On the Disadvantages of Pairing-based Cryptography

Zhengjun Cao[1], Lihua Liu[2,*]

Abstract. Pairing-based cryptography (PBC) has many elegant properties. It is claimed that PBC can offer a desired security level with smaller parameters as the general elliptic curve cryptography (ECC). In the note, we remark that this view is misleading. Suppose that an elliptic curve E is defined over the field $\mathbb{F}_q$. Then ECC is working with elements which are defined over $\mathbb{F}_q$. But PBC is working with the functions and elements defined over $\mathbb{F}_{q^k}$, where k is the *embedding degree*.

The security of PBC depends directly on the intractable level of either elliptic curve discrete log problem (ECDLP) in the group $E(\mathbb{F}_q)$ or discrete log problem (DLP) in the group $\mathbb{F}^*_{q^k}$. That means PBC protocols have to work in a running environment with parameters of 1024 bits so as to offer 80 bits security level. The shortcoming makes PBC lose its competitive advantages significantly.

Keywords. elliptic curve cryptography; bilinear-pairing based cryptography; inputting parameters; working parameters; embedding degree.

1 Introduction

In 1985, N. Koblitz [19] and V. Miller [20] introduced elliptic curve cryptography independently. Since then, ECC has been extensively investigated. In the late 1990's, a few companies included some elliptic curve protocols in their security products. The security of ECC is based directly on the intractablity of ECDLP. Parings derived from elliptic curves, including Weil paring [24] and Tate paring [15], have been used to reduce ECDLP to DLP [22].

In 2000, Joux [18] proposed one round protocol for tripartite Diffie-Hellman key agreement protocol using Weil pairing. This is the first instance to show that pairings can be used for "good". In Crypto 2001, Boneh and Fracklin [6] proposed a fully functional identity-based encryption scheme from Weil Pairing. After that, paring-based cryptography has gotten a full development [1-14], because it has many beautiful and elegant properties. It is widely believed that PBC can offer a desired security level with smaller parameters. For example, Boneh-Boyen short signatures [2], Boneh-Boyen-Shacham short group signatures [5], Boneh-Shacham-Lynn short signatures [11], and Boneh-Sahai-Waters traitor tracing schemes [12]. In fact, this view is misleading. Suppose that an

[1]Department of Mathematics, Shanghai University, Shanghai, China. [2]Department of Mathematics, Shanghai Maritime University, Shanghai, China. * liulh@shmtu.edu.cn

elliptic curve E is defined over the finite field $\mathbb{F}_q$. Then ECC is working with elements which are defined over the base field $\mathbb{F}_q$ (its parameters have size $O(\log q)$ bits). But PBC is working with the functions and elements defined over the extension field $\mathbb{F}_{q^k}$ (its parameters have size $O(k \log q)$ bits), where k is the *embedding degree*.

The security of PBC depends directly on the intractable level of either ECDLP in the group $E(\mathbb{F}_q)$ or DLP in the group $\mathbb{F}^*_{q^k}$. This gives us a dilemma. On the one hand, to ensure the immunity to the Weil and Tate pairing attacks, it requires that the imbedding degree $k > 20$ if the order n of the base point P satisfying $n > 2^{160}$. On the other hand, it requires $k \leq 6$ to ensure the efficiency of pairing computations in PBC protocols. This means the underlying field $\mathbb{F}_q$ is large enough so that the DLP in $\mathbb{F}^*_{q^k}$ is considered intractable. In a word, PBC protocols have to work in a running environment with parameters of 1024 bits, not 160 bits as supposed (someone has confused the *inputting-parameter's size* with the *working-parameter's size*), so as to offer 80 bits security level. The shortcoming makes PBC lose its competitive advantages significantly.

2 The Weil pairing over finite fields

Definition 1. *An elliptic curve E over a finite field $\mathbb{F}_q$ is defined by an equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ and $\triangle \neq 0$, where $\triangle$ is the discriminant of E and is defined as follows: $\triangle = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$, where $d_2 = a_1^2 + 4a_2, d_4 = 2a_4 + a_1a_3, d_6 = a_3^2 + 4a_6, d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

If L is any extension field of $\mathbb{F}_q$, then the set of L-rational points on E is

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

where ∞ is the point at infinity. The number of points in the group $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q)$, is called the order of E over $\mathbb{F}_q$. Hasse's theorem provides tighter bounds for $\#E(\mathbb{F}_q)$.

Theorem 1. (Hasse) *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

Let n be a prime and coprime to the characteristic of $\mathbb{F}_q$. Suppose n divides $\#E(\mathbb{F}_q)$. Then there exists a n-torsion group [24]

$$E(\mathbb{F}_{q^k})[n] := \{P \in E(\mathbb{F}_q^k) \,|\, nP = \mathcal{O}\},$$

where the number k is called the *embedding degree* which is the smallest positive integer such that n divides $(q^k - 1)$, and nP denotes the sum of n copies of P. The existence of the n-torsion group is due to Balasubramanian and Koblitz [16].

Theorem 2. *Let E be an elliptic curve over $\mathbb{F}_q$ and let n be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that n does not divide $(q-1)$ and that $\gcd(n,q)=1$. Then the n-torsion group $E[n] \subset E(\mathbb{F}_{q^k})$ if and only if n divides (q^k-1).*

The structure of n-torsion group $E(\mathbb{F}_{q^k})[n]$ is described by the following relation

$$E(\mathbb{F}_{q^k})[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

That means $\#E(\mathbb{F}_{q^k})[n] = n^2$. The Weil pairing is defined on the n-torsion group $E(\mathbb{F}_{q^k})[n]$, not on any n-order group $G \subset E(\mathbb{F}_q)$.

Let μ_n be the group of nth roots of unity. Clearly, $\mu_n \subset \mathbb{F}_{q^k}$, but $\mu_n \not\subset \mathbb{F}_{q^j}$ for $j = 1, \cdots, k-1$.

Definition 2. *The Weil pairing is a map*

$$e_n : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})[n] \to \mu_n$$

with the following properties:

1. *Linearity: If $P, Q, R \in E(\mathbb{F}_{q^k})[n]$, then*

$$e_n(P+Q, R) = e_n(P, R)e_n(Q, R),$$

$$e_n(P, Q+R) = e_n(P, Q)e_n(P, R).$$

2. *Alternating: If $P \in E(\mathbb{F}_{q^k})[n]$, then $e_n(P, P) = 1$. This, along with linearity, implies that if $P, Q \in E(\mathbb{F}_{q^k})[n]$, then $e_n(Q, P) = e_n(Q, P)^{-1}$.*

3. *Non-degeneracy: If $\mathcal{O} \neq P \in E(\mathbb{F}_{q^k})[n]$, there exists $Q \in E(\mathbb{F}_{q^k})[n]$ such that $e_n(P, Q) \neq 1$.*

4. *Compatibility: If $P \in E(\mathbb{F}_{q^k})[mn]$ and $Q \in E(\mathbb{F}_{q^k})[n]$, then $e_{mn}(P, Q) = e_n(mP, Q)$.*

5. *Galois action: Let $P, Q \in E(\mathbb{F}_{q^k})[n]$ and $\sigma \in Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$, then $e_n(P, Q)^\sigma = e_n(P^\sigma, Q^\sigma)$.*

To construct a concrete Weil pairing, we need the following equivalent definition [21]:

Definition 3 *Let $n > 1$ be an integer and let $\mathfrak{D}_1, \mathfrak{D}_2$ be divisors on an elliptic curve, E, with disjoint supports, such that $n\mathfrak{D}_1, n\mathfrak{D}_2 \sim 0$. This means that there are functions f_1 and f_2 such that $n\mathfrak{D}_i = div(f_i)$ for $i = 1, 2$. The Weil pairing is defined as*

$$e_n(\mathfrak{D}_1, \mathfrak{D}_2) = \frac{f_1(\mathfrak{D}_2)}{f_2(\mathfrak{D}_1)}.$$

Warning. Most literatures use the notation $E[n]$ to denote the n-torsion group, which does not specify that the representation of points, the computation of functions and the evaluation for those functions should be performed in the extension field $\mathbb{F}_{q^k}$.

3 Miller's algorithm for computing pairings

In order to calculate the Weil pairing, one should evaluate $f(\mathfrak{D})$, where $\operatorname{div}(f) = n([P] - [O])$. In 1985, Miller [21] gave an explicit algorithm for calculating the Weil pairing. Of course, it can be used to calculate the Tate pairing, because it is also defined on the n-torsion group.

Let E be an elliptic curve over the field K and $P, Q \in E(K)$. Let $L_{P,Q}$ be the normalized function, such that $L_{P,Q} = 0$ is the equation of the line passing through P and Q (or the equation of the tangent line to the curve if $P = Q$). Then

$$\operatorname{div}(L_{P,Q}) = [P] + [Q] + [-(P+Q)] - 3[\mathcal{O}].$$

Let

$$h_{P,Q} := \frac{L_{P,Q}}{L_{P+Q,-(P+Q)}}.$$

We have $\operatorname{div}(h_{P,Q}) = [P] + [Q] - [P+Q] - [\mathcal{O}]$.

Let $f_{0,P} = f_{1,P} = 1$. Inductively, for $n > 0$, define

$$f_{n+1,P} := f_{n,P}\, h_{P,nP},$$

we have

$$\operatorname{div}(f_{n,P}) = n[P] - (n-1)[\mathcal{O}] - [nP].$$

It is easy to find that

$$f_{m+n,P} = f_{m,P} f_{n,P} h_{mP,nP},\ f_{mn,P} = f_{m,P}^n f_{n,mP} = f_{n,P}^m f_{m,nP}.$$

This means the calculation of $f_{n,P}(Q)$ resembles exponentiation and it can be done in $O(\log n)$ point additions on E/K.

Using the constructed functions, we obtain the following formulas [21].

Proposition 1. *Suppose that T is a point in $E(K)$ different from $P, Q, Q-P$, and $\mathcal{O}$. Then $[P] - [\mathcal{O}] \sim [P+T] - [T]$, and the supports of $[Q] - [\mathcal{O}]$ and $[P+T] - [T]$ are disjoint. We have*

$$e_n(P,Q) = \frac{f_{n,Q}(T) f_{n,P}(Q-T)}{f_{n,P}(-T) f_{n,Q}(P+T)}.$$

Proposition 2. *Let E/K be an elliptic curve, $P, Q \in E(K)[n]$, and $P \neq Q$. Then*

$$e_n(P,Q) = (-1)^n \frac{f_{n,P}(Q)}{f_{n,Q}(P)}.$$

Warning. The functions $f_{n,P}, f_{n,Q}$ must be calculated in the group $E(K)$ where the field K satisfies $\mu_n \subset K$. So do the evaluations of $f_{n,P}(Q), f_{n,Q}(P)$.

4 Disadvantages of pairing-based cryptography

4.1 Large working parameters

It is well-known that ECC schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, a desired security level can be attained with significantly smaller parameters in ECC systems. For example, a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA parameter. Smaller parameters in ECC systems consequently save much power, bandwidth and storage, and bring a good speed.

The working parameters for an elliptic curve scheme describe an elliptic curve E over $\mathbb{F}_q$, a base point $P \in E(\mathbb{F}_q)$, and its order n. The parameters should be chosen so that the ECDLP is resistant to all known attacks. Usually, we select E so that $\#E(\mathbb{F}_q)$ is prime or almost prime, that is, $\#E(\mathbb{F}_q) = hn$ where n is prime and h is small (e.g., $h = 1, 2, 3$ or 4). That means the size of the working parameter q in an ECC scheme is approximately equal to the size of n. To avoid the Weil and Tate pairing attacks, one should ensure that n does not divide $q^k - 1$ for all $1 \leq k \leq 20$. The parameter size comparisons in Table 1 is adapted from [17].

security level (bits)	80 (SKIPJACK)	112 (Triple-DES)	128 (AES-Small)	192 (AES-Medium)	256 (AES-Large)
EC parameter n EC parameter q	160	224	256	384	512
EC parameter k	>20				
PBC parameter n	160	224	256	384	512
PBC parameter q^k	1024	2048	3072	8192	15360
PBC parameter k	≤6				
DL parameter q	160	224	256	384	512
DL modulus p	1024	2048	3072	8192	15360
RSA modulus n	1024	2048	3072	8192	15360

Table 1. RSA, DL, EC, PBC parameter sizes for equivalent security levels. Bitlengths are given for the DL parameter q and the EC parameter n, and the RSA modulus n and the DL modulus p, respectively.

As we know, pairing-based cryptography protocols require that:

- the base point $P \in E(K)$ has a sufficiently large prime order n such that ECDLP in $E(K)$ is intractable;
- DLP in K^* is intractable in order to resist the MOV reduction attacks [22];
- *it is efficient to compute pairings in $E(K)$.*

From the practical point of view, it is annoying for PBC schemes to have to work in extensions of the base fields, even though the inputting parameters are defined over the base field. Taking

into account the very long and complicated programming code for PBC systems (see *PBC 0.5.14*, maintained by Ben Lynn, released on Jun 14, 2013) we find that PBC schemes are far slow than its DL counterparts. Smaller inputting parameters in PBC systems can not truly bring them a good speed. We refer to the following Table 2 for the concrete comparisons between DSA and Boneh-Boyen short signature [2].

	DSA	Boneh-Boyen short signature
Setup	p : 1024-bit prime, q : 160-bit prime factor of $p-1$, g : a base element of order q mod p, $y = g^x \bmod p$, $x \in \mathbb{Z}_q^*$ (160-bit). a hash function $\mathcal{H} : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$. pk=$\{p, q, g, y, \mathcal{H}\}$, sk=$\{x\}$.	bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$, 160-bit prime p, $\lvert\mathbb{G}_1\rvert = \lvert\mathbb{G}_2\rvert = p$, generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, $x, y \in \mathbb{Z}_p^*$, $z = e(g_1, g_2)$, $u = xg_2, v = yg_2$, pk=$\{g_1, g_2, u, v, z\}$, sk=$\{x, y\}$.
Signing	for message m, pick $k \in \mathbb{Z}_q^*$, compute $r = (g^k \bmod p) \bmod q$, $s = k^{-1}(\mathcal{H}(m) + xr) \bmod q$, output the signature (r, s).	for message $m \in \mathbb{Z}_p$, pick $r \in Z_p$, compute $\sigma = \frac{1}{x+m+yr} g_1$, output the signature (σ, r).
Storage	(r, s): 320 bits.	(σ, r): 320 bits.
Computation	about 160 multiplications modulo p (1024-bit).	about 160 point additions in $\mathbb{G}_1$.
Verifying	$(g^{\mathcal{H}(m)s^{-1}} y^{rs^{-1}} \bmod p) \bmod q = r$, where s^{-1} is computed in $\mathbb{Z}_q^*$.	$e(\sigma, u \oplus mg_2 \oplus rv) = z$.
Computation	about 320 multiplications modulo p (1024-bit).	about 320 point additions in $\mathbb{G}_2$, for computing $\rho := u \oplus mg_2 \oplus rv$; about 320 point additions in $E(K)$, where $\mu_p \subset K$, not in $\mathbb{G}_1$ or $\mathbb{G}_2$, for computing $f_{p,\sigma}$, $f_{p,\rho}$; about 320 valuations for $f_{p,\sigma}(\rho)$, $f_{p,\rho}(\sigma)$. Each valuation needs 4 multiplications and 1 inverse over the extension field K (1024-bit).

Table 2: Comparisons between DSA and Boneh-Boyen signature

Remark. Taking into account the time delay for processing the long and complicated programming code of Boneh-Boyen signature, we conjecture DSA is almost 60 times faster than Boneh-Boyen signature.

4.2 The controversial setting of master key in PBC schemes

We know most PBC schemes have to set a master key for generating users' private keys. That is to say, each user's private key is not truly exclusive in theory, although there are some suggestions for alleviating this problem by introducing more key-generating centers. The inherent drawback of PBC indeed counteracts the benefits from ID-based public keys and bilinear property of parings.

5 Difficulties of implementing PBC schemes

To the best of our knowledge, there were few industrial products being integrated with paring-based cryptosystems. The reasons for this situation could be summarized as follows: (1) the pairing computation is hard to understand for most engineers; (2) the issue of key escrow in PBC does not exist with the current PKI system; (3) the heavy group operation of PBC really lowers the advantages that gained from smaller key size. In view of these difficulties, frankly speaking, we do not think it is possible for PBC to practically replace the position of RSA or ElGamal in the next twenty years.

For the current status of "applied" paring-based cryptography, we refer to the following links.

PBC Library [`http://crypto.stanford.edu/pbc/`]; pbc-0.5.14 (Released on Jun 14, 2013).

JPBC Library [`http://gas.dia.unisa.it/projects/jpbc/faq.html`]; v2.0.0 (Released on Dec 04, 2013).

TinyPairing [`http://www.cs.cityu.edu.hk/~ecc/TinyPairing/`]. TinyPairing v0.1 (Released on Oct 09, 2009).

Jmiracl [`https://dsl-external.bbn.com/tracsvr/openP3S/wiki/jmiracl\`].

6 Conclusion

The proposal of ID-based public key, suggested by Shamir [23] in 1984, aimed originally to mitigate the burden of key management. Thirty years later, we find the burden is not as heavy as one imagined before. The current PKI system works well. In some ways, the ID-based public key cryptography has become a pure academic issue. Thus, pairing-based cryptography shall lose its competitive advantages although it looks very beautiful. Just as the saying goes: "Beautiful flowers produce no fruits".

References

[1] D. Boneh. *Pairing-Based Cryptography: Past, Present, and Future.* In proceedings of Asiacrypt 2012. Lecture Notes in Computer Science, vol. 7658, pp. 1, Springer-Verlag, 2012.

[2] D. Boneh and X. Boyen. *Short Signatures without Random Oracles*, Journal of Cryptology, 21(2), pp. 149-177, 2008.

[3] D. Boneh, X. Boyen. *Efficient Selective Identity-Based Encryption Without Random Oracles*. J. Cryptology 24(4): 659-693, 2011.

[4] D. Boneh, X. Boyen and E. Goh. *Hierarchical Identity Based Encryption with Constant Size Ciphertext*, In proceedings of Eurocrypt 2005, Lecture Notes in Computer Science, Vol. 3494, pp. 440-456, Springer-Verlag, 2005.

[5] D. Boneh, X. Boyen and H. Shacham. *Short Group Signatures*, In proceedings of Crypto'04, Lecture Notes in Computer Science, vol. 3152, pp. 41-55, Springer-Verlag, 2004.

[6] D. Boneh and M. Franklin. *Identity-Based Encryption from the Weil Pairing*. In proceedings of Crypto 2001. Lecture Notes in Computer Science, vol. 2139, pp. 213-229. Springer-Verlag, 2001.

[7] D. Boneh, C. Gentry, B. Lynn, H. Shacham. *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*. In proceedings of Eurocrypt 2003, Lecture Notes in Computer Science, vol. 2656, PP. 416-432, Springer-Verlag, 2003.

[8] D. Boneh and M. Hamburg. *Generalized Identity Based and Broadcast Encryption Schemes*, In proceedings of Asiacrypt 2008, Lecture Notes in Computer Science, vol. 5350, 455-470, Springer-Verlag, 2008.

[9] D. Boneh, A. Raghunathan and G. Segev. *Function-Private Identity-Based Encryption: Hiding the Function in Functional Encryption*. In proceedings of Crypto 2013, Lecture Notes in Computer Science, Vol. 8043, pp. 461-478, Springer-Verlag, 2013.

[10] D. Boneh, A. Raghunathan and G. Segev. *Function-Private Subspace-Membership Encryption and Its Applications*. In proceedings of Asiacrypt 2013, Lecture Notes in Computer Science, Vol. 8269, pp. 255-275, Springer-Verlag, 2013.

[11] D. Boneh, H. Shacham and B. Lynn. *Short Signatures from the Weil Pairing*, Journal of Cryptology, Vol. 17, No. 4, pp. 297-319, 2004.

[12] D. Boneh, A. Sahai and B. Waters. *Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys*. In proceedings of Eurocrypt 2006, Lecture Notes in Computer Science, Vol. 4004, pp. 573-592, Springer-Verlag, 2006.

[13] D. Boneh, R. Canetti, S. Halevi and J. Katz. *Chosen-Ciphertext Security from Identity-Based Encryption*. SIAM J. Comput. 36(5): 1301-1328, 2007.

[14] J. Coron. *A Variant of Boneh-Franklin IBE with a Tight Reduction in the Random Oracle Model*. Des. Codes Cryptography 50(1): 115-133, 2009.

[15] I. Blake, G. Seroussi and N. Smart. *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

[16] R. Balasubramanian and N. Koblitz. *The Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the MenezesCOkamotoCVanstone Algorithm*. J. Cryptology, 11, pp. 141C145, 1998.

[17] D. Hankerson, A. Menezes and S. Vanstone. *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[18] A. Joux. *A One Round Protocol for Tripartite Diffie-Hellman*, In proceedings of fourth algorithmic number theory symposium, Lecture Notes in Computer Science, Vol. 1838, Springer-Verlag, pp. 385-394, Springer-Verlag, 2000.

[19] N. Koblitz. *Elliptic Curve Cryptosystems*. Mathematics of Computation, 48:203C209, 1987.

[20] V. Miller. *Use of Elliptic Curves in Cryptography*, In proceedings of Crypto'85, Lecture Notes in Computer Science, vol. 218, 417C426, Springer-Verlag, 1986.

[21] V. Miller. *The Weil Pairing, and Its Efficient Calculation*, J. Cryptology (2004) 17: 235C261.

[22] A. Menezes, T. Okamoto and S. Vanstone. *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, IEEE Transactions on Information Theory 39(5): 1639-1646, 1993.

[23] A. Shamir. *Identity-based Cryptosystems and Signature Schemes*, In proceedings of Crypto'84, Lecture Notes in Computer Science, Vol. 196, pp. 47-53, Springer-Verlag, 1984.

[24] J. Silverman. *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.