient if the sender chooses a string $\mathtt{ID}_A$ for which this is the case. However it is possible that

A's identity $\mathtt{ID}_A$ and public key Q_A are actually determined *before* the private key $[s]Q_A$. This can have interesting consequences. For example, the sender can encode in A's identity string a set of conditions (or a policy) that should be met before the TA, acting as a policy monitor, should issue the private key.

The idea of encoding conditions in identity strings can be combined with the use of multiple TAs to create a *cryptographic workflow*, that is, a sequence of private key issuances that must be successfully carried out before an entity can decrypt a ciphertext. In this context, the "I" in ID-PKC is better interpreted as "identifier", since rarely will identities be used alone.

As an example of this concept in action, consider the scenario where a customer wants his bank manager to have access to a particular instruction, but only after a certain time. Suppose the bank acts as a TA for its employees in a Boneh-Franklin IBE scheme with the usual parameters $\langle G_1, G_3, \hat{e}, P\rangle$, master secret s_{bank} and public parameter $Q_{bank} = [s_{bank}]P$. Suppose that the bank manager has received his private key $[s_{bank}]H_1(\mathtt{ID}_{bm})$. Suppose also that a third party operates an encrypted time service as follows. The third party, using the same basic public parameters as the bank, acts as a TA with master secret s_{time} and public parameter $Q_{time} = [s_{time}]P$. At time T, the third party broadcasts to all subscribers the private key $[s_{time}]H_1(T)$. Now to encrypt an instruction M for the bank manager to be read only after time T_0, the customer creates the ciphertext:

$$C = \langle [t]P, M \oplus H_2(\hat{e}(Q_{bank}, H_1(ID_{bm}))^t \cdot \hat{e}(Q_{time}, H_1(T_0))^t)\rangle.$$

Here, the customer has encrypted M using both the identity of the bank manager and the time T_0 after which the message is to become decryptable. Only after time T_0 can the bank manager access the value $[s_{time}]H_1(T_0)$ and combine this with his private key $[s_{bank}]H_1(\mathtt{ID}_{bm})$ in the bank's scheme to compute the value:

$$H_2(\hat{e}([t]P, [s_{bank}]H_1(\mathtt{ID}_{bm})) \cdot \hat{e}([t]P, [s_{time}]H_1(T_0)))$$

allowing decryption of ciphertext C.

In this example, the customer created a special public key for encryption out of two identifiers, the bank manager's identity and the time identifier. These identifiers come from two different schemes with two different TAs, but ones who share some parameters – perhaps they are using standardised groups and pairings.[17] The customer has used multiple TAs to create a work-flow that the bank manager must follow in order to access the desired information: first the bank manager must obtain his private key in the bank's scheme; then he must wait for the time service to reveal the private key at time T_0.

It is easy to imagine other scenarios where the dynamic creation of work-flows in this way could be very useful. There is no theoretical limit on the

[17] In fact the reliance on shared parameters can be almost completely eliminated by slightly modifying the encryption algorithm.

number of private keys that the recipient must fetch, or the types of roles or identifiers that can be used. The recipient may be required to perform some kind of authentication (based on identity, address, role in an organisation, etc) at each stage. Further research along these lines, allowing the expression of more complex conditions in identifiers, can be found in [**65, 288**].

X.7.2. New Infrastructures. Some form of hierarchy seems necessary in order to address the scalability and availability issues inherent in any system with a single point of distribution for keying material. We have seen how the work of Gentry and Silverberg [**135**] allows a hierarchy of TAs in ID-based systems. Chen *et al.* [**64**] have studied the benefits of developing a mixed architecture, with identity-based TAs administering users at the lowest levels of the hierarchy being supported by a traditional PKI hierarchy above.

In [**134**], Gentry introduced the concept of Certificate-Based Encryption (CBE), with a view to simplifying revocation in traditional PKIs, and used pairings to construct a concrete CBE scheme. We give a brief review of Gentry's scheme using notation as previously established: P generates G_1 of prime order r, $\hat{e} : G_1 \times G_1 \to G_3$ is a bilinear map and $H_2 : G_3 \to \{0,1\}^n$ is a hash function.

In Gentry's CBE scheme, an entity A's private key consists of two components. The first component $[s_C]P_A(i)$ is time-dependent and is issued as a certificate to A on a regular basis by a CA. Here s_C is the CA's private key and $P_A(i) \in G_1$ is derived from hashing certain parameters, including A's public key $[s_A]P$ and the current time interval i. The second component $[s_A]P'_A$ is chosen by A and kept private. Here, $P'_A \in G_1$ is derived from A's identifying data. So A's private key is the sum $[s_C]P_A(i) + [s_A]P'_A$, a time-dependent value that is only available to A if A is certified in the current time interval. Now to encrypt a message M for A, an entity selects t at random from $\mathbb{Z}_r^*$ and sets:

$$C = \langle [t]P, M \oplus H_2(\hat{e}([s_C]P, P_A(i))^t \cdot \hat{e}([s_A]P, P'_A)^t) \rangle.$$

Notice that $[s_C]P$ is available to encrypting parties as a public parameter of the CA, while $P_A(i)$, P'_A can be computed from A's public information, and $[s_A]P$ is A's public key. Decryption by A is straightforward if A has $[s_C]P_A(i)$. For if $C = \langle U, V \rangle$, then A can compute:

$$\begin{aligned} \hat{e}(U, [s_C]P_A(i) + [s_A]P'_A) &= \hat{e}([t]P, [s_C]P_A(i)) \cdot \hat{e}([t]P, [s_A]P'_A) \\ &= \hat{e}([s_C]P, P_A(i))^t \cdot \hat{e}([s_A]P, P'_A)^t. \end{aligned}$$

Notice that the private key $[s_C]P_A(i) + [s_A]P'_A$ used here can be regarded as a two-party aggregate signature in the scheme of [**38**]. The second private component $[s_C]P_A(i)$ acts as an *implicit certificate* for relying parties: one that a relying party can be assured is only available to A provided that A's certificate has been issued for the current time period by the CA. The security of CBE depends critically on the CA binding the correct public key into A's implicit certificate in each time period. Thus (quite naturally), the initial registration of users and their public keys must take place over an authentic channel and be bootstrapped from some other basis for trust between A and the CA.

This approach can significantly simplify revocation in PKIs. For notice that there is no need to make any status checks on A's public key before encrypting a message for A. So there is no requirement for either Certificate Revocation Lists or an on-line certificate status checking protocol. However, the basic CBE approach of [**134**] does have a major drawback: the CA needs to issue new values $[s_C]P_A(i)$ to every user in the scheme in every time period. A granularity of one hour per time period is suggested in [**134**]; this substantially adds to the computation and communication that takes place at the CA for a PKI with even a small user base. The basic CBE approach can be regarded as effectively trading simplified revocation for an increased workload at the CA. A number of enhancements to the basic CBE approach are also presented in [**134**]. These reduce the work that must be carried out by the CA.

A security model for CBE is also developed in [**134**], and Gentry goes on to show that the CBE scheme described above, but modified using the Fujisaki-Okamoto technique [**119**], meets the definition of security for the scheme, provided that the BDH problem is hard. It is clear that similar ideas to Gentry's can be applied to produce certificate-based signature schemes. A scheme of this type was developed in [**176**].

Al-Riyami and Paterson [**7**] proposed another new model for supporting the use of public key cryptography which they named certificateless public key cryptography (CL-PKC). Independently, Chen *et al.* [**69**] proposed similar ideas in the context of signatures and group signatures. The key feature of the model of [**7**] is that it eliminates the need for certificates, hence the (somewhat clumsy) adjective "certificateless."

Pairings are used to construct concrete CL-PKC schemes in [**7**]. As in [**134**], an entity A's private key is composed in two stages. Firstly, an identity-dependent *partial private key* $[s]Q_A = [s]H_1(\mathtt{ID}_A)$ is received over a confidential and authentic channel from a trusted authority (called a key generation centre, KGC).[18] Secondly, A combines the partial private key $[s]Q_A$ with a secret x_A to produce his private key $S_A = [x_A s]Q_A$. The corresponding public key is the pair $\langle X_A, Y_A\rangle = \langle [x_A]P, [x_A]Q_0\rangle$, where $Q_0 = [s]P$ is a public parameter of the system. The certificateless encryption (CL-PKE) scheme of [**7**] is obtained by adapting the IBE scheme of Boneh and Franklin [**37**], and operates as follows in its basic form. To encrypt a message for A, an entity

[18] This partial private key $[s]H_1(\mathtt{ID}_A)$ is identical to the private key in the IBE scheme of Boneh and Franklin. It can also be regarded as a BLS signature by the TA on A's identity, and hence as a form of certification, though one that does not involve A's public key.

first checks that the equality

$$\hat{e}(X_A, Q_0) = \hat{e}(Y_A, P)$$

holds, then selects t at random from $\mathbb{Z}_r^*$ and sets:

$$C = \langle [t]P, M \oplus H_2(\hat{e}(Q_A, Y_A)^t) \rangle.$$

It is easy to see that to decrypt $C = \langle U, V \rangle$, A can use his private key $S_A = [x_A s]Q_A$ and compute $M = V \oplus H_2(\hat{e}(S_A, U))$.

Notice that in this encryption scheme, A's public key need not be supported by a certificate. Instead, an entity A who wishes to rely on A's public key is assured that, if the KGC has done its job properly, only A who is in possession of the correct partial private key and user-generated secret could perform the decryption. Because there are no certificates, Al-Riymai and Paterson [**7**] were forced to consider a security model in which the adversary is allowed to replace the public keys of entities at will. The security of the scheme then rests on the attacker not knowing the partial private keys. Security against the KGC is also modelled in [**7**], by considering an adversary who knows the master secret s for the scheme, but who is trusted not to replace the public keys of entities. The security of the encryption scheme in [**7**] rests on the hardness of a new problem generalising the BDH problem:

Generalised bilinear-Diffie–Hellman problem (GBDH problem): Given P, $P_1 = [a]P$, $P_2 = [b]P$ and $P_3 = [c]P$ in G_1 with a, b and c selected uniformly at random from $\mathbb{Z}_r^*$, output a pair

$$Q, \quad \hat{e}(P, Q)^{abc}$$

where $Q \in G_1$.

Al-Riyami and Paterson [**7**] also present certificateless signature, key exchange and hierarchical schemes. These are obtained by adapting schemes of [**149, 286, 135**]. CL-PKC supports the temporal re-ordering of public and private key generation in the same way that ID-PKC does, thus it can be used to support workflows of the type discussed in Section X.7.1.2.

CL-PKC combines elements from ID-PKC and traditional PKI. On the one hand the schemes are no longer identity-based: they involve the use of A's public key which is no longer simply derived from A's identity. On the other hand, CL-PKC avoids the key escrow inherent in ID-PKC by having user-specific private information involved in the key generation process. CL-PKC does not need certificates to generate trust in public keys; instead this trust is produced in an implicit way. This would appear to make CL-PKC ideal for systems where escrow is unacceptable, but where the full weight of PKI is untenable.

There is a close relationship between the ideas in [**134**] and [**7**]. It is possible to convert CL-PKE scheme into a CBE scheme: if A's identity in the CL-PKE scheme is extended to include a time period along with the public key, then the CL-PKE scheme effectively becomes a CBE scheme. On the other hand, if one omits certain fields from the certificates in a CBE scheme, one obtains an encryption scheme that is functionally similar to a CL-PKE scheme. Differences do remain: in the strength and scope of the two security models developed in [**134**] and [**7**], as well as in the technical details of the schemes' realizations.

X.7.3. Applications and Implementations. In this section, we provide brief notes on recent work putting pairings into practice or using pairings in the broader context of Information Security.

A number of authors have examined how pairings can be put to use to enhance network security. Kempf *et al.* [**182**] described a lightweight protocol for securing certain aspects of IPv6. The protocol adds identity-based signatures to router and neighbour advertisements, with identities being based on IP addresses. Khalili *et al.* [**183**] combined identity-based techniques with threshold cryptography to build a key distribution mechanism suitable for use in ad hoc networks.

Appenzeller and Lynn [**9**] proposed using the NIKDS of Sakai *et al.* [**260**] to produce identity-based keys for securing IP packets between hosts. Their approach adds security while avoiding the introduction of state at the network layer, and so provides an attractive alternative to IPSec. However, it can only be used by pairs of entities who share a common TA. On the other hand, Smetters and Durfee [**289**] proposed a system in which each DNS domain runs its own IBE scheme and is responsible for distributing private keys to each of its hosts (or e-mail users). Inter-domain IPSec key exchanges and e-mail security are enabled by extending DNS to give a mechanism for distributing IBE scheme parameters. In [**289**], a protocol of [**66**] is used to provide an alternative to IKE (IPSec Key Exchange) for inter-domain exchanges, while the NIKDS of Sakai *et al.* [**260**] can be used to set up IKE in pre-shared key mode for intra-domain communications. The protocol resulting in the latter case in [**289**] is similar to a protocol proven secure in [**44**].

Dalton [**90**] described the particular computing and trust challenges faced in the UK's National Health Service, and studied the applicability of identity-based techniques in that environment.

Waters *et al.* [**314**] modified the IBE scheme of Boneh and Franklin [**37**] to provide a solution to the problem of searching through an encrypted, sensitive audit log. In the scheme of [**314**], a machine attaches a set of IBE-encrypted tags to each entry in its log, each tag corresponding to a single keyword W. The "identity" used in the encryption to produce a tag is the string W, while the plaintext encrypted is the symmetric key that was used to encrypt the entry in the log (plus some redundancy allowing the plaintext to be recognised). The TA for the IBE system acts as an audit escrow agent: when an entity requests the capability to obtain log entries containing a particular keyword, the TA may provide the private key $[s]H_1(W)$ matching that keyword. Now the testing entity can simply try to decrypt each tag for the log entry. When the correct tag is decrypted, a key allowing the entry to be decrypted results. A more theoretical and formal approach to the related problem of searchable public key encryption (SPKE) can be found in [**35**]. One of the three constructions for an SPKE scheme in [**35**] is based on pairings, specifically, it is again an adaptation of the IBE scheme of Boneh and Franklin.

Currently, we know of at least one company, Voltage Security, who are actively developing and marketing identity-based security systems. Their products include secure e-mail and file encryption applications. An early identity-based secure e-mail demonstrator, implementing Boneh and Franklin's IBE scheme, is still available from

`http://crypto.stanford.edu/ibe/download.html`

at the time of writing. Routines for Weil and Tate pairing computations are built into a number of software libraries, including Magma.

X.8. Concluding Remarks

We have seen in this chapter how pairings have been used to build some entirely new cryptographic schemes and to find more efficient instantiations of existing primitives. Although we have not been exhaustive in our coverage, we trust that the breathless pace of research in the area is apparent. What might the future hold for this subject, and what are the most important questions yet to be tackled?

The techniques and ideas used in pairing-based cryptography are very new, so it is hard to envisage where they will be taken next. The applications in topics like intrusion-resilient encryption and cryptographic workflows are so surprising (at least to the author) that accurately predicting an answer to the first question seems fraught. One might expect the rate of publication of new pairing-based schemes to slow a little, and a period of consolidation to occur. On a more theoretical note, the subject is rife with random oracles and inefficient reductions. Removing these whilst keeping the full strength of the security models and obtaining practical schemes should keep cryptographers busy.

We suggest that much more work above and below the purely cryptographic level is needed.

As Section X.7.3 illustrates, techniques from pairing-based cryptography are beginning to have an effect on other domains of Information Security. Attempts at commercialisation will provide a true test of the applicability of what, on paper, seem like very neat ideas. Identity-based cryptography is certainly interesting, but it still has much to prove when measured against traditional PKIs. One topic we have not addressed here is that of intellectual property and patents. This may become a major factor in the take-up of the technology, in the same way that it was for elliptic curve cryptography in the last decade, and public key cryptography before that.

Below the cryptographic level, more work on the fundamental question of understanding the hardness of the BDH problem (and the associated decisional problem) seems essential. While the relationships to the CDH problem and other problems in related groups are well understood, this is of course not the whole story. Pairings also give new relevance to "old" problems, for example, evaluating the performance of discrete logarithm algorithms in fields of small characteristic for concrete parameters. One might also worry about relying too much on the extremely narrow class of supersingular curves for constructing pairings. This is akin to the days before point counting for curves of cryptographic sizes became routine, when CM curves were suggested as a way of proceeding. It is interesting to note that recent constructions for curves with prescribed embedding degrees (as described in Chapter IX) also rely on CM methods, while it is known that the embedding degree of a random curve of a particular size will be very high. The challenge to computational number theorists is evident.

Bibliography

[ECC] I.F. Blake, G. Seroussi and N.P. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 1999.

[EP] IACR e-print archive. Available from `http://eprint.iacr.org/`.

[A-1] L. Adleman and M.-D. Huang, editors. *ANTS-1: Algorithmic Number Theory.* Springer-Verlag, LNCS 877, 1994.

[A-2] H. Cohen, editor. *ANTS-2: Algorithmic Number Theory.* Springer-Verlag, LNCS 1122, 1996.

[A-3] J. P. Buhler, editor. *ANTS-3: Algorithmic Number Theory.* Springer-Verlag, LNCS 1423, 1998.

[A-4] W. Bosma, editor. *ANTS-4: Algorithmic Number Theory.* Springer-Verlag, LNCS 1838, 2000.

[A-5] C. Fieker and D.R. Kohel, editors. *ANTS-5: Algorithmic Number Theory.* Springer-Verlag, LNCS 2369, 2002.

[A98] K. Ohta and D. Pei, editors. *Advances in Cryptology – ASIACRYPT '98.* Springer-Verlag, LNCS 1514, 1998.

[A99] K.Y. Lam, E. Okamoto and C. Xing, editors. *Advances in Cryptology – ASIACRYPT '99.* Springer-Verlag, LNCS 1716, 1999.

[A00] T. Okamoto, editor. *Advances in Cryptology – ASIACRYPT 2000.* Springer-Verlag, LNCS 1976, 2000.

[A01] C. Boyd, editor. *Advances in Cryptology – ASIACRYPT 2001.* Springer-Verlag, LNCS 2248, 2001.

[A02] Y. Zheng, editor. *Advances in Cryptology – ASIACRYPT 2002.* Springer-Verlag, LNCS 2501, 2002.

[A03] C.S. Laih, editor. *Advances in Cryptology – ASIACRYPT 2003.* Springer-Verlag, LNCS 2894, 2003.

[C84] G.R. Blakley and D. Chaum, editors. *Advances in Cryptology – CRYPTO '84.* Springer-Verlag, LNCS 196, 1985.

[C89] G. Brassard, editor. *Advances in Cryptology – CRYPTO '89.* Springer-Verlag, LNCS 435, 1990.

[C91] J. Feigenbaum, editor. *Advances in Cryptology – CRYPTO '91.* Springer-Verlag, LNCS 576, 1992.

[C92] E.F. Brickell, editor. *Advances in Cryptology – CRYPTO '92.* Springer-Verlag, LNCS 740, 1993.

[C93] D. Stinson, editor. *Advances in Cryptology – CRYPTO '93.* Springer-Verlag, LNCS 773, 1993.

[C96] N. Koblitz, editor. *Advances in Cryptology – CRYPTO '96.* Springer-Verlag, LNCS 1109, 1996.

[C97] B.S. Kaliski Jr., editor. *Advances in Cryptology – CRYPTO '97.* Springer-Verlag, LNCS 1294, 1997.

[C98] H. Krawczyk, editor. *Advances in Cryptology – CRYPTO '98.* Springer-Verlag, LNCS 1462, 1998.

[C99] M. Wiener, editor. *Advances in Cryptology – CRYPTO '99*. Springer-Verlag, LNCS 1666, 1999.

[C00] M. Bellare, editor. *Advances in Cryptology – CRYPTO 2000*. Springer-Verlag, LNCS 1880, 2000.

[C01] J. Kilian, editor. *Advances in Cryptology – CRYPTO 2001*. Springer-Verlag, LNCS 2139, 2001.

[C02] M. Yung, editor. *Advances in Cryptology – CRYPTO 2002*. Springer-Verlag, LNCS 2442, 2002.

[C03] D. Boneh, editor. *Advances in Cryptology – CRYPTO 2003*. Springer-Verlag, LNCS 2729, 2003.

[CH99] Ç.K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems – CHES '99*. Springer-Verlag, LNCS 1717, 1999.

[CH00] Ç.K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems – CHES 2000*. Springer-Verlag, LNCS 1965, 2000.

[CH01] Ç.K. Koç, D. Naccache and C. Paar, editors. *Cryptographic Hardware and Embedded Systems – CHES 2001*. Springer-Verlag, LNCS 2162, 2001.

[CH02] B.S. Kaliski Jr., Ç.K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems – CHES 2002*. Springer-Verlag, LNCS 2523, 2003.

[CH03] C.D. Walter, Ç.K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems – CHES 2003*. Springer-Verlag, LNCS 2779, 2003.

[E90] I.B. Damgård, editor. *Advances in Cryptology – EUROCRYPT '90*. Springer-Verlag, LNCS 473, 1990.

[E94] A. De Santis, editor. *Advances in Cryptology – EUROCRYPT '94*. Springer-Verlag, LNCS 950, 1994.

[E97] W. Fumy, editor. *Advances in Cryptology – EUROCRYPT '97*. Springer-Verlag, LNCS 1233, 1997.

[E00] B. Preneel, editor. *Advances in Cryptology – EUROCRYPT 2000*. Springer-Verlag, LNCS 1807, 2000.

[E01] B. Pfitzmann, editor. *Advances in Cryptology – EUROCRYPT 2001*. Springer-Verlag, LNCS 2045, 2001.

[E02] L. Knudsen, editor. *Advances in Cryptology – EUROCRYPT 2002*. Springer-Verlag, LNCS 2332, 2002.

[E03] E. Biham, editor. *Advances in Cryptology – EUROCRYPT 2003*. Springer-Verlag, LNCS 2656, 2003.

[P01] K. Kim, editor. *Public Key Cryptography – PKC 2001*. Springer-Verlag, LNCS 1992, 2001.

[P02] D. Naccache and P. Paillier, editors. *Public Key Cryptography – PKC 2002*. Springer-Verlag, LNCS 2274, 2002.

[P03] Y.G. Desmedt, editor. *Public Key Cryptography – PKC 2003*. Springer-Verlag, LNCS 2567, 2003.

[ANSI X9.62] ANSI X9.62. *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standards Institute, 1999.

[ANSI X9.63] ANSI X9.63. *Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Transport Protocols*. American National Standards Institute, 2001. Draft.

[EU 1999] EU Directive 1999/93/EC of the European Parliament and of the Council. *On a community framework for electronic signatures*, December 1999.

[FIPS 140.1] FIPS PUB 140-1. *Security requirements for cryptographic modules*. National Institute for Standards and Technology, 1994.

[FIPS 180.1] FIPS PUB 180-1. *Secure Hash Standard*. National Institute for Standards and Technology, 1995.

[FIPS 180.2] FIPS PUB 180-2. *Secure Hash Standard*. National Institute for Standards and Technology, 2001.

[FIPS 186] FIPS PUB 186. *Digital Signature Standard (DSS)*. National Institute for Standards and Technology, 1994.

[FIPS 186.2] FIPS PUB 186-2. *Digital Signature Standard (DSS)*. National Institute for Standards and Technology, 2000.

[IBM CoPro] IBM Corporation. *IBM PCI Cryptographic Coprocessor–General Information Manual*, 6th ed., 2002.

[IEEE 1363] IEEE 1363. *Standard Specifications for Public Key Cryptography*. IEEE, 2000.

[ISO 15946-2] ISO X9.62. *International Standard 15946-2: Information Technology — Security Techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital Signatures*. International Standards Organization, 2000.

[NESSIE] NESSIE. *Security Evaluation Report*. NESSIE, 2002.

[RFC 2412] IETF. *The Oakley Key Determination Protocol*, 1998.

[RFC 3278] IETF. *The Use of Elliptic Curve Cryptography in the Cryptographic Message Syntax*, 2001.

[SECG] SEC 1. *Elliptic Curve Cryptography*. Standards for Efficient Cryptography Group, 1999.

[1] M. Abdalla, M. Bellare and P. Rogaway. DHAES: An encryption scheme based on the Diffie-Hellman problem. Submission to *P1363a: Standard Specifications for Public-Key Cryptography, Additional Techniques*, 2000.

[2] L.M. Adleman. The function field sieve. In [**A-1**], 108–121.

[3] L.M. Adleman and M.-D. Huang. Function field sieve method for discrete logarithms over finite fields. *Information and Computation*, **151**, 5–16, 1999.

[4] L.M. Adleman, J. DeMarrais and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In [**A-1**], 28–40.

[5] D. Agrawal, B. Archambeault, J.R. Rao and P. Rohatgi. The EM side-channel(s). In [**CH02**], 29–45.

[6] S.S. Al-Riyami and K.G. Paterson. Authenticated three party key agreement protocols from pairings. In K.G. Paterson, editor, *Cryptography and Coding*, LNCS 2898, 332–359. Springer-Verlag, 2003.

[7] S.S. Al-Riyami and K.G. Paterson. Certificateless public key cryptography. In [**A03**], 452–473.

[8] M.-L. Akkar and C. Giraud. An implementation of DES and AES secure against some attacks. In [**CH01**], 309–318.

[9] G. Appenzeller and B. Lynn. Minimal-overhead IP security using identity-based encryption. Submitted.

[10] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. *Series of e-mails to the* `NMBRTHRY` *mailing list*, 1992.

[11] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *J. Cryptology*, **11**, 141–145, 1998.

[12] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon and H.-C. Wong. Secret handshakes from pairing-based key agreements. In *Proceedings IEEE Symposium on Security and Privacy*, 180–196. IEEE Press, 2003.

[13] R. Barua, R. Dutta and P. Sarkar. Extending Joux's protocol to multi party key agreement. In T. Johansson and S. Maitra, editors, *INDOCRYPT 2003*, LNCS 2551, 205–217. Springer-Verlag, 2003.

[14] P. Barreto. The pairing-based crypto lounge. http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html.

[15] P.S.L.M. Barreto, H.Y. Kim, B. Lynn and M. Scott. Efficient algorithms for pairing-based cryptosystems. In [**C02**], 354–368.

[16] P.S.L.M. Barreto, B. Lynn and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In S. Cimato, C. Galdi and G. Persiano, editors, *Security in Communication Networks (SCN 2002)*, LNCS 2576, 257–267. Springer-Verlag, 2002.

[17] P.S.L.M. Barreto, B. Lynn and M. Scott. Efficient algorithms. Preprint (for J. Cryptology).

[18] M. Bellare, A. Desai, E. Jokipii and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proc. of the 38th Symposium on Foundations of Computer Science*, IEEE, 1997.

[19] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. Relations among notions of security for public-key encryption schemes. In [**C98**], 26–45.

[20] M. Bellare, S. Goldwasser and D. Micciancio. "Pseudo-Random" number generation within cryptographic algorithms: The DSS case. In [**E97**], 277–291.

[21] M. Bellare, R. Canetti and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In *Proceedings of the 30th Annual Symposium on the Theory of Computing*, 419–428. ACM, 1998.

[22] M. Bellare and A. Palacio. Protecting against key exposure: strongly key-insulated encryption with optimal threshold. See [**EP**], # 2002/064, 2002.

[23] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. of the First ACM Conference on Computer and Communications Security*, 62–73, 1993.

[24] M. Bellare and P. Rogaway. Entity authentication and key distribution. In [**C93**], 232–249.

[25] I. Biehl, B. Meyer and V. Müller. Differential fault attacks on elliptic curve cryptosystems. In [**C00**], 131–146.

[26] O. Billet and M. Joye. The Jacobi model of an elliptic curve and side-channel analysis. In M. Fossorier, T. Høholdt and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LNCS 2643, 34–42. Springer-Verlag, 2003.

[27] S. Blake-Wilson, D. Johnson and A. Menezes. Key agreement protocols and their security analysis. In *Cryptography and Coding*, LNCS 1355, 30–45. Springer-Verlag, 1997.

[28] S. Blake-Wilson and A. Menezes. Security proofs for entity authentication and authenticated key transport protocols employing asymmetric techniques. In B. Christianson, B. Crispo, T. Lomas and M. Roe, editors, *Proceedings of the 5th International Workshop on Security Protocols*, LNCS 1361, 137–158. Springer-Verlag, 1997.

[29] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In [**C98**], 1–12.

[30] D. Bleichenbacher. On the generation of DSS one-time keys. Preprint, 2001.

[31] A. Boldyreva. Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature scheme. In [**P03**], 31–46.

[32] A. Boldyreva, A. Palacio and B. Warinschi. Secure proxy signature schemes for delegation of signing rights. See [**EP**], # 2003/096, 2003.

[33] D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. Advances in Cryptology – EUROCRYPT 2004, to appear, 2004.

[34] D. Boneh and X. Boyen. Short signatures without random oracles. Advances in Cryptology – EUROCRYPT 2004, to appear, 2004.

[35] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano. Searchable public key encryption. See [**EP**], # 2003/195, 2003.

[36] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In [**C01**], 213–229.

[37] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM J. Comp.*, **32**, 586–615, 2003.

[38] D. Boneh, C. Gentry, B. Lynn and H. Shacham. Aggregate and verfiably encrypted signatures from bilinear maps. In [**E03**], 416–432.

[39] D. Boneh, A. Joux and P. Nguyen. Why textbook ElGamal and RSA encryption are insecure. In [**A00**], 30–43.

[40] D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. In [**A01**], 514–532.

[41] D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. Technical report, 2003. Revised version of [**40**], available from `http://crypto.stanford.edu/ dabo/abstracts/weilsigs.html`.

[42] D. Boneh, I. Mironov and V. Shoup. Provably secure signature scheme from bilinear mapping. In M. Joye, editor, *Topics in Cryptology – CT-RSA 2003*, LNCS 2612, 98–110. Springer-Verlag, 2003.

[43] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comp.*, **24, 3/4**, 235–265, 1997.

[44] C. Boyd, W. Mao and K.G. Paterson. Deniable authenticated key establishment for Internet protocols. In *Proceedings of 11th International Workshop on Security Protocols*, LNCS XXXX. Springer-Verlag, to appear.

[45] X. Boyen. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In [**C03**], 382–398.

[46] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. See [**EP**], # 2003/143, 2003.

[47] É. Brier, I. Déchène and M. Joye. Unified addition formulæ for elliptic curve cryptosystems. *International Journal of Computer Research*, To appear.

[48] É. Brier and M. Joye. Weierstraß elliptic curves and side-channel attacks. In [**P02**], 335–345.

[49] D.R.L. Brown. Generic groups, collision resistance and ECDSA. See [**EP**], # 2002/026, 2002.

[50] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In [**E94**], 267–275.

[51] R. Canetti, O. Goldreich and S. Halevi. The random oracle model, revisited. In *Proc. of the 30th Annual ACM Symposium on the Theory of Computing*, 209–218, 1998.

[52] R. Canetti, S. Halevi and J. Katz. A forward-secure public-key encryption scheme. In [**E03**], 255–271.

[53] R. Canetti, S. Halevi and J. Katz. Chosen-ciphertext security from identity-based encryption. See [**EP**], # 2003/182, 2003.

[54] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In [**E01**], 453–474.

[55] R. Canetti, H. Krawczyk and J.B. Nielsen. Relaxing chosen-ciphertext security. In [**C03**], 565–582.

[56] D.G. Cantor. Computing in the Jacobian of an hyperelliptic curve. *Math. Comp.*, **48**, 95–101, 1987.

[57] J. Cathalo, F. Koeune and J.-J. Quisquater. A new type of timing attack: Application to GPS. In [**CH03**], 291–303.

[58] J.C. Cha and J.H. Cheon. An identity-based signature from gap Diffie–Hellman groups. In [**P03**], 18–30. See also Cryptology ePrint Archive, Report 2002/018.

[59] L. S. Charlap and R. Coley. An elementary introduction to elliptic curves ii. Institute for Defense Analysis, CCR Expository Report 34, 1990.

[60] S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi. Towards sound approaches to counteract power-analysis attacks. In [**C99**], 398–412.

[61] D. Chaum. Security without identification: Transaction systems to make Big Brother obsolete. *Comm. ACM*, **28**, 1030–1044, 1985.

[62] D. Chaum. Zero-knowledge undeniable signatures. In [**E90**], 458–464.

[63] D. Chaum and H. van Antwerpen. Undeniable signatures. In [**C89**], 212–216.

[64] L. Chen, K. Harrison, A. Moss, D. Soldera and N.P. Smart. Certification of public keys within an identity based system. In A. H. Chan and V. D. Gligor, editors, *Information Security, 5th International Conference, ISC*, LNCS 2433, 322–333. Springer-Verlag, 2002.

[65] L. Chen, K. Harrison, D. Soldera and N.P. Smart. Applications of multiple trust authorities in pairing based cryptosystems. In G. I. Davida, Y. Frankel and O. Rees, editors, *Infrastructure Security, International Conference, InfraSec*, LNCS 2437, 260–275. Springer-Verlag, 2002.

[66] L. Chen and C. Kudla. Identity based authenticated key agreement protocols from pairings. See [**EP**], # 2002/184, 2002.

[67] L. Chen and C. Kudla. Identity based authenticated key agreement protocols from pairings. In *IEEE Computer Security Foundations Workshop*, 219–233. IEEE Computer Society Press, 2003.

[68] L. Chen and J. Malone-Lee. Improved identity-based signcryption. Preprint, 2004.

[69] X. Chen, F. Zhang and K. Kim. A new ID-based group signature scheme from bilinear pairings. See [**EP**], # 2003/116, 2003.

[70] Z. Chen. Security analysis of Nalla-Reddy's ID-based tripartite authenticated key agreement protocols. See [**EP**], # 2003/103, 2003.

[71] J.H. Cheon. A universal forgery of Hess's second ID-based signature against the known-message attack. See [**EP**], # 2002/028, 2002.

[72] B. Chevallier-Mames, M. Ciet and M. Joye. Low-cost solutions for preventing simple side-channel analysis: Side-channel atomicity. *IEEE Trans. Computers*, To appear.

[73] D.V. Chudnovsky and G.V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. Applied Math.*, **7**, 385–434, 1987.

[74] M. Ciet and M. Joye. Elliptic curve cryptosystems in the presence of permanent and transient faults. *Designs, Codes and Cryptography*, To appear.

[75] M. Ciet, J.-J. Quisquater and F. Sica. Preventing differential analysis in GLV elliptic curve scalar multiplication. In [**CH02**], 540–550.

[76] M. Ciet, J.-J. Quisquater and F. Sica. A secure family of composite finite fields suitable for fast implementation of elliptic curve cryptography. In C. Pandu Rangan and C. Ding, editors, *Progress in Cryptology – INDOCRYPT 2001*, LNCS 2247, 108–116. Springer-Verlag, 2001.

[77] C. Clavier, J.-S. Coron and N. Dabbous. Differential power analysis in the presence of hardware countermeasures. In [**CH00**], 252–263.

[78] C. Clavier and M. Joye. Universal exponentiation algorithm: A first step towards provable SPA-resistance. In [**CH01**], 300–308.

[79] C. Cocks. An identity based encryption scheme based on quadratic residues. In B. Honary, editor, *Cryptography and Coding*, LNCS 2260, 360–363. Springer-Verlag, 2001.

[80] C. Cocks and R.G.E. Pinch. ID-based cryptosystems based on the Weil pairing. Unpublished manuscript, 2001.

[81] H. Cohen, A. Miyaji and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. In [**A98**], 51–65.

[82] D. Coppersmith. Fast evaluation of logarithms in fields of characteristic 2. *IEEE Trans. Inf. Theory*, **30**, 587–594, 1984.

[83] J.-S. Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In [**CH99**], 292–302.

[84] J.-S. Coron and L. Goubin. On Boolean and arithmetic masking against differential power analysis. In [**CH00**], 231–237.

[85] J.-S. Coron and D. Naccache. Boneh *et al.*'s k-element aggregate extraction assumption is equivalent to the Diffie-Hellman assumption. In [**A03**], 392–397.

[86] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. PhD thesis, Université de Bordeaux, 1994.

[87] J.-M. Couveignes. Computing l-isogenies with the p-torsion. In [**A-2**], 59–65.

[88] J.-M. Couveignes. Algebraic groups and discrete logarithms. In *Public Key Cryptography and Computational Number Theory*, 17–27, Warsaw (2000). Walter de Gruyter, 2001.

[89] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. Available from `http://shoup.net/`, 2002.

[90] C.R. Dalton. The NHS as a proving ground for cryptosystems. *Information Security Technical Report*, **8**(3), 73–88, 2003.

[91] B. den Boer, K. Lemke and G. Wicke. A DPA attack against the modular reduction within a CRT implementation of RSA. In [**CH02**], 228–234.

[92] A.W. Dent. An evaluation of EPOC-2. NESSIE, Public report, 2001.

[93] A.W. Dent. Adapting the weaknesses of the random oracle model to the generic group model. In [**A02**], 100–109.

[94] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, **14**, 197–272, 1941.

[95] E. De Win, S. Mister, B. Preneel and M. Wiener. On the performance of signature schemes based on elliptic curves. In [**A-3**], 252–266.

[96] C. Diem. *A study on theoretical and practical aspects of Weil-restrictions of varieties*. PhD thesis, Universtität-Gesamthochschule Essen, 2001.

[97] C. Diem. The GHS-attack in odd characteristic. *J. Ramanujan Math. Soc.*, **18**(1), 2002.

[98] C. Diem. Private communication, 2003.

[99] C. Diem and N. Naumann. On the structure of Weil restrictions of abelian varieties. *J. Ramanujan Math. Soc.*, **18**, 2003.

[100] Y. Dodis, M. Franklin, J. Katz, A. Miyaji and M. Yung. Intrusion-resilient public-key encryption. In M. Joye, editor, *Topics in Cryptology – CT-RSA 2003*, LNCS 2612, 19–32. Springer-Verlag, 2003.

[101] R. Dupont and A. Enge. Practical non-interactive key distribution based on pairings. See [**EP**], # 2002/136, 2002.

[102] R. Dupont, A. Enge and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. See [**EP**], # 2002/094, 2002.

[103] I.M. Duursma. Class numbers for some hyperelliptic curves. In R. Pellikaan, M. Perret and S.G. Vladut, editors, *Arithmetic, Geometry and Coding Theory*, 45–52. Walter de Gruyter, 1996.

[104] I.M. Duursma, P. Gaudry and F. Morain. Speeding up the discrete log computation on curves with automorphisms. In [**A99**], 103–121.

[105] I.M. Duursma and H.-S. Lee. Tate-pairing implementations for tripartite key agreement. See [**EP**], # 2003/053, 2003.

[106] K. Eisenträger, K. Lauter and P.L. Montgomery. Fast elliptic curve arithmetic and improved Weil pairing evaluation. In M. Joye, editor, *Topics in Cryptology – CT-RSA 2003*, LNCS 2612, 343–354. Springer-Verlag, 2003.

[107] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory*, 21–76, 1998.

[108] A. Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Math. Comp.*, **71**, 729–742, 2002.

[109] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arith.*, **102**, 83–103, 2002.

[110] A. Enge and A. Stein. Smooth ideals in hyperelliptic function fields. *Math. Comp.*, **71**, 1219–1230, 2002.

[111] P. Fahn and P. Pearson. IPA: A new class of power attacks. In [**CH99**], 173–186.

[112] W. Fischer, C. Giraud, E.W. Knudsen and J.-P. Seifert. Parallel scalar multiplication on general elliptic curves over $\mathbb{F}_p$ hedged against non-differential side-channel attacks. See [**EP**], # 2002/007, 2002.

[113] R. Flassenberg and S. Paulus. Sieving in function fields. *Experiment. Math.*, **8**, 339–349, 1999.

[114] P.-A. Fouque and F. Valette. The doubling attack – Why upwards is better than downwards. In [**CH03**], 269–280.

[115] M. Fouquet, P. Gaudry and R. Harley. On Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, **15**, 281–318, 2000.

[116] G. Frey. How to disguise an elliptic curve. Talk at ECC' 98, Waterloo, 1998.

[117] G. Frey, M. Müller and H.-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inf. Theory*, **45**, 1717–1719, 1999.

[118] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, **62**, 865–874, 1994.

[119] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In [**C99**], 537–554.

[120] S. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, **2**, 118–138, 1999.

[121] S.D. Galbraith. Supersingular curves in cryptography. In [**A01**], 495–513.

[122] S.D. Galbraith, K. Harrison and D. Soldera. Implementing the Tate pairing. In [**A-5**], 324–337.

[123] S. Galbraith, F. Hess and N.P. Smart. Extending the GHS Weil descent attack. In [**E02**], 29–44.

[124] S.D. Galbraith, H.J. Hopkins and I.E. Shparlinski. Secure Bilinear Diffie-Hellman bits. See [**EP**], # 2002/155, 2002.

[125] S. Galbraith and J. McKee. The probability that the number of points on an elliptic curve over a finite field is prime. *J. London Math. Soc.*, **62**, 671–684, 2000.

[126] S. Galbraith and N.P. Smart. A cryptographic application of Weil descent. In M. Walker, editor, *Cryptography and Coding*, LNCS 1746, 191–200. Springer-Verlag, 1999.

[127] R. Gallant, R. Lambert and S. Vanstone. Improving the parallelized Pollard lambda search on binary anomalous curves. *Math. Comp.*, **69**, 1699–1705, 2000.

[128] K. Gandolfi, C. Mourtel and F. Olivier. Electromagnetic analysis: Concrete results. In [**CH01**], 251–261.

[129] T. Garefalakis. The generalised Weil pairing and the discrete logarithm problem on elliptic curves. In S. Rajsbaum, editor, *LATIN 2002: Theoretical Informatics*, LNCS 2286, 118–130. Springer-Verlag, 2002.

[130] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, 1999.

[131] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In [**E00**], 19–34.

[132] P. Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In [**A02**], 311–327.

[133] P. Gaudry, F. Hess and N.P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, **15**, 19–46, 2002.

[134] C. Gentry. Certificate-based encryption and the certificate revocation problem. In [**E03**], 272–293.

[135] C. Gentry and A. Silverberg. Heirarchical ID-based cryptography. In [**A02**], 548–566.

[136] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Science*, **28**, 270–299, 1984.

[137] S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comp.*, **17**, 281–308, 1988.

[138] L. Goubin. A refined power-analysis attack on elliptic curve cryptosystems. In [**P03**], 199–210.

[139] L. Goubin and J. Patarin. DES and differential power analysis – The duplication method. In [**CH99**], 158–172.

[140] L. Granboulan. RSA hybrid encryption schemes. Available from `http://www.di.ens.fr/~granboul/recherche/publications/abs-2001-RSAenc.html`, 2001.

[141] R. Granger. Estimates for discrete logarithm computations in finite fields. In K.G. Paterson, editor, *Cryptography and Coding*, LNCS 2898, 190–206. Springer-Verlag, 2003.

[142] G. Grimmett and D. Stirzaker. *Probability and Random Processes*. Oxford University Press, 2nd ed., 1992.

[143] J. Ha and S. Moon. Randomized signed-scalar multiplication of ECC to resist power attacks. In [**CH02**], 551–563.

[144] H. Handschuh, P. Paillier and J. Stern. Probing attacks on tamper-resistant devices. In [**CH99**], 303–315.

[145] R. Harley. Asymptotically optimal p-adic point-counting. e-mail to NMBRTHRY list, December 2002.

[146] M.A. Hasan. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz cryptosystems. In [**CH00**], 93–108.

[147] J. Herranz and G. Sáez. A provably secure ID-based ring signature scheme. See [**EP**], # 2003/261, 2003.

[148] F. Hess. Exponent group signature schemes and efficient identity based signature schemes based on pairings. See [**EP**], # 2002/012, 2002.

[149] F. Hess. Efficient identity based signature schemes based on pairings. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography – SAC 2002*, LNCS 2595, 310–324. Springer-Verlag, 2003.

[150] F. Hess. The GHS attack revisited. In [**E03**], 374–387.

[151] F. Hess. On the security of the verifiably-encrypted signature scheme of Boneh, Gentry, Lynn and Shacham. *Information Processing Letters*, **89**, 111–114, 2004.

[152] F. Hess. The GHS attack revisited. *LMS Journal of Computation and Mathematics*, To appear.

[153] F. Hess. Computing relations in divisor class groups of algebraic curves over finite fields. Submitted, 2003.

[154] F. Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math.*, To appear.

[155] Y. Hitchcock and P. Montague. A new elliptic curve scalar multiplication algorithm to resist simple power analysis. In L.M. Batten and J. Seberry, editors, *Information Security and Privacy (ACISP 2002)*, LNCS 2384, 214–225. Springer-Verlag, 2002.

[156] J. Horowitz and B. Lynn. Toward hierarchical identity-based encryption. In [**E02**], 466–481.

[157] E. W. Howe. The Weil pairing and the Hilbert symbol. *Math. Ann.*, **305**, 387–392, 1996.

[158] N. Howgrave-Graham and N.P. Smart. Lattice attacks on digital signature schemes. *Designs, Codes and Cryptography*, **23**, 283–290, 2001.

[159] K. Itoh, T. Izu and M. Takaneka. Address-bit differential power analysis of cryptographic schemes OK-ECDH and OK-ECDSA. In [**CH02**], 129–143.

[160] K. Itoh, T. Izu and M. Takaneka. A practical countermeasure against address-bit differential power analysis. In [**CH03**], 382–396.

[161] K. Itoh, J. Yajima, M. Takaneka and N. Torii. DPA countermeasures by improving the window method. In [**CH02**], 303–317.

[162] T. Izu and T. Takagi. A fast parallel elliptic curve multiplication resistant against side channel attacks. In [**P02**], 280–296.

[163] T. Izu and T. Takagi. Exceptional procedure attack on elliptic curve cryptosystems. In [**P03**], 224–239.

[164] T. Izu and T. Takagi. Efficient computations of the Tate pairing for the large MOV degrees. In P.J. Lee and C.H. Lim, editors, *Information Security and Cryptology – ICISC 2002*, LNCS 2587, 283–297. Springer-Verlag, 2003.

[165] M. Jacobson, A. Menezes and A. Stein. Solving elliptic curve discrete logarithm problems using Weil descent. *J. Ramanujan Math. Soc.*, **16**, 231–260, 2001.

[166] M. Jacobson and A. van der Poorten. Computational aspects of NUCOMP. In [**A-5**], 120–133.

[167] A. Joux. A one round protocol for tripartite diffie–hellman. In [**A-4**], 385–394.

[168] A. Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. In [**A-5**], 20–32.

[169] A. Joux and R. Lercier. The function field sieve is quite special. In [**A-5**], 431–445.

[170] A. Joux and K. Nguyen. Separating Decision Diffie–Hellman from Diffie–Hellman in cryptographic groups. *J. Cryptology*, **16**, 239–248, 2003.

[171] M. Joye. Recovering lost efficiency of exponentiation algorithms on smart cards. *Electronics Letters*, **38**, 1095–1097, 2002.

[172] M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In [**CH01**], 402–410.

[173] M. Joye, J.-J. Quisquater and M. Yung. On the power of misbehaving adversaries and security analysis of the original EPOC. In D. Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, LNCS 2020, 208–222. Springer-Verlag, 2001.

[174] M. Joye and C. Tymen. Protections against differential analysis for elliptic curve cryptography: An algebraic approach. In [**CH01**], 377–390.

[175] M. Joye and S.-M. Yen. The Montgomery powering ladder. In [**CH02**], 291–302.

[176] B.G. Kang, J.H. Park and S.G. Hahn. A certificate-based signature scheme. In T. Okamoto, editor, *Topics in Cryptology – CT-RSA 2004*, LNCS 2964, 99–111. Springer-Verlag, 2004.

[177] Kant group. *Kash.* `http://www.math.tu-berlin.de/~kant`, 2003.

[178] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Doklady*, **7**, 595–596, 1963.

[179] C. Karlof and D. Wagner. Hidden Markov model cryptanalysis. In [**CH03**], 17–34.

[180] J. Katz. A forward secure public-key encryption scheme. See [**EP**], # 2002/060, 2002.

[181] K.S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, **16**, 323–338, 2001.

[182] J. Kempf, C. Gentry and A. Silverberg. Securing IPv6 neighbor discovery using address based keys (ABKs). Internet Draft Document, expired December 2002, 2002. Available from `http://www.docomolabs-usa.com/pdf/PS2003-080.pdf`.

[183] A. Khalili, J. Katz and W.A. Arbaugh. Toward secure key distribution in truly ad-hoc networks. In *Proceedings 2003 Symposium on Applications and the Internet Workshops (SAINT 2003).* IEEE Computer Society, 2003.

[184] H.Y. Kim, J.Y. Park, J.H. Cheon, J.H. Park, J.H. Kim. and S.G. Hahn. Fast elliptic curve point counting using Gaussian Normal Basis. In [**A-5**], 292–307.

[185] V. Klima and T. Rosa. Further results and considerations on side channel attacks on RSA. In [**CH02**], 244–259.

[186] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions.* Springer-Verlag, GTM 58, 1984.

[187] N. Koblitz. CM curves with good cryptographic properties. In [**C91**], 279–287.

[188] N. Koblitz. *Algebraic aspects of cryptography.* Springer-Verlag, 1997.

[189] H. Koch. *Algebraic Number Theory.* Springer-Verlag, 2nd ed., 1997.

[190] P.C. Kocher. Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. In [**C96**], 104–113.

[191] P.C. Kocher, J. Jaffe and B. Jun. Differential power analysis. In [**C99**], 388–397.

[192] D.R. Kohel and I.E. Shparlinski. On exponential sums and group generators for elliptic curves over finite fields. In [**A-4**], 395–404.

[193] S. Lang. *Algebra.* Addison-Wesley, 3rd ed., 1993.

[194] T. Lange. *Efficient arithmetic on hyperelliptic curves.* PhD thesis, Universität-Gesamthochschule Essen, 2001.

[195] T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves, 2003. Preprint.

[196] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone. An efficient protocol for authenticated key agreement. *Designs, Codes and Cryptography*, **28**, 119–134, 2003.

[197] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, École Polytechnique, 1997.

[198] R. Lercier and D. Lubicz. Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time. In [**E03**], 360–373.

[199] P.-Y. Liardet and N.P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In [**CH01**], 391–401.

[200] B. Libert and J.-J. Quisquater. New identity based signcryption schemes from pairings. See [**EP**], # 2003/023, 2003.

[201] B. Libert and J.-J. Quisquater. Identity based undeniable signatures. In T. Okamoto, editor, *Topics in Cryptology – CT-RSA 2004*, LNCS 2964, 112–125. Springer-Verlag, 2004.

[202] B. Libert and J.-J. Quisquater. Efficient signcryption with key privacy from gap Diffie-Hellman groups. In F. Bao, editor, *Public Key Cryptography – PKC 2004*, LNCS 2947, 187–200. Springer-Verlag, 2004.

[203] S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Inventiones Math.*, **7**, 120–136, 1969.

[204] J. López and R. Dahab. Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation. In [**CH99**], 316–327.

[205] D. Lorenzini. *An Invitation to Arithmetic Geometry.* AMS, Graduate Studies in Mathematics 106, 1993.

[206] J. Lubin, J.-P. Serre and J. Tate. Elliptic curves and formal groups. *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry*, Whitney Estate, Woods Hole, Massachusetts, 1964.

[207] B. Lynn. Authenticated identity-based encryption. See [**EP**], # 2002/072, 2002.

[208] Magma Comp. algebra group. *Magma.* Available from `http://www.maths.usyd.edu.au:8000/u/magma/`, 2003.

[209] J. Malone-Lee. Identity-based signcryption. See [**EP**], # 2002/098, 2002.

[210] J. Malone-Lee. Signcryption with non-interactive non-repudiation. Preprint, 2004.

[211] J. Manger. A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS # 1 v2.0. In [**C01**], 230–238.

[212] M. Maurer, A. Menezes and E. Teske. Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree. *LMS Journal of Computation and Mathematics*, **5**, 127–174, 2002.

[213] D. May, H.L. Muller and N.P. Smart. Random register renaming to foil DPA. In [**CH01**], 28–38.

[214] R. Mayer-Sommer. Smartly analyzing the simplicity and the power of simple power analysis on smartcards. In [**CH00**], 78–92.

[215] A. Miyaji, T. Ono and H. Cohen. Efficient elliptic curve exponentiation. In Y. Han, T. Okamoto and S. Qing, editors, *Information and Communications Security (ICICS '97)*, LNCS 1334, 282–290. Springer-Verlag, 1997.

[216] W. Meier and O. Staffelbach. Efficient multiplication on certain non-supersingular elliptic curves. In [**C92**], 333–344.

[217] A.J. Menezes, T. Okamoto and S.A. Vanstone. Reducing elliptic curve logarithms to a finite field. *IEEE Trans. Inf. Theory*, **39**, 1639–1646, 1993.

[218] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[219] A. Menezes and M. Qu. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In D. Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, LNCS 2020, 308–318. Springer-Verlag, 2001.

[220] A. Menezes, E. Teske and A. Weng. Weak fields for ECC. In T. Okamoto, editor, *Topics in Cryptology – CT-RSA 2004*, LNCS. Springer-Verlag, To appear.

[221] A. Menezes, Y.-H. Wu and R. Zuccherato. An elementary introduction to hyperelliptic curves. In [**188**], 155-178.

[222] T.S. Messerges. Using second-order power analysis to attack DPA resistant software. In [**CH00**], 238–251.

[223] T.S. Messerges, E.A. Dabbish and R.H. Sloan. Power analysis attacks of modular exponentiation in smartcards. In [**CH99**], 144–157.

[224] W. Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes.* Springer-Verlag, GTM 264, 1972.

[225] J.-F. Mestre. Lettre adressée à Gaudry et Harley, December 2000. Available at `http://www.math.jussieu.fr/~mestre/`.

[226] V. Miller. Short programs for functions on curves. Unpublished manuscript, 1986.

[227] S. Mitsunari, R. Sakai and M. Kasahara. A new traitor tracing. *IEICE Trans. Fundamentals*, **E84**, 481–484, 2002.

[228] A. Miyaji, M. Nakabayashi and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans. Fundamentals*, **E84**, 1234–1243, 2001.

[229] R.T. Moenck. Fast computation of GCDs. In *Proceedings of the 5th Annual ACM Symposium on the Theory of Computing*, 142–151, 1973.

[230] B. Möller. Securing elliptic curve point multiplication against side-channel attacks. In G.I. Davida and Y. Frankel, editors, *Information Security*, LNCS 2200, 324–334. Springer-Verlag, 2001.

[231] P.L. Montgomery. Modular multiplication without trial division. *Math. Comp.*, **44**, 519–521, 1985.

[232] P.L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, **48**, 243–264, 1987.

[233] F. Morain and J. Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. In *Theoretical Informatics and Applications*, 24, 531–543, 1990.

[234] V. Müller, A. Stein and C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.*, **68**, 807–822, 1999.

[235] K. Nagao. Improving group law algorithms for Jacobians of hyperelliptic curves. In [**A-4**], 439–447.

[236] D. Nalla and K.C. Reddy. ID-based tripartite authenticated key agreement protocols from pairings. See [**EP**], # 2003/04, 2003.

[237] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999.

[238] P.Q. Nguyen and I.E. Shparlinski. The insecurity of the Digital Signature Algorithm with partially known nonces. *J. Cryptology*, **15**, 151–176, 2002.

[239] P.Q. Nguyen and I.E. Shparlinski. The insecurity of the Elliptic Curve Digital Signature Algorithm with partially known nonces. *Designs, Codes and Cryptography*, **30**, 201–217, 2003.

[240] T. Okamoto and D. Pointcheval. The gap problems: a new class of problems for the security of cryptographic schemes. In [**P01**], 104–118.

[241] K. Okeya and K. Sakurai. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. In B. Roy and E. Okamoto, editors, *Progress in Cryptology – INDOCRYPT 2000*, LNCS 1977, 178–190. Springer-Verlag, 2000.

[242] K. Okeya and K. Sakurai. On insecurity of the side channel attack countermeasure using addition-subtraction chains under distinguishability between addition and doubling. In L. Batten and J. Seberry, editors, *Information Security and Privacy (ACISP 2002)*, LNCS 2384, 420–435. Springer-Verlag, 2002.

[243] P.C. van Oorschot and M.J. Wiener. Parallel collision search with cryptanalytic applications. *J. Cryptology*, **12**, 1–28, 1999.

[244] G. Orlando and C. Paar. A high performance reconfigurable elliptic curve processor for $GF(2^m)$. In [**CH00**], 41–56.

[245] S.B. Örs, E. Oswald and B. Preneel. Power-analysis attacks on FPGAs – First experimental results. In [**CH03**], 35–50.

[246] E. Oswald. Enhancing simple power-analysis attacks on elliptic curve cryptosystems. In [**CH02**], 82–97.

[247] E. Oswald. Markov model side-channel analysis. Unpublished manuscript, 2003.

[248] E. Oswald and M. Aigner. Randomized addition-subtraction chains as a countermeasure against power attacks. In [**CH01**], 39–50.

[249] K.G. Paterson. ID-based signatures from pairings on elliptic curves. *Electronics Letters*, **38**, 1025–1026, 2002. See also Cryptology ePrint Archive, Report 2002/004.

[250] K.G. Paterson. Cryptography from pairings: a snapshot of current research. *Information Security Technical Report*, **7**, 41–54, 2002.

[251] K.G. Paterson and G. Price. A comparion between traditional PKIs and identity-based cryptography. *Information Security Technical Report*, **8**, 57–72, 2003.

[252] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In [**A-3**], 576–591.

[253] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, **13**, 361–396, 2000.

[254] J. Pelzl, T. Wollinger, J. Guajardo and C. Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In [**CH03**], 351–365.

[255] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In S. Attali and T. Jensen, editors, *Smart Card Programming and Security (E-smart 2001)*, LNCS 2140, 200–210. Springer-Verlag, 2001.

[256] M.O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. MIT Laboratory for Computer Science, Technical Report MIT/LCS/TR-212, 1979.

[257] C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In [**C91**], 434–444.

[258] K.C. Reddy and D. Nalla. Identity based authenticated group key agreement protocol. In A. Menezes and P. Sarkar, editors, *INDOCRYPT 2002*, LNCS 2551, 215–233. Springer-Verlag, 2002.

[259] H.G. Rück. On the discrete logarithm in the divisor class group of curves. *Math. Comp.*, **68**, 805–806, 1999.

[260] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security (SCIS2000)*, 2000.

[261] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, **15**, 247–270, 2000.

[262] T. Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In [**A-5**], 43–66.

[263] T. Satoh, B. Skjernaa and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields Appl.*, **9**, 89–101, 2003.

[264] W. Schindler. A timing attack against RSA with the Chinese remainder theorem. In [**CH00**], 109–124.

[265] W. Schindler. A combined timing and power attack. In [**P02**], 263–279.

[266] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing (Arch. Elektron. Rechnen)*, **7**, 281–292, 1971.

[267] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod$p$. *Math. Comp.*, **44**, 483–494, 1985.

[268] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, **46**, 183–211, 1987.

[269] J.-P. Serre. *Local Fields*. Springer-Verlag, GTM 67, 1979.

[270] A. Shamir. Identity based cryptosystems and signature schemes. In [**C84**], 47–53.

[271] A. Shamir. Protecting smart cards from passive power analysis with detached power supplies. In [**CH00**], 71–77.

[272] D. Shanks. On Gauss and composition I and II. In R. Mollin, editor, *Number theory and its applications*, 163–204. Kluwer Academic Publishers, 1989.

[273] K. Shim. A man-in-the-middle attack on Nalla-Reddy's ID-based tripartite authenticated key agreement protocol. See [**EP**], # 2003/115, 2003.

[274] K. Shim. Cryptanalysis of Al-Riyami-Paterson's authenticated three party key agreement protocols. See [**EP**], # 2003/122, 2003.

[275] K. Shim. Efficient ID-based authenticated key agreement protocol based on Weil pairing. *Electronics Letters*, **39**, 653–654, 2003.

[276] K. Shim. Efficient one round tripartite authenticated key agreement protocol from Weil pairing. *Electronics Letters*, **39**, 208–209, 2003.

[277] V. Shoup. Lower bounds for discrete logarithms and related problems. In [**C97**], 256–266.

[278] V. Shoup. Using hash functions as a hedge against chosen ciphertext attack. In [**E00**], 275–288.

[279] V. Shoup. A proposal for an ISO standard for public key encryption, v2.1. Preprint, 2001.

[280] A. Silverberg and K. Rubin. Supersingular abelian varieties in cryptology. In [**C02**], 336–353.

[281] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, GTM 106, 1986.

[282] B. Skjernaa. Satoh's algorithm in characteristic 2. *Math. Comp.*, **72**, 477–487, 2003.

[283] N.P. Smart. The Hessian form of an elliptic curve. In [**CH01**], 118–125.

[284] N.P. Smart. The exact security of ECIES in the generic group model. In B. Honary, editor, *Coding and Cryptography*, LNCS 2260, 73–84. Springer-Verlag, 2001.

[285] N.P. Smart. How secure are elliptic curves over composite extension fields? In [**E01**], 30–39.

[286] N.P. Smart. An identity based authenticated key agreement protocol based on the Weil pairing. *Electronics Letters*, **38**, 630–632, 2002.

[287] N.P. Smart. An Analysis of Goubin's Refined Power Analysis Attack. In [**CH03**], 281–290.

[288] N.P. Smart. Access control using pairing based cryptography. In M. Joye, editor, *Topics in Cryptology – CT-RSA 2003*, LNCS 2612, 111–121. Springer-Verlag, 2003.

[289] D.K. Smetters and G. Durfee. Domain-based administration of identity-based cryptosystems for secure email and IPSEC. In *Proceedings 12th USENIX Security Symposium*, 215–229, 2003.

[290] J. Solinas. Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography*, **19**, 195–249, 2000.

[291] A. Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. *J. Ramanujan Math. Soc.*, **16**, 1–86, 2001.

[292] E. Steinfeld, L. Bull, H. Wang and J. Pieprzyk. Universal designated-verifier signatures. In [**A03**], 523–542.

[293] H. Stichtenoth. *Algebraic function fields and codes.* Springer-Verlag, 1993.

[294] H. Stichtenoth and C. Xing. On the structure of the divisor class group of a class of curves over finite fields. *Arch. Math,*, **65**, 141–150, 1995.

[295] D.R. Stinson. Some observations on the theory of cryptographic hash functions. See [**EP**], # 2001/020, 2002.

[296] H.-M. Sun and B.-T. Hsieh. Security analysis of Shim's authenticated key agreement protocols from pairings. See [**EP**], # 2003/113, 2003.

[297] E. Teske. Speeding up Pollard's rho method for computing discrete logarithms. In [**A-3**], 541–554.

[298] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In [**A03**], 75–92.

[299] É. Thomé. Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm. *J. Symbolic Comput.*, **33**, 757–775, 2002.

[300] E. Trichina and A. Bellezza. Implementation of elliptic curve cryptography with built-in countermeasures against side channel attacks. In [**CH02**], 98–113.

[301] S. Vaudenay. Security flaws induced by CBC padding – Applications to SSL, IPSEC, WTLS... In [**E02**], 534–546.

[302] S. Vaudenay. Hidden collisions on DSS. In [**C96**], 83–87.

[303] J. Vélu. Isogénies entre courbes elliptiques. *C.R. Acad. Sc. Paris*, Série A, **273**, 238–241, 1971.

[304] F. Vercauteren, B. Preneel and J. Vandewalle. A memory efficient version of Satoh's algorithm. In [**E01**], 1–13.

[305] E.R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. In [**E01**], 195–210.

[306] E.R. Verheul. Self-blindable credential certificates from the Weil pairing. In [**A01**], 533–551.

[307] C.D. Walter. Montgomery's multiplication technique: How to make it smaller and faster. In [**CH99**], 80–93.

[308] C.D. Walter. Sliding windows succumbs to Big Mac attack. In [**CH01**], 286–299.

[309] C.D. Walter. Breaking the Liardet-Smart randomized exponentiation algorithm. In P. Honeyman, editor, *Smart Card Research and Advanced Applications*, 59–68. Usenix Association, 2002.

[310] C.D. Walter. Some security aspects of the MIST randomized exponentiation algorithm. In [**CH02**], 276–290.

[311] C.D. Walter and S. Thompson. Distinguishing exponent digits by observing modular subtractions. In D. Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, LNCS 2020, 192–207. Springer-Verlag, 2001.

[312] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography.* CRC Press, 2003.

[313] E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 4th series, **2**, 521–560, 1969.

[314] B.R. Waters, D. Balfanz, G. Durfee and D.K. Smetters. Building an encrypted and searchable audit log. Palo Alto Research Center Technical Report, 2003.

[315] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, **55**, 497–508, 1949.

[316] A. Weil. The field of definition of a variety. *Am. J. Math.*, **78**, 509–524, 1956.

[317] N. Weste and K. Eshraghian. *Principles of CMOS VLSI Design.* Addison-Wesley, 2nd ed., 1993.

[318] P. Wright. *Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer.* Viking Press, 1987.

[319] X. Yi. An identity-based signature scheme from the weil pairing. *IEEE Communications Letters*, **7**, 76–78, 2003.

[320] X. Yi. Efficient ID-based key agreement from Weil pairing. *Electronics Letters*, **39**, 206–208, 2003.

[321] D.H. Yum and P.J. Lee. Efficient key updating signature schemes based on IBS. In K.G. Paterson, editor, *Cryptography and Coding*, LNCS 2898, 167–182. Springer-Verlag, 2003.

[322] F. Zhang and K. Kim. ID-based blind signature and ring signature from pairings. In [**A02**], 533–547.

[323] F. Zhang and X. Chen. Attack on two ID-based group key agreement schemes. See [**EP**], # 2003/259, 2003.

[324] F. Zhang and K. Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings. In R. Safavi-Naini, editor, *Proceedings of ACISP'03*, LNCS 2727, 312–323. Springer-Verlag, 2003.

[325] F. Zhang and S. Liu. ID-based one round authenticated tripartite key agreement protocol with pairings. See [**EP**], # 2002/122, 2002.

[326] F. Zhang, R. Safavi-Naini and C.-Y. Lin. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairing. See [**EP**], # 2003/104, 2003.

[327] F. Zhang, R. Safavi-Naini and W. Susilo. Efficient verifiably encrypted signatures and partially blind signatures from bilinear pairings. In T. Johansson and S. Maitra, editors, *INDOCRYPT 2003*, LNCS 2904, 191–204. Springer-Verlag, 2003.

[328] F. Zhang, R. Safavi-Naini and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In F. Bao, editor, *Public Key Cryptography – PKC 2004*, LNCS 2947, 277–290. Springer-Verlag, 2004.

Summary of Major LNCS Proceedings

For ease of reference we include here a table listing the main conference proceedings and the associated LNCS volume numbers. This includes all conferences in the relevant series which were published by Springer-Verlag and not necessarily those just referenced in this book.

Year	Crypto	Eurocrypt	Asiacrypt	CHES	PKC	ANTS
2003	2729	2656	2894	2779	2567	
2002	2442	2332	2501	2523	2274	2369
2001	2139	2045	2248	2162	1992	
2000	1880	1807	1976	1965		1838
1999	1666	1592	1716	1717	1560	
1998	1462	1403	1514		1431	1423
1997	1294	1233				
1996	1109	1070	1163			1122
1995	963	921				
1994	839	950	917			877
1993	773	765				
1992	740	658				
1991	576	547	739			
1990	537	473				
1989	435	434				
1988	403	330				
1987	293	304				
1986	263					
1985	218	219				
1984	196	209				
1982		149				

Author Index

Subject Index