Invited paper appearing in the Proceedings of the IEEE Information Theory Workshop 2006—ITW 2006, Punta del Este, Uruguay, March 2006. © *IEEE. Available online at* `http://www.cs.stanford.edu/~xb/itw06/`.

A Promenade through the New Cryptography of Bilinear Pairings

Xavier Boyen
Voltage Inc.
Arastradero Road
Palo Alto, California
Email: `xb@boyen.org`

***Abstract*— This paper gives an introductory account of the origin, nature, and uses of bilinear pairings, arguably the newest and hottest toy in a cryptographer's toolbox. A handful of cryptosystems built on pairings are briefly surveyed, including a couple of realizations of the famously elusive identity-based encryption primitive.**

I. Introduction

It can be said that much of contemporaneous cryptography can be traced to Shannon's legacy of "secrecy systems", an information theoretic foundation. To escape from the one-time pad, however, it has become necessary to appeal to a variety of computational complexity notions, *e.g.*, to leverage short secrets in order to protect long messages. Modern cryptography is, in essence, a computational game of cat and mouse between honest secret holders and resource-bounded adversaries.

Traditionally, cryptographic scheme development has evolved along two separate paths that differ in their complexity theoretic meanderings. On the one hand, the delicate art of "symbolic obfuscation" has roots in the early ciphers of the Antiquity; from it most of today's secret-key systems and hash functions have been crafted, due to its unsurpassed performance. On the other hand, the comparatively recent advent of algebraic methods has started to open, a few decades ago, a Pandora's Box of cryptosystems with astonishing features, encompassing virtually all of today's public-key cryptography.

Many public-key systems have been proposed in the past three decased, based on sundry algebra and a fair share of complexity theoretic assumptions. Some are based on NP-hard problems or coding theoretic tricks (*e.g.*, the McEliece cryptosystem); others involve exotic branches of group theory such as braid groups, or Lattice reduction problems that blur the boundary between the discrete and the continuous. The most prolific and successful approaches, however, all rely on the same handful of complexity assumptions, which are rooted either in the hardness of integer factorization (*e.g.*, RSA) or in that of taking discrete logarithms (*e.g.*, Diffie-Hellman).

Assumptions rooted in Factoring and the Discrete Logarithm problem are interesting in that they tend to have complementary properties. Factoring, via the RSA and Strong-RSA assumptions, offers a realization of the tremendously useful primitive of trapdoor permutation. Discrete Logarithm, in the guises of the Computational and Decision Diffie-Hellman (CDH and DDH), offers us the option to work with either a computational or a decisional complexity assumption, the latter being useful to build public-key encryption systems with formal proofs of security; by contrast, Factoring and RSA-like problems are essentially computational, and are thus inherently more suited for signature and authentication schemes—although we note that the Random Oracle heuristic blurs that disctinction, and exceptions abound. The common situation before the apparition of bilinear pairings was that CDH and DDH were concomitantly hard in all algebraic groups of cryptographic interest.

Bilinear maps—or pairings as they are often called—first appeared in cryptographic constructions around the turn of the millennium [1] [2], although they had been used cryptanalytically a few years prior [3]. Pairings have vastly expanded the world of Discrete Logarithm assumptions. The simplest examples of this is that they provide algebraic groups in which the DDH problem is easy even though CDH is still believed to be hard, a state of affair abstractly referred to as the Gap Diffie-Hellman (GapDH) assumption. GapDH is perhaps the simplest non-trivial assumption to be made in bilinear groups, although there are many others as we shall see.

We start in §II with a simple definition of pairings. In §III we give a brief overview of a concrete number theoretic implementation of pairings, and in §IV discuss a few useful complexity theoretic abstractions. We then turn our attention to the good uses that cryptographers have made of pairings, with a keen interest in §V for realizations of the identity-based encryption primitive, and in §VI for signature schemes with novel properties. We conclude in §VII with long-standing open problems.

II. Bilinear Groups

Before delving into the actual realization of bilinear groups and maps, it is helpful to understand why they are so desirable in cryptography.

For illustration, consider a cyclic group $\mathbb{G}$ of (finite) size or order n, such as the set $\mathbb{Z}_n$ of integer residues modulo n. If we use the multiplication symbol '$\cdot$' to denote the group operation (which in $\mathbb{Z}_n$ is the arithmetic addition modulo n), then we know that every element $h \in \mathbb{G}$ can be expressed as an integral power of some fixed element $g \in \mathbb{G}$ called a generator of the group, *i.e.*, $\exists a \in \mathbb{Z} : \underbrace{g \cdot g \cdots g}_{a \text{ times}} = g^a = g^{(a \bmod n)} = h$.

In this context, the CDH problem is the task of calculating $g^{a\,b}$ given only g, g^a, g^b, and an implicit description of $\mathbb{Z}_n$. The DDH problem is to decide whether or not $h = g^{a\,b}$ in a given quadruple of group elements $\langle g, g^a, g^b, h\rangle$. For $\mathbb{G}$ the set of integers under addition modulo n, both problems are of course easy to solve. On the contrary, if we take $\mathbb{G}$ to be the multiplicative subgroup of order p in the set of integer residues $\mathbb{Z}_q$, such that p and $q = 1 + 2\,p$ are prime numbers, then suddenly both CDH and DDH are believed to be hard problems.

Now, abstractly, a bilinear pairing is an efficiently computable map $\mathbf{e} : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$, where for simplicity $\mathbb{G}$ and $\hat{\mathbb{G}}$ are two cyclic groups of equal order p that are respectively generated by some $g \in \mathbb{G}$ and $\hat{g} \in \hat{\mathbb{G}}$. (We could even have $\mathbb{G} = \hat{\mathbb{G}}$ and $g = \hat{g}$, though in general we do not.) The range of $\mathbf{e}$ is a multiplicative group of order p, denoted $\mathbb{G}_T$, and generated by $\mathbf{e}[g, \hat{g}]$. The pairing must be non-trivially bilinear, meaning that the equality $\mathbf{e}[g^a, \hat{g}^b] = \mathbf{e}[g, \hat{g}]^c$ holds if and only if the integer exponents satisfy $a\,b = c \pmod p$.

With this definition, it is easy to see that the pairing is a powerful tool that lets us compute something similar to a Diffie-Hellman operation, with the important caveat that the process takes us from $\mathbb{G}$ and $\hat{\mathbb{G}}$ to the different group $\mathbb{G}_T$ from which we generally cannot get back. Nevertheless, this is sufficient to give us a direct test for the DDH problem (for $\mathbb{G} = \hat{\mathbb{G}}$) or a dual-group version of DDH (when $\mathbb{G} \neq \hat{\mathbb{G}}$). Indeed, given an instance $\langle g, g^a, \hat{g}^b, \hat{h}\rangle \in \mathbb{G}^2 \times \hat{\mathbb{G}}^2$, it is easy to determine whether $\hat{h} = \hat{g}^{a\,b}$ by verifying the equality $\mathbf{e}[g^a, g^b] = \mathbf{e}[g, \hat{h}]$.

In spite of this ability, it is not obvious how one would compute $\hat{h}$ from $\langle g, \hat{g}, g^a, \hat{g}^b\rangle$ without knowing at least one of the exponents a and b; in fact, it is widely believed that this CDH-like problem is hard for the bilinear pairings of cryptographic interest, which are based on algebraic curves. We shall give a very rough intuition for this in the next section.

III. Algebraic Realizations

Algebraic curves and elliptic curves in particular have provided an avenue for the construction of cryptographically suitable bilinear pairings, known as the Weil and the Tate pairings. In the next few paragraphs we give a very brief overview of how these pairing come to existence.

To start, consider a finite field (or Galois field) $\mathbb{F}_q$ of size q, usually a large prime. Roughly speaking, an elliptic curve over the field $\mathbb{F}_q$ is defined by a bivariate equation in x and y, such as $E : y^2 = x^3 + a\,x + b$, where a and b are constants in $\mathbb{F}_q$. We can view a pair $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ as representing the coordinates of a point on the doubly periodic integer "plane" (or torus) $\mathbb{F}_q \times \mathbb{F}_q$. We say that such a point is on the curve if its coordinates satisfy the curve equation in $\mathbb{F}_q$. It turns out that the set of points on the curve (to which we add a special zero point to serve as neutral element) forms a group, denoted $E(\mathbb{F}_q)$, under a simple group operation called point addition on the curve. Hasse's theorem states that the group size, $\#E(\mathbb{F}_q)$, is always roughly the same as the field size, $\#\mathbb{F}_q = q$; more precisely, $|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$. With a suitable choice of field and curve, the group size $\#E(\mathbb{F}_q)$ can be made to contain a large prime factor p, in which case the group $E(\mathbb{F}_q)$ will have a cyclic subgroup of prime order p, which can be our candidate for $\mathbb{G}$.

To proceed, we consider the same curve equation E as above, but on a larger field $\mathbb{F}_{q^k}$ which for $k > 1$ is called an algebraic extension of the ground field $\mathbb{F}_q$. Elements of $\mathbb{F}_{q^k}$ can be represented, *e.g.*, as polynomials of degree (up to) k with coefficients in $\mathbb{F}_q$. What this entails is that the elements of $\mathbb{F}_{q^k}$ are compatible with those of $\mathbb{F}_q$, so that the product of, say, $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^k}$ is a well-defined element of $\mathbb{F}_{q^k}$. Thus, and by analogy with what we did earlier, we can define $E(\mathbb{F}_{q^k})$ as the set of points $(x, y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ that satisfy the curve equation in $\mathbb{F}_{q^k}$. Under the point addition rule, $E(\mathbb{F}_{q^k})$ forms a group, albeit a much larger one than $E(\mathbb{F}_q)$. The point of this discussion is that as k is increased, there is a special value of $k > 1$ for which $E(\mathbb{F}_{q^k})$ contains a subgroup of order p. This subgroup will be our candidate for $\hat{\mathbb{G}}$, and the smallest such k its embedding degree in $E(\mathbb{F}_q)$.

The last step involves a bit of magic. Recall that we have identified two (distinct) subgroups of points on the curve E, both of them having the same prime order p. Consider two points $U \in E(\mathbb{F}_q)$ and $V \in E(\mathbb{F}_{q^k})$. In general, any element $g_1 \in \mathbb{G} \subset E(\mathbb{F}_q)$ can be expressed as a linear combination of U and V, and the same is true of any $\hat{g}_2 \in \hat{\mathbb{G}} \subset E(\mathbb{F}_{q^k})$. Since $\mathbb{G}$ and $\hat{\mathbb{G}}$ are linearly independent, the linear coefficients of g_1 and $\hat{g}_2$ have a

typically non-zero determinant:

$$\Delta = \begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix} \qquad \text{for} \quad \begin{array}{l} g_1 = U^{u_1} \cdot V^{v_1} \\ \hat{g}_2 = U^{u_2} \cdot V^{v_2} \end{array}$$

The Weil pairing (and the closely related Tate pairing) can then be viewed as the function ω^{Δ}, where ω is some primitive p-th root of unity in $\mathbb{F}_{q^k}$. Bilinearity arises from the observation that if we let $g_1' = g_1^a$ and $\hat{g}_2' = g_2^b$, we get $\Delta' = a\,b\,\Delta$. The magic of the Weil pairing is that it has an efficient algorithm, discovered by Miller [4], that computes the value of ω^{Δ} based solely on g_1 and $\hat{g}_2$, without necessitating Δ or the linear coefficients. We remark that for k as previously defined, the extension field $\mathbb{F}_{q^k}$ always has a multiplicative subgroup of order p; this subgroup is our target group $\mathbb{G}_T$.

All of the above is true in general, so in that sense bilinear pairings are not hard to obtain. However, this only works in practice if the embedding degree k is small. The reason is that elements of $\hat{\mathbb{G}}$ are points $(x, y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$, whose coordinates will be intractably difficult to represente and calculate with for large k. Since a random curve generally produces extremely large embedding degrees, a lot of recent effort has been dedicated to devise clever ways to generate practical curves, yielding large subgroups with tiny embedding degrees—such as $k = 2$ and 6 [5], and 12 [6].

Lastly, we mention that it is sometimes possible to obtain a modified "symmetric" pairing whose arguments are interchangeable and both live in the group $\mathbb{G}$. The idea is to reduce this case to the earlier "asymmetric" case, by lifting one of the arguments from $\mathbb{G}$ into $\hat{\mathbb{G}}$ using a homomorphic distortion function $\psi : \mathbb{G} \to \hat{\mathbb{G}}$ (not to be confused with the more commonly available trace map $\phi : \hat{\mathbb{G}} \to \mathbb{G}$, which goes in the other direction). Distortion functions are guaranteed by a special algebraic structure, exemplified by the so-called supersingular curves that have enjoyed a recent bout of popularity in cryptographic circles for precisely that reason.

IV. Complexity Assumptions

The upshot of the previous section is that the cryptographic pairing implementations that we know of, are functions of the form $\mathbf{e}[g_1, \hat{g}_2] = \omega^{\Delta}$ with $\Delta = \left|\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right|$ for $g_1 = U^{u_1} \cdot V^{v_1}$ and $\hat{g}_2 = U^{u_2} \cdot V^{v_2}$.

As noted, the 2-by-2 determinant causes bilinearity. Furthermore, since Δ appears in the exponent, it stands to reason that a function that evaluates to ω^{Δ} should be hard to invert, for the same reason that vanilla Discrete Logarithm is presumed hard in the same groups.

Similarly to (non-bilinear) groups in which the formulation of stronger assumptions such as CDH and DDH have proven very useful, there are a many plausible DL-like complexity assumptions that can be made in bilinear groups, based on the preceding observations. We briefly review some of the main ones, most of them having both a computational and a decisional version.

a) Bilinear Diffie-Hellman (BDH): On input the generators $g \in \mathbb{G}$ and $\hat{g} \in \hat{\mathbb{G}}$, and their powers to each of the undisclosed exponents $a, b, c \in \mathbb{Z}_p$, it is hard to compute the element $\mathbf{e}[g, \hat{g}]^{a\,b\,c} \in \mathbb{G}_T$ (or to recognize it from random, in the decisional version denoted D-BDH). This assumption was formally stated in [7].

BDH and D-BDH are direct analogues of CDH and DDH in non-bilinear groups, except that here a third secret exponent is needed since it is easy to compute $\mathbf{e}[g, \hat{g}]^{a\,b}$ from g^a and $\hat{g}^b$.

b) Strong Diffie-Hellman (SDH): Given as input $g \in \mathbb{G}$, and the powers of $\hat{g} \in \hat{\mathbb{G}}$ to each of the exponents $1, a, a^2, ..., a^{\ell} \in \mathbb{Z}_p$ for some number ℓ and secret a, it is hard to find $b \in \mathbb{Z}_p$ and $h \in \mathbb{G}$ such that $h^{a+b} = g$. Purported solutions are easy to verify by checking that $\mathbf{e}[h, (\hat{g}^a)(\hat{g})^b] = \mathbf{e}[g, \hat{g}]$. SDH was first stated in [8].

SDH is a Discrete Logarithm counterpart to Strong RSA. Both assumptions have in common that a problem instance has not one but a very large number of admissible solutions. SDH, like S-RSA before it, has found many application in signatures and authentication schemes. It has no obvious decisional version.

c) Linear: On input $g, g^a, g^b, g^{a\,x}, g^{b\,y} \in \mathbb{G}$, it is hard to compute $g^{x+y} \in \mathbb{G}$ (or to distinguish it from random, in the decisional version of the assumption). Linear was originally proposed in [9].

Since (D-)Linear instances involve no elements of $\mathbb{G}_T$, the assumption remains meaningful in ordinary non-bilinear groups. Its appeal in bilinear groups stems from the design as a weakening of (DDH/)CDH that is believed to hold even in the presence of a bilinear map.

We note that many more complexity assumptions have been stated and used in the context of pairings—probably more than in any other branch of cryptography. The flexibility to tailor complexity assumptions to build cryptosystems with novel properties has undoubtedly been a major factor in the rapid rise of pairings. We shall describe some of those in the remaining few sections.

Although it is reasonable to be suspicious of assumptions made for a single purpose, we note that in many cases powerful supportive arguments can be made based on generic group structural arguments. In other words, properly constructed cryptosystems based on pairings can be impervious to (mathematical) attacks, unless the underlying pairing realization itself has a vulnerability independent of the cryptosystem.

V. Identity-Based Encryption

Public-key differs from secret-key encryption in that the key used for encryption cannot feasibly be used for decryption, which requires a separate key. The two keys are related "by birth" through the key pair generation process; and obviously the encryption key must be made available to the encrypting party before the system can be used. Usually, a public key is bound to her owner's legal name or other identifying information with a digital signature issued by a trusted certificate authority.

Identity-based encryption (IBE) is public key encryption with a twist. Here, the public key can be any string, such as the legal name of the recipient. The private key is generated from it by a central trusted authority (TA) who holds a master secret key. To encrypt in such a system, one needs only to know the name of the recipient, and a set of public system parameters that are common to all users under the purview of the TA. Since the public key does not functionally depend on the private key, the sender need not wait for the recipient to send him her public key. Also, there is less of a need for certificates and revocation lists, since public keys can be reasonably short lived and are unambiguous by design.

The notion of IBE was suggested two decades ago [10], without any suggestion as to how it could be realized. Slow progress was made over the years using traditional cryptographic techniques, until it became apparent that bilinear maps provided the perfect answer to the question [2] [7]. This came as a breakthrough in 2001 with the publication of the first practical IBE system whose security could be reduced to the simple BDH complexity assumption [7]. As good things never come alone, the same year saw a completely different proposal for a simpler but less practical IBE based on a Factoring assumption [11]. The discovery of pairing-based IBE has spurred a great deal of research in this new area, which in particular resulted in the invention of a less demanding and more flexible paradigm [12] that was also more secure: its distinct advantage was to admit a security reduction that did not rely on the random oracle heuristic.

We now describe the two main IBE schemes.

A. Boneh-Franklin (BF) [7]

The Boneh-Franklin system ideally necessitates a "symmetric" bilinear map $\mathbf{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ (*cf.* §III), and requires a "full domain" cryptographic hash function H from identities to elements of $\mathbb{G}$, available to all.

Setup: The master secret is a random integer $\sigma \in \mathbb{Z}_p$. The public parameters are g and $f = g^\sigma \in \mathbb{G}$.

Issue: To issue a private key to a user with name ID, the TA returns $d = (H[\mathrm{ID}])^\sigma \in \mathbb{G}$.

Encr.: To encrypt a message for a user named ID, the sender picks a random $r \in \mathbb{Z}_p$ and uses $\mathbf{e}[H[\mathrm{ID}], f]^r$ as session key. The header $h = g^r$ is added to the ciphertext.

Decr.: To decrypt a ciphertext with header h, the recipient recovers the session key as $\mathbf{e}[d, h]$, which will be correct if the identities match.

This is a simplified description; in the real scheme additional hash functions are needed in order for the security proofs to go through. Nonetheless, the scheme is very simple to understand once we have abstracted away the notion of pairing. In practice, the requirement to hash into $\mathbb{G}$ complicates matters with asymmetric pairings.

B. Boneh-Boyen (BB_1) [12]

The Boneh-Boyen system works well with the general bilinear map $\mathbf{e} : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$, and uses only a collision-resistant hash function H from identities to (a subset of) $\mathbb{Z}_p$, or none at all if identities are encoded as integers.

Setup: The master secret is a triple of random integers $\alpha, \beta, \gamma \in \mathbb{Z}_p$. The public system parameters are g, $u = g^\alpha$, $w = g^\gamma \in \mathbb{G}$, and $z = \mathbf{e}[g, \hat{g}]^{\alpha\,\beta}$.

Issue: To issue a private key to a user with name ID, the TA selects a random $t \in \mathbb{Z}_p$ and outputs $d_0 = \hat{g}^{\alpha\,\beta + (\gamma + \alpha\,H[\mathrm{ID}])\,t}$ and $d_1 = \hat{g}^t$.

Encr.: To encrypt a message for a user named ID, the sender selects a random $r \in \mathbb{Z}_p$ and uses v^r as session key. A header consisting of $h_0 = g^r$ and $h_1 = w^r \cdot u^{r\,H[\mathrm{ID}]}$ is added to the ciphertext.

Decr.: To decrypt a ciphertext with header h_0 and h_1, the recipient recovers the session key as the ratio $\mathbf{e}[h_0, d_0]/\mathbf{e}[h_1, d_1]$, which will be equal to z^r if the identities match.

Again, this is a simplified description. Here, the private keys are randomized. This scheme appears more complicated than the previous one, but it is faster since all exponentiations are to fixed bases, and hence can be greatly optimized.

Much like BF, the BB_1 scheme has been extended in many ways to offer, *e.g.*, hierarchical identities [13], improved security [14], and threshold decryption [15]. Both schemes are secure under the BDH assumption, without random oracles in the case of BB_1. Both can be made to conceal the recipient identity in addition to the message, as well as to withstand active attacks.

Very recently, Boyen and Waters [16] built a fully anonymous hierarchical IBE scheme, upon the Linear assumption. Systems that exploit stronger complexity assumptions have also been suggested; these include Boneh and Boyen's second IBE construction (BB_2) [12], as well as a very recent IBE scheme by Gentry [17], whose proofs both rely on SDH-like assumptions.

VI. Signature and Authentication

It has been observed that IBE implies digital signature: disguise the messages as identities, and use the IBE private keys as signatures. Since a BF private key is a single element of $\mathbb{G}$, it is natural to seek to turn BF IBE into a compact signature (in the random oracle model). This is the essence of the BLS signature scheme [18], which unlike BF uses asymmetric pairings to reduce the size of elements of $\mathbb{G}$. Notably, these signatures can be aggregated [19]. The basic BLS scheme is as follows:

Setup: The signing key is a random integer $\sigma \in \mathbb{Z}_p$. The verification key is $\hat{g}$ and $\hat{f} = \hat{g}^\sigma \in \hat{\mathbb{G}}$.

Sign: To sign a message M, give $s = (H[M])^\sigma \in \mathbb{G}$.

Verif.: To verify $\langle M, s\rangle$, check $\mathbf{e}[s, \hat{g}] = \mathbf{e}[H[M], \hat{f}]$.

Short signatures built from pairings need not directly correspond to an IBE scheme. The BB scheme [8] uses a construction whose security can be directly reduced to the SDH assumption without requiring random oracles. A collision-resistant function H into $\mathbb{Z}_p$ is needed only if messages cannot be encoded in $\mathbb{Z}_p$. The scheme is:

Setup: The signing key is a pair of integers $\alpha, \beta \in \mathbb{Z}_p$. The verification key is made of $\hat{a} = \hat{g}^\alpha$, $\hat{b} = \hat{g}^\beta$, $\hat{g}$, and $z = \mathbf{e}[g, \hat{g}]$.

Sign: To sign a message M, choose a random $r \in \mathbb{Z}_p$, and output r and $s = g^{1/(\alpha+\beta\, r+H[M])} \in \mathbb{G}$.

Verif.: To publicly verify a signed message $\langle M, r, s\rangle$, test the equality $\mathbf{e}[s,\ \hat{a} \cdot \hat{b}^r \cdot \hat{g}^{H[M]}] = z$.

Bilinear maps have been useful in more complicated schemes, such as group and ring signatures. In these, signers sign on behalf of a plurality of users, who have willingly constituted a group, or are conscripted in a ring. In group signatures, a tracing authority also has the ability to expose the true signer. Group signatures have especially benefited from pairings [9] [20] [21], for they blend authentication and encryption: with bilinear maps, complementary goals can be tackled by combining assumptions (*e.g.*, SDH for signing, Linear for tracing).

Other surprising ways in which pairings have been used include homomorphic encryption [22] as well as non-interactive zero-knowledge proof systems [23].

VII. Conclusion

In this tour, we have explored some of the foundations and applications of bilinear maps in cryptography.

For the mathematician, a long-standing open question concerns the existence of multilinear maps, which could have far reaching consequences in both cryptography and cryptanalysis. For the cryptographer, as a counterpoint to IBE appearing to be so closely connected to pairings, a fascinating open problem is to devise an IBE scheme from generic trapdoor permutations.

References

[1] A. Joux, "A one round protocol for tripartite Diffie-Hellman," *Journal of Cryptology*, vol. 17, no. 4, pp. 263–76, 2004, extended abstract in *Proceedings of ANTS IV, 2000*.

[2] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairings," in *Proceedings of the Symposium on Cryptography and Information Security—SCIS 2000*, 2000.

[3] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms in a finite field," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639–46, 1993.

[4] V. Miller, "The Weil pairing, and its efficient calculation," *Journal of Cryptology*, vol. 17, no. 4, 2004.

[5] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundamentals*, vol. E84-A, no. 5, pp. 1234–43, 2001.

[6] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," Cryptology ePrint Archive, Report 2005/133, 2005, http://eprint.iacr.org/.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615, 2003, extended abstract in *CRYPTO 2001*.

[8] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Advances in Cryptology—EUROCRYPT 2004*, ser. LNCS, vol. 3027. Springer, 2004, pp. 56–73.

[9] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology—CRYPTO 2004*, ser. LNCS, vol. 3152. Springer, 2004, pp. 41–55.

[10] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology—CRYPTO 1984*, ser. LNCS, vol. 196. Springer, 1984, pp. 47–53.

[11] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, 2001.

[12] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT 2004*, ser. LNCS, vol. 3027. Springer, 2004, pp. 223–38.

[13] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology—EUROCRYPT 2005*.

[14] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT 2005*, ser. LNCS, vol. 3494. Springer, 2005.

[15] D. Boneh, X. Boyen, and S. Halevi, "Chosen ciphertext secure public key threshold encryption without random oracles," in *Proceedings of RSA-CT 2006*.

[16] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," Manuscript, 2006.

[17] C. Gentry, "Identity based encryption without random oracles with a tight security reduction," Manuscript, 2006.

[18] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004, extended abstract in *ASIACRYPT 2001*.

[19] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology—EUROCRYPT 2003*.

[20] X. Boyen and B. Waters, "Compact group signatures without random oracles," Cryptology ePrint Archive, Report 2005/381, 2005, http://eprint.iacr.org/.

[21] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros, "Practical group signatures without random oracles," Cryptology ePrint Archive, Report 2005/385, 2005, http://eprint.iacr.org/.

[22] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proceedings of TCC 2005*, ser. LNCS. Springer, 2005.

[23] J. Groth, R. Ostrovsky, and A. Sahai, "Perfect non-interactive zero knowledge for np," Cryptology ePrint Archive, Report 2005/290, 2005, http://eprint.iacr.org/.