Introduction to Identity-Based Encryption

Luther Martin

ARTECH
HOUSE

BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

ISBN-13: 978-1-59693-238-8

Cover design by Yekaterina Ratner

685 Canton Street
Norwood, MA 02062

10 9 8 7 6 5 4 3 2 1

Contents

Preface *xiii*

1 Introduction 1

1.1 What Is IBE? 1

1.2 Why Should I Care About IBE? 8

References 13

2 Basic Mathematical Concepts and Properties 15

2.1 Concepts from Number Theory 15
2.1.1 Computing the GCD 16
2.1.2 Computing Jacobi Symbols 24

2.2 Concepts from Abstract Algebra 25

References 39

3 Properties of Elliptic Curves 41

3.1 Elliptic Curves 41

3.2 Adding Points on Elliptic Curves 47
3.2.1 Algorithm for Elliptic Curve Point Addition 52
3.2.2 Projective Coordinates 53
3.2.3 Adding Points in Jacobian Projective Coordinates 54

3.2.4	Doubling a Point in Jacobian Projective Coordinates	55
3.3	Algebraic Structure of Elliptic Curves	55
3.3.1	Higher Degree Twists	61
3.3.2	Complex Multiplication	65
	References	66
4	**Divisors and the Tate Pairing**	**67**
4.1	Divisors	67
4.1.1	An Intuitive Introduction to Divisors	68
4.2	The Tate Pairing	76
4.2.1	Properties of the Tate Pairing	81
4.3	Miller's Algorithm	84
	References	87
5	**Cryptography and Computational Complexity**	**89**
5.1	Cryptography	91
5.1.1	Definitions	91
5.1.2	Protection Provided by Encryption	93
5.1.3	The Fujisaki-Okamoto Transform	95
5.2	Running Times of Useful Algorithms	95
5.2.1	Finding Collisions for a Hash Function	96
5.2.2	Pollard's Rho Algorithm	98
5.2.3	The General Number Field Sieve	99
5.2.4	The Index Calculus Algorithm	102
5.2.5	Relative Strength of Algorithms	102
5.3	Useful Computational Problems	104
5.3.1	The Computational Diffie-Hellman Problem	105
5.3.2	The Decision Diffie-Hellman Problem	106
5.3.3	The Bilinear Diffie-Hellman Problem	107
5.3.4	The Decision Bilinear Diffie-Hellman Problem	107
5.3.5	q-Bilinear Diffie-Hellman Inversion	108
5.3.6	q-Decision Bilinear Diffie-Hellman Inversion	109
5.3.7	Cobilinear Diffie-Hellman Problems	109

5.3.8 Integer Factorization 109
5.3.9 Quadratic Residuosity 109

5.4 Selecting Parameter Sizes 110
5.4.1 Security Based on Integer Factorization and Quadratic Residuosity 110
5.4.2 Security Based on Discrete Logarithms 110

5.5 Important Special Cases 111
5.5.1 Anomalous Curves 112
5.5.2 Supersingular Elliptic Curves 112
5.5.3 Singular Elliptic Curves 113
5.5.4 Weak Primes 113

5.6 Proving Security of Public-Key Algorithms 114

5.7 Quantum Computing 116
5.7.1 Grover's Algorithm 116
5.7.2 Shor's Algorithm 117

References 118

6 Related Cryptographic Algorithms 121

6.1 Goldwasser-Michali Encryption 121

6.2 The Diffie-Hellman Key Exchange 124

6.3 Elliptic Curve Diffie-Hellman 125

6.4 Joux's Three-Way Key Exchange 126

6.5 ElGamal Encryption 128

References 129

7 The Cocks IBE Scheme 131

7.1 Setup of Parameters 131

7.2 Extraction of the Private Key 133

7.3 Encrypting with Cocks IBE 133

7.4 Decrypting with Cocks IBE 135

7.5 Examples 136

7.6	Security of the Cocks IBE Scheme	139
7.6.1	Relationship to the Quadratic Residuosity Problem	139
7.6.2	Chosen Ciphertext Security	142
7.6.3	Proof of Security	142
7.6.4	Selecting Parameter Sizes	143
7.7	Summary	143
	References	145
8	**Boneh-Franklin IBE**	**147**
8.1	Boneh-Franklin IBE (Basic Scheme)	149
8.1.1	Setup of Parameters (Basic Scheme)	149
8.1.2	Extraction of the Private Key (Basic Scheme)	150
8.1.3	Encrypting with Boneh-Franklin IBE (Basic Scheme)	150
8.1.4	Decrypting with Boneh-Franklin IBE (Basic Scheme)	151
8.1.5	Examples (Basic Scheme)	151
8.2	Boneh-Franklin IBE (Full Scheme)	156
8.2.1	Setup of Parameters (Full Scheme)	156
8.2.2	Extraction of the Private Key (Full Scheme)	157
8.2.3	Encrypting with Boneh-Franklin IBE (Full Scheme)	157
8.2.4	Decrypting with Boneh-Franklin IBE (Full Scheme)	158
8.3	Security of the Boneh-Franklin IBE Scheme	158
8.4	Summary	159
	Reference	160
9	**Boneh-Boyen IBE**	**161**
9.1	Boneh-Boyen IBE (Basic Scheme—Additive Notation)	162
9.1.1	Setup of Parameters (Basic Scheme—Additive Notation)	162
9.1.2	Extraction of the Private Key (Basic Scheme—Additive Notation)	164

9.1.3 Encrypting with Boneh-Boyen IBE (Basic Scheme—Additive Notation) 164
9.1.4 Decrypting with Boneh-Boyen IBE (Basic Scheme—Additive Notation) 164

9.2 Boneh-Boyen IBE (Basic Scheme—Multiplicative Notation) 168
9.2.1 Setup of Parameters (Basic Scheme—Multiplicative Notation) 168
9.2.2 Extraction of the Private Key (Basic Scheme—Multiplicative Notation) 170
9.2.3 Encrypting with Boneh-Boyen IBE (Basic Scheme—Multiplicative Notation) 170
9.2.4 Decrypting with Boneh-Boyen IBE (Basic Scheme—Multiplicative Notation) 170

9.3 Boneh-Boyen IBE (Full Scheme) 171
9.3.1 Setup of Parameters (Full Scheme) 172
9.3.2 Extraction of the Private Key (Full Scheme) 173
9.3.3 Encrypting with Boneh-Boyen IBE (Full Scheme) 173
9.3.4 Decrypting with Boneh-Boyen IBE (Full Scheme) 173

9.4 Security of the Boneh-Boyen IBE Scheme 174

9.5 Summary 175

Reference 176

10 Sakai-Kasahara IBE 177

10.1 Sakai-Kasahara IBE (Basic Scheme—Additive Notation) 177
10.1.1 Setup of Parameters (Basic Scheme—Additive Notation) 178
10.1.2 Extraction of the Private Key (Basic Scheme—Additive Notation) 178
10.1.3 Encrypting with Sakai-Kasahara IBE (Basic Scheme—Additive Notation) 180
10.1.4 Decrypting with Sakai-Kasahara IBE (Basic Scheme—Additive Notation) 180

10.2 Sakai-Kasahara IBE (Basic Scheme—Multiplicative Notation) 182

10.2.1 Setup of Parameters (Basic Scheme—Multiplicative Notation) 182
10.2.2 Extraction of the Private Key (Basic Scheme—Multiplicative Notation) 183
10.2.3 Encrypting with Sakai-Kasahara IBE (Basic Scheme—Multiplicative Notation) 184
10.2.4 Decrypting with Sakai-Kasahara IBE (Basic Scheme—Multiplicative Notation) 184

10.3 Sakai-Kasahara IBE (Full Scheme) 185
10.3.1 Setup of Parameters (Full Scheme) 185
10.3.2 Extraction of the Private Key (Full Scheme) 185
10.3.3 Encrypting with Sakai-Kasahara IBE (Full Scheme) 185
10.3.4 Decrypting with Sakai-Kasahara IBE (Full Scheme) 187

10.4 Security of the Sakai-Kasahara IBE Scheme 187

10.5 Summary 188

Reference 189

11 Hierarchial IBE and Master Secret Sharing 191

11.1 HIBE Based on Boneh-Franklin IBE 193
11.1.1 GS HIBE (Basic) Root Setup 194
11.1.2 GS HIBE (Basic) Lower-Level Setup 194
11.1.3 GS HIBE (Basic) Extract 194
11.1.4 GS HIBE (Basic) Encrypt 194
11.1.5 GS HIBE (Basic) Decrypt 195

11.2 Example of a GS HIBE System 195
11.2.1 GS HIBE (Basic) Root Setup 196
11.2.2 GS HIBE (Basic) Lower-Level Setup 196
11.2.3 GS HIBE (Basic) Extraction of Private Key 196
11.2.4 GS HIBE (Basic) Encryption 197
11.2.5 GS HIBE (Basic) Decryption 197

11.3 HIBE Based on Boneh-Boyen IBE 197
11.3.1 BBG HIBE (Basic) Setup 198
11.3.2 BBG HIBE (Basic) Extract 199

11.3.3 BBG HIBE (Basic) Encryption 199
11.3.4 BBG HIBE (Basic) Decryption 199

11.4 Example of a BBG HIBE System 200
11.4.1 BBG HIBE (Basic) Setup 200
11.4.2 BBG HIBE (Basic) Extraction of Private Key 200
11.4.3 BBG HIBE (Basic) Encryption 201
11.4.4 BBG HIBE (Basic) Decryption 201

11.5 Master Secret Sharing 201

11.6 Master Secret Sharing Example 202

References 204

12 Calculating Pairings 207

12.1 Pairing-Friendly Curves 207
12.1.1 Relative Efficiency of Parameters of Pairing-Friendly Curves 209

12.2 Eliminating Irrelevant Factors 210
12.2.1 Eliminating Random Components 211
12.2.2 Eliminating Extension Field Divisions 214
12.2.3 Denominator Elimination 215

12.3 Calculating the Product of Pairings 216

12.4 The Shipsey-Stange Algorithm 217

12.5 Precomputation 221

References 222

Appendix: Useful Test Data 225

About the Author 229

Index 231

4

Divisors and the Tate Pairing

This chapter introduces divisors, which are then used to construct the Tate pairing. The Tate pairing in turn provides the basis for many IBE schemes, including the Boneh-Franklin, Bohen-Boyen, and Sakai-Kasahara schemes. The discussion of the Tate pairing here is designed to provide an overview of the pairing, its properties, and how to calculate it. Further detail of the properties of the Tate pairing can be found in [1, 2].

The Tate pairing by itself turns out to be unsuitable for cryptographic applications because it frequently returns the value 1, but by modifying one of the inputs to the Tate pairing using either a distortion map or a point on the twist of an elliptic curve, it is easy to overcome this limitation.

4.1 Divisors

The divisors discussed in this section are very different from those discussed in Chapter 2, but they unfortunately share the same name. In this context, a divisor is a way of characterizing a function f based only on its zeroes, where $f(x) = 0$, and poles, where $f(x) = \pm\infty$, like when dividing by zero. We say that a function $f(x)$ has a pole at infinity if $f(1/x)$ has a pole at $x = 0$, so that a polynomial of degree n has a pole of degree n at infinity. Similarly, we say that a function $f(x)$ has a zero at infinity if $f(1/x)$ has a zero at $x = 0$. For example, the function

$$f(x) = \frac{(x-1)^2}{(x+2)^3} = (x-1)^2(x+2)^{-3}$$

has a zero of order 2 at $x = 1$, a zero of order 1 at infinity, and a pole of order 3 at $x = -2$. Because a divisor characterizes a function based on its zeroes and poles, two functions that differ by a constant will have the same divisor.

4.1.1 An Intuitive Introduction to Divisors

We keep track of the zeroes and poles of a rational function f in what we call a divisor, which we write as $div(f)$. We write such a divisor as the sum of the points where f has a zero or pole weighted by the multiplicities of the zeroes and poles, with the convention that zeroes get positive weights according to their multiplicities and poles get negative weights according to their multiplicities. In the example above, we write $div(f) = 2(1) + (\infty) - 3(-2)$, to indicate that f has a zero of order 2 at $x = 1$, a zero or order 1 at infinity, and a pole of order 3 at $x = -2$. In general, if we can write

$$f(x) = \prod_i (x - x_i)^{a_i}$$

then we write

$$div(f) = \sum_i a_i (x_i)$$

The notation for divisors can be a bit tricky, and we will need to be able tell from the context that we dealing with divisors instead of numbers, so that we are not tempted to treat divisors as numbers, trying to simplify expressions like $2(1) - 3(-2)$ to get a number instead of a divisor.

Note that multiplying rational functions corresponds to addition of their divisors and division of rational functions corresponds to subtraction of their divisors. So if we have $f(x)$ as defined above and

$$g(x) = \frac{(x+2)^3}{(x+1)^4}$$

then

$$\begin{aligned} f(x)g(x) &= \frac{(x-1)^2}{(x+2)^3}\frac{(x+2)^3}{(x+1)^4} \\ &= \frac{(x-1)^2}{(x+1)^4} \end{aligned}$$

which corresponds to adding the divisors:

$$\begin{aligned} div(fg) &= div(f) + div(g) \\ &= 2(1) + (\infty) - 3(-2) + 3(-2) + (\infty) - 4(-1) \\ &= 2(1) + 2(\infty) - 4(-1) \end{aligned}$$

We can formalize this informal description of divisors with the following definitions.

Definition 4.1

A *formal sum* of a set S is series $\{s_0, s_1, s_2, \ldots\}$ of elements of S. A formal sum is often written using a placeholder, with the understanding that the placeholder is not to be evaluated.

Example 4.1

(i) A power series is a formal sum which we usually write as $a_0 + a_1x + a_2x^2 + \ldots$, where each $a_i \in S$ for some set S. We write a power series with the understanding that the placeholder x is not to be evaluated, and we could also write the same power series as $\{a_0, a_1, a_2, \ldots\}$.

(ii) If $P = \{P_1, P_2, \ldots P_n\}$ is a set of points on an elliptic curve, then $D = a_1(P_1) + a_2(P_2) + \ldots + a_n(P_n)$ is a formal sum of the elements of P. In this case, we understand that in D the points in the set P are just placeholders like the variable x in a power series, and are not to be evaluated.

Definition 4.2

Let E be an elliptic curve. A *divisor* on E is a formal sum of the form

$$D = \sum_{P \in E} n_P(P)$$

where each n_P is an integer and all but finitely many n_P are zero.

Example 4.2

For points P_1 and P_2 on an elliptic curve, $D = (P_1) + 2(P_2) - 3(O)$ is a divisor.

Definition 4.3

We say that a divisor D is a *principal divisor* if there is a rational function f such that $D = div(f)$. An equivalent definition is that a divisor D on an elliptic curve is principal if we can write

$$D = \sum_i a_i(P_i)$$

where $\sum a_i = 0$ and $\sum a_i P_i = O$, with the last sum using the addition of points on an elliptic curve. In particular, if P is a point of order n, then the divisor $n(P) - n(O)$ is a principal divisor.

Example 4.3

(i) Let P_1, P_2 and P_3 be points on an elliptic curve with $P_3 = P_1 + P_2$. Then $D = (P_1) + (P_2) + (-P_3) - 3(O)$ is a principal divisor.

(ii) Let P be a point on an elliptic curve of order n. Then $D = n(P) - n(O)$ is a principal divisor.

Definition 4.4

If E is an elliptic curve and

$$D = \sum_{P \in E} n_P(P)$$

is a divisor then the *support* of D is the set of all points P such that $n_P \neq 0$.

Example 4.4

For the divisor $D = (P_1) + (P_2) + (-P_3) - 3(O)$, the support of D is the set $\{P_1, P_2, -P_3, O\}$.

Definition 4.5

Let D_1 and D_2 be divisors. Then we say that D_1 and D_2 have *disjoint support* if the intersection of the support of D_1 and the support of D_2 is the empty set, or $D_1 \cap D_2 = \varnothing$.

Example 4.5

(i) The divisors $D_1 = (P_1) - (O)$ and $D_2 = (P_1 + R) - (R)$ have disjoint support as long as $\{P_1, O\} \cap \{P_1 + R, R\} = \varnothing$.

(ii) The divisors $D_1 = (P) - (O)$ and $D_2 = (Q) - (O)$ do not have disjoint support.

We can think of the divisors as keeping track of where the graph of an elliptic curve E intersects the graph of a function $f(x)$, or where $E = f(x)$, so they keep track of zeroes and poles of $E = f(x)$. In particular, we get a zero when $E = f(x)$, or when the function $f(x)$ crosses the elliptic curve E and we get a pole when $f(x)$ has a pole.

The functions u and v that appear in Figure 4.1 are very important in implementing operations on divisors, and in the following, u will always represent a line through two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on an elliptic curve and v will always represent a vertical line that goes through $P_3 = (x_3, y_3)$, where $P_3 = P_1 + P_2$.

Suppose that we do not have the case where $P_1 + P_2 = O$ and neither $P_1 = O$ nor $P_2 = O$. Then we can write the point-slope form of a line through (x_1, y_1) as

$$y - y_1 = m(x - x_1)$$

or

$$y - y_1 = -mx + mx_1 = 0$$

which gives us an explicit way to find the line u. Similarly, the line v is given by

$$x - x_3 = 0$$

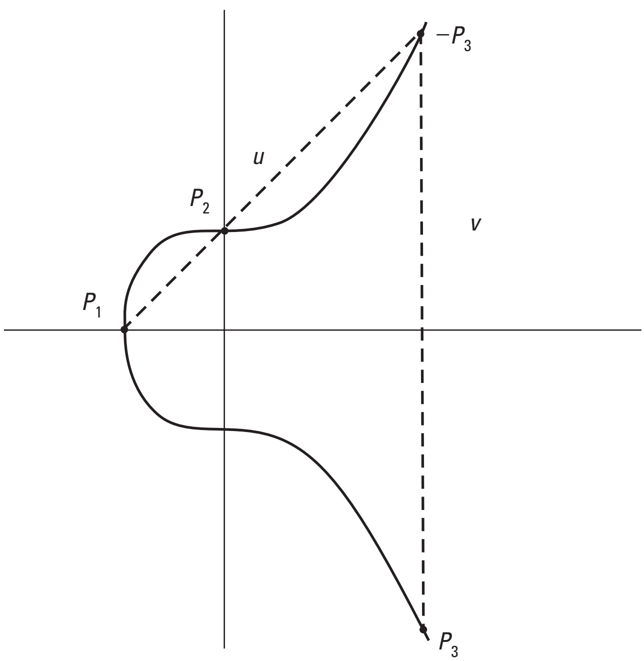

Figure 4.1 Illustration of the lines u and v in the addition of points on an elliptic curve.

If one of the two points is O, then u is the vertical line through the point that is not O, and if the point $(x_3, y_3) = O$ then v is the vertical line $x = 0$. These forms of the lines (x_1, y_1) and (x_1, y_1) are shown in Figure 4.2. The cases where either $P_1 = O$, $P_2 = O$, or $P_1 = P_2$ are shown in Algorithm 4.2, 4.3, and 4.4.

The particular points that we use to define the lines u and v should be clear from the context, so we will usually omit the points to keep the notation simpler. If we need to clarify which points are being used, we will write u_{P_1,P_2} or v_{P_3} to indicate the line through P_1 and P_2 or the vertical line through P_3, respectively. With this notation, u and v have the following divisors:

$$div(u) = (P_1) + (P_2) + (-P_3) - 3(O)$$

$$div(v) = (P_3) + (-P_3) - 2(O)$$

where we have now accounted for the poles that the lines u and v have at O.

Another useful fact is what we get when we subtract the divisor of u from the divisor of v:

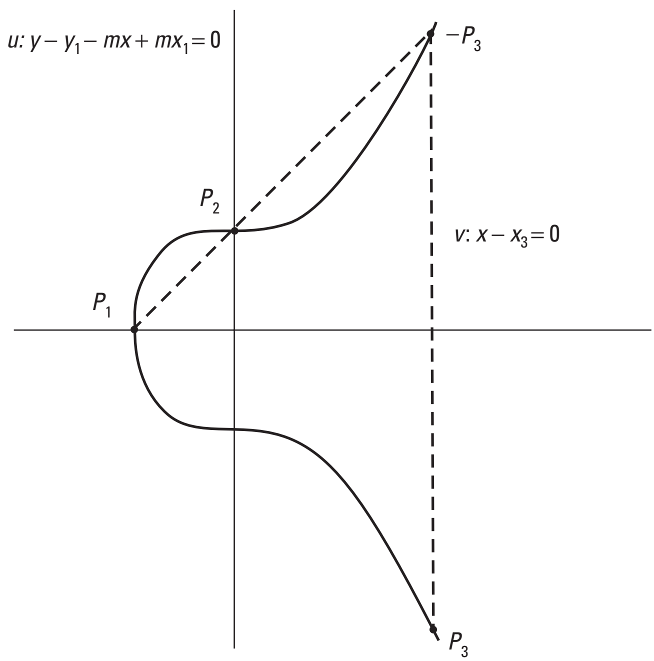

Figure 4.2 Forms of the lines u and v used to add divisors on an elliptic curve.

$$div(u) - div(v) = div(u/v) \tag{4.1}$$
$$= (P_1) + (P_2) + (P_3) - (O)$$

If we have two divisors of the form:

$$D_1 = (P_1) - (O) + div(f_1)$$
$$D_2 = (P_2) - (O) + div(f_2)$$

we can add the two divisors to get

$$D_1 + D_2 = (P_1) + (P_2) - 2(O) + div(f_1 f_2) \tag{4.2}$$

Solving for $(P_1) + (P_2)$ in (4.1) and substituting the result into (4.2) we find that

$$D_1 + D_2 = (P_3) - (O) + div(f_1 f_2 u/v) \tag{4.3}$$

So the divisors of the lines u and v provide a way to add two divisors and keep the result in the form $(P) - (O) + div(f)$.

To clarify how this works, we will now step through a calculation of the sum of two divisors, where the arithmetic is done on the curve $y^2 = x^3 + 1$ over $\mathbb{F}_5$, as is defined in Table 3.2.

In particular, we consider the divisor $D = (\hat{P}_2) - (O)$ and see what we get when we add it to itself. Using (4.3) and the fact that we can also write the divisor D as $div(1)$ we find that

$$D + D = (\hat{P}_2) - (O) + div(1) + (\hat{P}_2) - (O) + div(1)$$
$$= (\hat{P}_1) - (O) + div(u/v)$$

Now u is the line tangent to the elliptic curve at $\hat{P}_2$, and v is the line connecting $\hat{P}_2 + \hat{P}_2 = \hat{P}_1$ and $-(\hat{P}_2 + \hat{P}_2) = \hat{P}_2$. Solving for u and v we find that we have $y - 4 = 0$ for the line u, or $y + 1 = 0$ in $\mathbb{F}_5$. Similarly, we have $x = 0$ for the line v. Substituting these for u and v we get that

$$D + D = (\hat{P}_1) - (O) + div\left(\frac{y+1}{x}\right)$$

If we add the divisor D to this sum one more time we find that we are just left with the divisor of a rational function when the terms of the divisor involving points on the curve cancel each other when we reach

$3D = 3(\hat{P}_2) - 3(O)$ because $\hat{P}_2$ is a point of order 3. At the next step, the line u through $\hat{P}_1$ and $\hat{P}_2$ is the vertical line $x = 0$, since $x = 0$ is the common x coordinate that $\hat{P}_1$ and $\hat{P}_2$ share. We define the vertical line v through the point $\hat{P}_1 + \hat{P}_2 = O$ to be 1. Thus, we have

$$\begin{aligned} 3D &= 3(\hat{P}_2) - 3(O) \\ &= (\hat{P}_2 + \hat{P}_1) - (O) + div\left(\frac{y+1}{x}\frac{u}{v}\right) \\ &= (O) - (O) + div\left(\frac{y+1}{x}\frac{x}{1}\right) \\ &= div(y+1) \end{aligned}$$

Definition 4.6

If D is a divisor of the form

$$D = \sum_i a_i(P_i)$$

then we define what it means to evaluate a rational function f at D by

$$f(D) = \prod_i f(P_i)^{a_i}$$

Example 4.6

(i) If $D = 2(P_1) - 3(P_2)$ then

$$\begin{aligned} f(D) &= f(P_1)^2 f(P_2)^{-3} \\ &= \frac{f(P_1)^2}{f(P_2)^3} \end{aligned}$$

(ii) If $P = (2, 3)$ and $Q = (0, 1)$ are points on $E/\mathbb{F}_{11}$ and D is the divisor $D = (P) - (Q)$ and f is the rational function $f(x, y) = y + 1$, then

$$f(D) = \frac{3+1}{1+1} = 4 \cdot 2^{-1} = 4 \cdot 6 \equiv 2 \pmod{11}$$

In many cases, it is possible to exchange the roles of a function f and a divisor D in expressions like $f(D)$. This is formalized in the following.

Property 4.1 (Weil Reciprocity)

Let f and g be rational functions defined on some field F. If $div(f)$ and $div(g)$ have disjoint support then we have that $f(div(g)) = g(div(f))$.

Example 4.7

Suppose that we have two rational functions f and g defined on $\mathbb{F}_{11}$ where

$$f(x) = \frac{x-2}{x-7}$$

and

$$g(x) = \frac{x-6}{x-5}$$

so that we have

$$div(f) = (2) - (7)$$

and

$$div(g) = (6) - (5)$$

then

$$f(div(g)) = \frac{f(6)}{f(5)} = \frac{7}{4} = 7 \cdot 3 = 10 \pmod{11}$$

and

$$g(div(f)) = \frac{g(2)}{g(7)} = \frac{5}{6} = 5 \cdot 2 = 10 \pmod{11}$$

Definition 4.7

Divisors D_1 and D_2 are *equivalent* if they differ by a principal divisor, that is, $D = D_1 - D_2$ is a principal divisor.

Example 4.8

(i) If f is a rational function, the divisors $(P) - (O)$ and $(P) - (O) + div(f)$ are equivalent.

(ii) We can see that $(P + R) - (R)$ is equivalent to $(P) - (O)$ by using the line u that goes through the points P, R and $-(P + R)$ and the line v that goes through the points $-(P + R)$ and $P + R$. Then we have that

$$div(u) = (P) + (R) + (-(P + R)) - 3(O)$$
$$div(v) = (-(P + R)) + (P + R) - 2(O)$$

so that

$$(P) - (O) = (P + R) - (R) + div(u/v)$$

So the difference between $(P + R) - (R)$ and $(P) - (O)$ is a principal divisor, since it is the divisor of the rational function u/v, and $(P + R) - (R)$ is equivalent to $(P) - (O)$.

4.2 The Tate Pairing

Now that we have defined divisors and how to manipulate them, we can define the Tate pairing and describe how to calculate it. The Tate pairing operates on pairs of points $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_{q^k})$, and produces a result in $\mathbb{F}^*_{q^k}$. We write $e(P, Q)$ for the Tate pairing of the points P and Q. For a point P of order n, to get $e(P, Q)$ we first find a rational function f_P so that $div(f_P)$ is equivalent to $n(P) - n(O)$ and then evaluate f_P at a divisor equivalent to $(Q) - (O)$. We can summarize this in the following.

Definition 4.8

Let $E/\mathbb{F}_q$ be an elliptic curve, $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_{q^k})$. Let f_P be a rational function with $div(f_P)$ equivalent to $n(P) - n(O)$ and A_Q be a divisor equivalent to $(Q) - (O)$ with the support of $div(f_P)$ and A_Q disjoint. Then the Tate pairing is defined to be $e(P, Q) = f_P(A_Q)$. This definition does not produce a unique value, and will include a constant that is an nth power of some element of $\mathbb{F}_{q^k}$.

It is not immediately obvious why the Tate pairing is well defined by this definition. So we should convince ourselves that this definition is actually independent of our choices for f_P and A_Q. In doing so, we will see why the Tate pairing is only defined up to multiplication by an nth power of some constant. In the following we will see that it is easy to get rid of this unwanted constant, leaving a unique value.

Note that f_P is defined up to a constant multiple. Applying the definition of evaluating a divisor at a function to such a constant multiple shows that this has no influence on the value of $f_P(A_Q)$, so it is independent of the choice of f_P.

Now suppose that D_1 and D_2 are both divisors equivalent to $(Q) - (O)$, say $D_1 = D_2 + div(g)$ for some rational function g. To be careful, we also need to assume that the support of $div(f_P)$ is disjoint from the support of $div(g)$. Then we have that

$$\begin{aligned} f_P(D_1) &= f_P(D_2 + div(g)) \\ &= f_P(D_2) f_P(div(g)) \\ &= f_P(D_2) g(div(f_P)) \text{ (by Weil reciprocity)} \\ &= f_P(D_2) g(n(P) - n(O)) \\ &= f_P(D_2) g((P) - (O))^n \end{aligned}$$

We can then abuse the notation of congruences slightly to write this as

$$f_P(D_1) \equiv f_P(D_2)$$

which we think of as meaning that $f_P(D_1) = f_P(D_2)$ up to a constant that is an nth power.

The examples of adding divisors above show how to find a divisor equivalent to $n(P) - n(O)$: we can add the divisor $(P) - (O)$ to itself n times by using the divisors $div(u)$ and $div(v)$ that we get from the lines through various points on the elliptic curve, and after reaching $n(P) - n(O)$ we will be left with a divisor of a rational function that we call f_P when all of the terms involving the point P disappear. To avoid the troubles with evaluating a function at the point at infinity that appears in $(Q) - (O)$, we can pick a random point R on our elliptic curve and evaluate f_P at $(Q + R) - (R)$ instead, which is equivalent to the divisor $(Q) - (O)$.

Because the point P is of order n, if we repeatedly add the divisor $(P) - (O)$ to get $n(P) - n(O)$ using the technique that is summarized in (4.3), we find that we end up with a divisor of a rational function that is the product of terms of the form u/v, where u is the line through two points (the points P_1 and P_2 in Figure 4.1, for example) on our elliptic curve and v is the vertical line that passes though the point that is the sum of the same two points (the point P_3 in Figure 4.1, for example).

Suppose that A_Q is a divisor of the form $(Q + R) - (R)$ that we get from a random $R \neq O$. Note that the requirement that the support of the divisors $n(P) - n(O)$ and A_Q are disjoint means that $Q + R \neq P$, and $R \neq P$. We exclude these cases because they either reduce the value of the pairing to zero by introducing a factor of zero in a calculation, or cause a division by zero error. An examination of Algorithms 4.2 through 4.4 should clarify the ways in which this can happen.

To give an example of how this works, we will use the same example that we used above to find $e(\hat{P}_2, \hat{P}_2)$. We found that $3(\hat{P}_2) - 3(O)$ is equivalent to the divisor $div(y + 1)$, so we have $f_{\hat{P}_2} = y + 1$. Next, we need a random point to add to $\hat{P}_2$, for which we pick $\hat{P}_4$, so we want to evaluate $f_{\hat{P}_2}$ at $(\hat{P}_2 + \hat{P}_4) - (\hat{P}_4) = (\hat{P}_3) - (\hat{P}_4)$, or we want to find $f_{\hat{P}_2}(\hat{P}_3)/f_{\hat{P}_2}(\hat{P}_4)$. Note that it is possible to pick a random point that causes division by zero, for example if we picked the point $\hat{P}_2$ in this example. If this happens, we can just pick another random point until we find one that works. Substituting the appropriate values from Table 3.2, we find that

$$\begin{aligned} e(\hat{P}_2, \hat{P}_2) &= \frac{f_{\hat{P}_2}(\hat{P}_3)}{f_{\hat{P}_2}(\hat{P}_4)} = \frac{3}{4} \\ &= 3 \cdot 4^{-1} = 2 \in \mathbb{F}_5 \end{aligned} \tag{4.4}$$

As mentioned above, the Tate pairing has an additional multiplicative factor of r^n for some $r \in \mathbb{F}_{q^k}$, so that we actually get $e(P, Q) = a \cdot r^n$ for when we calculate it. From Property 2.13 we have that for any $\xi \in \mathbb{F}_{q^k}$ we have that $\xi^{q^k - 1} = 1$, so if we raise $a \cdot r^n$ to the power $(q^k - 1)/n$ we get that

$$(a \cdot r^n)^{(q^k - 1)/n} = a^{(q^k - 1)/n} \cdot 1 = a^{(q^k - 1)/n}$$

so that such an exponentiation eliminates the extra multiplicative factor and leaves a unique result. Thus while $e(P, Q)$ is not unique, the additional exponentiation that gives us

$$e(P, Q)^{(q^k - 1)/n}$$

determines a unique value, and thus more suitable for many uses. The use of such an exponentiation to determine a unique value is called the *final exponentiation* and the unique value is called the *reduced pairing*.

Example 4.9

(i) Consider the case where we have $E/\mathbb{F}_{11} : y^2 = x^3 + x$ and $P = (5, 3) \in E(\mathbb{F}_{11})$ [3]. To find $f_P(x, y)$ we want to find the rational function so that $div(f_P)$ is equivalent to the divisor $3(P) - 3(O)$. We get this through a repeated application of (4.3).

We want to find

$$\begin{aligned}3(P) - 3(O) &= 3((P) - (O))\\ &= ((P) - (O)) + ((P) - (O)) + ((P) - (O))\end{aligned}$$

We can start calculating this by first finding

$$\begin{aligned}2(P) - 2(O) &= 2((P) - (O))\\ &= ((P) - (O)) + ((P) - (O))\end{aligned}$$

by

$$\begin{aligned}(P) - (O) + (P) - (O) &= (P) - (O) + div(1) + (P) - (O) + div(1)\\ &= (2P) - (O) + div(y + 2x + 9)\end{aligned}$$

Then

$$\begin{aligned}3(P) - 3(O) &= (2P) - (O) + div(y + 2x + 9) + (P) - (O) + div(1)\\ &= (3P) - (O) + div(y + 2x + 9)\\ &= (O) - (O) + div(y + 2x + 9)\\ &= div(y + 2x + 9)\end{aligned}$$

so that

$$f_P(x, y) = y + 2x + 9$$

If we have $Q = (7, 8)$ and $R = (10, 3)$, then $Q + R = (9, 10)$ and we evaluate f_P at $A_Q = (Q + R) - (R)$ we get

$$\begin{aligned}f_P((Q + R) - (R) &= \frac{f_P(Q + R)}{f_P(R)} = \frac{4}{10}\\ &= 4 \cdot 10^{-1} = 4 \cdot 10 \equiv 7 \pmod{11}\end{aligned}$$

Thus $e(P, Q) = f_P(A_Q) = 7$.

(ii) Consider the case where we have $E/\mathbb{F}_{11} : y^2 = x^3 + 1$ and $P = (5, 4) \in E(\mathbb{F}_{11})$ [4]. Because P is of order 4, to find $f_P(x, y)$ we want to find the rational function so that $div(f_P)$ is equivalent to the divisor $4(P) - 4(O)$. We get this through a repeated application of (4.3).

We want to find

$$
\begin{aligned}
4(P) - 4(O) &= 4((P) - (O)) \\
&= ((P) - (O)) + ((P) - (O)) + ((P) - (O)) + ((P) - (O))
\end{aligned}
$$

We can start calculating this by first finding

$$
\begin{aligned}
2(P) - 2(O) &= 2((P) - (O)) \\
&= ((P) - (O)) + ((P) - (O))
\end{aligned}
$$

by

$$
\begin{aligned}
(P) - (O) + (P) - (O) &= (P) - (O) + div(1) + (P) - (O) + div(1) \\
&= (2P) - (O) + div\left(\frac{y + 3x + 3}{x + 1}\right)
\end{aligned}
$$

Then

$$
\begin{aligned}
3(P) - 3(O) &= (2P) - (O) + div\left(\frac{y + 3x + 3}{x + 1}\right) + (P) - (O) + div(1) \\
&= (3P) - (O) + div\left(\frac{(y + 3x + 3)^2}{(x + 1)(x + 6)}\right)
\end{aligned}
$$

And finally

$$
\begin{aligned}
4(P) - 4(O) &= (3P) - (O) + div\left(\frac{(y + 3x + 3)^2}{(x + 1)(x + 6)}\right) + (P) - (O) + div(1) \\
&= (4P) - (O) + div\left(\frac{(y + 3x + 3)^2}{x + 1}\right) \\
&= (O) - (O) + div\left(\frac{(y + 3x + 3)^2}{x + 1}\right) \\
&= div\left(\frac{(y + 3x + 3)^2}{x + 1}\right)
\end{aligned}
$$

so that

$$f_P(x, y) = \frac{(y + 3x + 3)^2}{x + 1}$$

If we have $Q = (5, 7)$ and $R = (9, 9)$, then $Q + R = (0, 1)$ and we evaluate f_P at $A_Q = (Q + R) - (R)$ we get

$$f_P((Q + R) - (R)) = \frac{f_P(Q + R)}{f_P(R)} = \frac{5}{8}$$

$$= 5 \cdot 8^{-1} = 5 \cdot 7 \equiv 2 \pmod{11}$$

Thus $e(P, Q) = f_P(A_Q) = 2$.

4.2.1 Properties of the Tate Pairing

As defined earlier, the Tate pairing has the following properties:

1. The Tate pairing is *nondegenerate*, that is, for each $P \in E(\mathbb{F}_q)[n]/\{O\}$ there is some $Q \in E(\mathbb{F}_{q^k})$ with $e(P, Q) \neq 1$.
2. The Tate pairing is *bilinear*, that is, for each $P, P_1, P_2 \in E(\mathbb{F}_q)[n]$ and $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})$ we have $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$.

To convince ourselves that the Tate pairing is bilinear, we need to consider two separate cases.

To see that the Tate pairing is linear in its first parameter, let f_{P_1}, f_{P_2}, and $f_{P_1+P_2}$ be rational functions such that we have

$$div\left(f_{P_1}\right) = n(P_1) - n(O)$$

$$div\left(f_{P_2}\right) = n(P_2) - n(O)$$

and

$$div\left(f_{P_1+P_2}\right) = n(P_1 + P_2) - n(O)$$

Note that the divisor

$$D = (P_1 + P_2) - (P_1) - (P_2) + (O)$$

is a principal divisor so it is the divisor of some rational function, say

$$div(g) = D$$

then

$$div\left(f_{P_1+P_2}\right) - div(f_1) - div(f_2) = n(P_1 + P_2) - n(P_1) - n(P_2) - n(O)$$
$$= nD = ndiv(g) = div(g^n)$$

so that

$$div\left(f_{P_1+P_2}\right) = div(f_1) + div(f_2) + div(g^n)$$

so we can write

$$f_{P_1+P_2} = f_1 f_2 g^n$$

Thus

$$e(P_1 + P_2, Q) = f_{P_1+P_2}(A_Q) = f_{P_1}(A_Q) f_{P_2}(A_Q) g^n(A_Q)$$
$$= e(P_1, Q)\, e(P_2, Q)\, g^n(A_Q)$$

So if we are ignoring nth powers, we find that

$$e(P_1 + P_2, Q) = e(P_1, Q)\, e(P_2, Q)$$

as desired.

To see that the Tate pairing is bilinear in the second parameter, let $A_{Q_1+Q_2}$ be a divisor equivalent to $(Q_1 + Q_2) - (O)$, A_{Q_1} be a divisor equivalent to $(Q_1) - (O)$ and A_{Q_2} be a divisor equivalent to $(Q_1) - (O)$. Then $A_{Q_1+Q_2} - A_{Q_1} - A_{Q_2}$ is equivalent to

$$D = (Q_1 + Q_2) - (Q_1) - (Q_2) + (O)$$

which is a principal divisor. So $A_{Q_1+Q_2}$ is equivalent to $A_{Q_1} + A_{Q_2}$ because they differ by a principal divisor. Thus we can write

$$e(P, Q_1 + Q_2) = f_P\left(A_{Q_1+Q_2}\right)$$
$$= f_P\left(A_{Q_1} + A_{Q_2}\right) = f_P\left(A_{Q_1}\right) f_P\left(A_{Q_2}\right)$$
$$= e(P, Q_1)\, e(P, Q_2)$$

A mapping that is nondegenerate and bilinear and is also efficiently computable is called a *pairing*, and such mappings are the fundamental primitives from which many cryptographic algorithms are constructed. On the other hand, the Tate pairing also has the following property that limits its usefulness because it returns the value 1 in many cases.

Property 4.2 (Galbraith) [3]

Let $P \in E(\mathbb{F}_q)[n]\backslash\{O\}$ and n relatively prime to q. Then to have $e(P, P) \neq 1$, we must have $k = 1$.

So for an embedding degree $k > 1$ we have $e(P, P) = 1$, which also means that $e(aP, bP) = e(P, P)^{ab} = 1$ for integers a and b, so that the Tate pairing may not seem very useful at first. The following result provides insight into how to overcome this limitation.

Property 4.3 (Verheul) [4]

Let n be a prime, $P \in E(\mathbb{F}_q)[n]\backslash\{O\}$, $Q \in E(\mathbb{F}_{q^k})$ be linearly independent from P, and $k > 1$. Then we have that $e(P, Q)$ is nondegenerate.

So if we have $P \in E(\mathbb{F}_q)[n]$ and a nontrivial embedding degree, that is, we have $k > 1$, then one way to make sure that the Tate pairing $e(P, Q)$ is nondegenerate is to make sure that Q is linearly independent of P. One way to do this is to use a distortion map, so that instead of computing $e(P, Q)$, we compute $e(P, \phi(Q))$ instead, where ϕ is an appropriate distortion map. Another way is to compute $e(P, \phi_d(Q))$ where $Q \in E'$ is on the twist of the elliptic curve E and $\phi_d : E' \to E$ is the mapping defined in Section 3.3.1. In either case, we denote the resulting pairing by $\hat{e}(P, Q)$, where either $\hat{e}(P, Q) = e(P, \phi(Q))$ or $\hat{e}(P, Q) = e(P, \phi_d(Q))$ as appropriate and call such an $\hat{e}$ the *modified Tate pairing*.

Example 4.10

(i) (Distortion Map). From Example 4.1(ii), we have where $E/\mathbb{F}_{11} : y^2 = x^3 + 1$ and $P = (5, 4) \in E(\mathbb{F}_{11})$ [4], we get

$$f_P(x, y) = \frac{(y + 3x + 3)^2}{x + 1}$$

If we have $Q = (5, 7)$ and $R = (9, 9)$, then $Q + R = (0, 1)$ and we evaluate f_P at $A_Q = (Q + R) - (R)$ we get $e(P, Q) = f_P(A_Q) = 2 \in \mathbb{F}_{11}$, so that for the reduced Tate pairing we get

$$e(P, Q)^{(q^k - 1)/n} = 2^{(11^2 - 1)/4} = 2^{30} \equiv 1 \pmod{11}$$

In this case, $\phi(x, y) = (\xi x, y)$, where $\xi = 5 + 3 \cdot i$, is a distortion map for the point Q, and we find that $\phi(Q) = (3 + 4 \cdot i, 7)$ and that $\phi(Q) + R = (1 + 4 \cdot i, 5)$. Thus, we have that

$$
\begin{aligned}
f_P((\phi(Q) + R) - (R)) &= \frac{f_P(\phi(Q) + R)}{f_P(R)} \\
&= \frac{1 + 9i}{8} = 7 + 8i
\end{aligned}
$$

so that for the reduced modified Tate pairing we get

$$
e(P, \phi(Q))^{(q^k - 1)/n} = (7 + 8i)^{(11^2 - 1)/4} = (7 + 8i)^{30} \equiv 10 \pmod{11}
$$

(ii) (Twist). We have that $E' : y^2 = x^3 + 10$ is the quadratic twist of $E/\mathbb{F}_{11} : y^2 = x^3 + 1$ that is created using the quadratic nonresidue $v = 10$. If $P = (5, 4) \in E(\mathbb{F}_{11})$ [4], then from Example 4.1(ii) we get

$$
f_P(x, y) = \frac{(y + 3x + 3)^2}{x + 1}
$$

In this case, we have

$$
\phi_2(x, y) = (v^{-1}x, v^{-3/2}y) = (10 \cdot x, i \cdot y)
$$

If we have $Q = (3, 2) \in E'$ and $R = (9, 9)$, then $\phi_2(Q) = (8, 2i)$ then $\phi_2(Q) + R = (5 + 8i, 8i)$. Thus we have that

$$
\begin{aligned}
f_P((\phi_2(Q) + R) - (R) &= \frac{f_P(\phi_2(Q) + R)}{f_P(R)} \\
&= \frac{4 + 8i}{6 + 8I} = 5i
\end{aligned}
$$

so that for the reduced modified Tate pairing we get

$$
e((P, \phi_2(Q))^{(q^k - 1)/n} = (5i)^{(11^2 - 1)/4} = (5i)^{30} \equiv 10 \pmod{11}
$$

4.3 Miller's Algorithm

The technique that we used above to find a divisor equivalent to $n(P) - n(O)$, in which we iteratively find divisors equivalent to $(P) - (O)$, $2(P) - 2(O)$,

..., up to $n(P) - n(O)$ by a repeated application of (4.3) will certainly work, but it is extremely inefficient. In a typical cryptographic application, n is typically at least 2^{160}, so iterating in this way is impractical. Instead, the way we calculate $n(P) - n(O)$ is by the double-and-add technique, and finding a divisor equivalent to $n(P) - n(O)$ in this way is called *Miller's algorithm* [5]. Miller's algorithm is based on the observation that it is easy to generalize (4.3) to divisors

$$D_1 = (aP) - (O) + div(f_1)$$

and

$$D_2 = (bP) - (O) + div(f_2)$$

to find that

$$D_1 + D_2 = (a+b)P - (O) + div\left(f_1 f_2 \frac{u_{aP,\,bP}}{v_{(a+b)P}}\right)$$

We can formalize Miller's algorithm as follows. Pick an elliptic curve E on which all of the following calculations will be performed. Let $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_{q^k})$ with

$$n = \sum_{i=0}^{t} b_i 2^i \text{s}$$

so that $(b_i, \ldots, b_1, b_0)$ is the binary expansion of n. We start with $f = 1$, $S = P$, and R a random point on E. We then do a double-and-add iteration through the binary expansion of n, performing the doubling step at each iteration and the adding step if the bit we are at is a 1. This will let us build the rational function equivalent to $n(P) - n(O)$ out of the repeatedly doubled terms, and we evaluate each of these terms at $(Q + R) - (R)$ as we calculate them. We do this by the following algorithms.

Algorithm 4.1: TatePairing (Miller's algorithm for computing the Tate pairing)
INPUT: Elliptic curve $E : y^2 = x^3 + ax + b$, $P \in E[n]$ with $n = \sum_{i=0}^{t} b_i 2^i$, Q
OUTPUT: $e(P, Q)$

1. $f \leftarrow 1$, $t \leftarrow \lfloor \log_2 n \rfloor$, $S \leftarrow P$, $R \leftarrow$ a random point of E, $R \neq O$, $Q + R \neq O$

2. For $i \leftarrow t-1$ down to 0
3. $f \leftarrow f^2 \dfrac{u_{S,S}(Q+R)\, v_{2S}(R)}{v_{2S}(Q+R)\, u_{S,S}(R)}$
4. $S \leftarrow 2S$
5. If $b_i = 1$
6. $f \leftarrow f \dfrac{u_{S,P}(Q+R)\, v_{S+P}(R)}{v_{S+P}(Q+R)\, u_{S,P}(R)}$
7. $S \leftarrow S + P$
8. Return f

Algorithm 4.2: v
INPUT: P, Q
OUTPUT: $v_P(Q)$

1. If $P = O$
2. Return 1
3. Return $x_Q - x_P$

Algorithm 4.3: tangent_u
INPUT: P, Q on an elliptic curve $E : y^2 = x^3 + ax + b$
OUTPUT: $u_{P,P}(Q)$

1. If $P = O$
2. Return 1
3. If $y_P = 0$
4. Return $v(P, Q)$
5. $m \leftarrow \dfrac{3x_P^2 + a}{2y_P}$
6. Return $y_Q - y_P - mx_Q + mx_P$

Algorithm 4.4: u
INPUT: P_1, P_2, Q
OUTPUT: $u_{P_1,P_2}(Q)$

1. If $P_1 = O$
2. Return $v(P_2, Q)$
3. If $P_2 = O$ or $P_1 + P_2 = O$
4. Return $v(P_1, Q)$

5. If $P_1 = P_2$
6. Return *tangent_u*(P_1, Q)
7. $m \leftarrow \dfrac{y_{P_2} - y_{P_1}}{x_{P_2} - x_{P_1}}$
8. Return $y_Q - y_{P_1} - mx_Q + mx_{P_1}$

References

[1] Lang, S., *Elliptic Functions*, New York: Springer-Verlag, 1987.

[2] Silverman, J., *The Arithmetic of Elliptic Curves*, New York: Springer-Verlag, 1986.

[3] Galbraith, S., "Supersingular Curves in Cryptography," *Proceedings of Asiacrypt 2001*, Gold Coast, Australia, December 9–13, 2001, pp. 495–513.

[4] Verheul, E., "Evidence That XTR Is More Secure Than Supersingular Elliptic Curve Cryptosystems," *Journal of Cryptology*, Vol. 17, No. 4, 2004, pp. 277–296.

[5] Miller, V., "The Weil Pairing and Its Efficient Calculation," *Journal of Cryptology*, Vol. 17, No. 4, 2004, pp. 235–261.