

# Implementing Cryptographic Pairings over the KSS $k = 18$ curves in magma

Ezekiel J Kachisa, Luis J Domínguez P

Dublin City University

December, 2008

<http://www.computing.dcu.ie/~ldominguez/module6/pairing-tutorial.pdf>



- 1 KSS family of curves
- 2 Curve generation
  - Finding  $p$  and  $r$
- 3 Tate Pairing
  - Miller loop
- 4 Twist of a curve
  - Twists
- 5 ate pairing
  - Definition
- 6 Final Exponentiation
  - Frobenius
  - Hard part
- 7 Conclusion

The parameters of this type of curves is as follows:

- $t(x) = (x^4 + 16x + 7)/7$
- $p(x) = (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21$
- $r(x) = (x^6 + 37x^3 + 343)/343$
- $\rho = 4/3$
- $p(x)$  and  $r(x)$  represents primes and  $t(x)$  represents integers when  $x \equiv 14 \pmod{42}$

There has been much speculation about the exact sizes of  $r$  and  $p^k$  required to match standard sizes of keys for symmetric encryption, using for example the Advanced Encryption Standard (AES). The problem is complicated by the fact that the effectiveness of index calculus attacks is not yet fully understood, especially over extension fields.

Security level (in bits)	Subgroup size $r$ (in bits)	Extension field size $p^k$ (in bits)	Embedding degree $k$	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960–1280	6–8	2*,3–4
112	224	2200–3600	10–16	5–8
128	256	3000–5000	12–20	6–10
<b>192</b>	<b>384</b>	8000–10000	20–26	10–13
256	512	14000–18000	28–36	14–18

Table: Bitsize comparison between levels of security

Levels: SKIPJACK, Triple-DES, AES-Small, AES-Medium, and AES-Large.

5/ 21

Ezekiel J  
Kachisa, Luis  
J Domínguez  
P

KSS family of  
curves

Curve  
generation

Finding  $p$  and  $r$

Tate Pairing  
Miller loop

Twist of a  
curve

Twists

ate pairing  
Definition

Final Expo-  
nentiation

Frobenius  
Hard part

Conclusion

For KSS:  $k = 18$ , the  $D = -3$ , one can use the same approach as in the BN curves.

See code: [FINDPR].

Note:  $r \times c = \text{number of points on the curve}$

For generating the curve, see code: [ECDEF]

One needs to create an elliptic curve over the extension field.  
See code: [EXTECDEF]

7 / 21

Ezekiel J  
Kachisa, Luis  
J Domínguez  
P

KSS family of  
curves

Curve  
generation  
Finding  $p$  and  $r$

Tate Pairing  
Miller loop

Twist of a  
curve  
Twists

ate pairing  
Definition

Final Expo-  
nentiation  
Frobenius  
Hard part

Conclusion

The number of points on an elliptic curve is related to the size of the field as follows  $\#E(\mathbb{F}_p) = p + 1 - t$ , where  $t$  is the trace of the Frobenius of Endomorphism. If  $\alpha$  is a root to the characteristic polynomial  $X^2 - tX + p$ , then the number of points on the curve defined over the extension field is defined as follows,  $\#E(\mathbb{F}_{p^k}) = p^k + 1 - \alpha^k - \bar{\alpha}^k$ .

See code: [NPFPK]

For the Tate pairing to be non degenerate,  $P \in G_1$  and  $Q \in G_2$  must be linearly independent.

### Subgroup $S$ and subgroup $T$

Let  $Tr$  be the Trace map,  $Tr : E(\mathbb{F}_{p^k}) \rightarrow S$ , and  $ATr(P) = P - Tr(P)$  the anti-Trace map,  $ATr : E(\mathbb{F}_{p^k}) \rightarrow T$ . A general point from any other group of order  $r$  can always be written as:  $P = P_s + P_t$ , where  $P_s = Tr(P)/k$  and  $P_t = P - P_s$ , with  $P_s \in S$  and  $P_t \in T$ .

Efficient way is to define  $G_1$  as  $S$  and  $G_2$  as  $T$ . For simplicity, one can multiply  $k \times Q \in G_2$  to avoid costly division in the  $P_s$  computation.

See code [GETQFPK]

Let  $P \in E(\mathbb{F}_p)[r]$  and  $Q \in E(\mathbb{F}_{p^k})$ , consider the divisor  $D = (Q + S) - (S)$  with  $S$  a random point in  $E(\mathbb{F}_{p^k})$ . Let  $f_{a,P}$  be a function with a divisor  $(f_{a,P}) = a(P) - (aP) - (a-1)(\mathcal{O})$  for  $a \in \mathbb{Z}$ . A non degenerate bilinear Tate pairing can be defined as a map:

### Definition

$$e_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \rightarrow \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r$$

$$(P, Q) \mapsto \langle P, Q \rangle_r = f_{r,P}(D)$$

This value of the pairing is in an equivalence class,  $\mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r$ , for practical purposes it is preferred to raise the value of the pairing to the power of  $(p^k - 1)/r$  to obtain a unique representative of the class.

It is necessary to apply the double-and-add, line-and-tangent algorithm until the point  $P$ , on being multiplied by its order  $r$ , finally reaches the  $\mathcal{O}$ . It will arrive there after  $\lg(r - 1)$  iterations of the miller loop.

Implementing the Tate Pairing is almost as easy as implementing the miller loop.

See code [LFUNC] [MILLER]

## Definition

Let  $E$  and  $E'$  be elliptic curves defined over a finite field  $\mathbb{F}_p$ . Then  $E'$  is said to be a twist of degree  $d$  if there exists an isomorphism  $\psi : E \rightarrow E'$  defined over  $\mathbb{F}_{p^d}$  with  $d$  minimal.

## Possible twists

- Quadratic
- Cubic
- Quartic
- Sextic

Since  $k = 18$  curves have  $D = 3$  and is divisible by 6 then *sextic* twists exists.

To utilize the sextic twists:

- Define the point  $Q \in G_2$  over the twist curve  $E'(\mathbb{F}_{p^3})$
- choose  $\chi \in \mathbb{F}_{p^3}$  such that  $W^6 - \chi$  is irreducible over  $\mathbb{F}_{p^3}[W]$
- if  $\delta \in \mathbb{F}_{p^{18}}$  is a root of  $W^6 - \chi$ , then there exists a homomorphism which maps points on the sextic twist to the points of the original curve

$$\psi : E'(F_{p^3}) \rightarrow E(\mathbb{F}_{p^{18}}) \text{ defined by: } (x', y') \rightarrow (x'\delta^{1/3}, y'\delta^{1/2})$$

- with an isomorphism given by  $[\cdot] : \mu_6 \rightarrow \text{Aut}(E) : \delta \mapsto [\delta]$  with  $[\delta](x, y) = (\delta^2 x, \delta^3 y)$

$$E' : y' = x'^3 + \frac{b}{\chi}$$

One way to find  $\chi$  is to set  $1/\chi = \lambda^2\mu^3$  where  $\lambda \in \mathbb{F}_p$  is a noncube and  $\mu \in \mathbb{F}_{p^2}$  is a nonsquare. However, in a practical implementation, one may prefer smaller values of  $\chi$ ...

We can have a linear search from  $\chi = x + 1$  until we find the a twist of the right order. For doing this, we must use a try-and-error technique with  $\chi$  for creating the twist.

We also need to calculate the number of points on the twist of the curve over the extension field.

See code [SEARCHX]

Once the  $\chi$  is selected, one need to create the twist of the elliptic curve, and the elliptic curve over the extension field with this value.

Also, since it is a new curve, one needs to create a new point  $P$  and  $Q$ .

See code [MyX]

The Ate pairing is a variant of Tate pairing and it is a generalisation of the Eta pairing to ordinary pairing-friendly elliptic curves.

To measure if the family of curves is ate-friendly, we use the parameter  $\omega = \frac{\deg r(x)}{\deg m(x)}$ .

In the case of the KSS:  $k=18$  curves,  $m(x) = x^3 + 18$ , and  $\omega \approx 2$ . Giving a family of curves with efficient ate pairing.

This pairing is suitable to pairing-friendly curves with small values of trace of Frobenius.

**Frobenius endomorphism:  $\pi_p$**

$$\pi_p : E \longmapsto E : (x, y) \longmapsto (x^p, y^p).$$

We denote

$$G_1 = E[r] \cap \text{Ker}(\pi_p - [1]), G_2 = E[r] \cap \text{Ker}(\pi_p - [p]).$$

Let  $T = t - 1$ . Let  $N = \gcd(T^k - 1, p^k - 1)$ ,  $T^k - 1 = LN$ .

### The ate pairing

For  $Q \in G_2$  and  $P \in G_1$  Ate pairing is defined as:

$$a_T : (Q, P) \mapsto f_{T,Q}(P)^{c_T(p^k-1)/N}$$

where  $c_T = \sum_{i=0}^{k-1-i} p^i \equiv kp^{k-1} \pmod{r}$ . The ate pairing is a bilinear non-degenerate pairing if  $r \nmid L$ . The first parameter should be defined over the extension field, but will be over  $\mathbb{F}_{p^3}$  for compression.

See code: [ATE]

See the modified L function. We are avoiding the full arithmetic in  $\mathbb{F}_{p^{18}}$ .

One of most expensive operation in pairing computations

- In Tate and Ate one is required to perform an exponentiation by  $(p^k - 1)/r$
- To speed up this operation one can factor  $(p^{18} - 1)/r$  to  $(p^9 - 1)(p^3 + 1)(p^6 - p^3 + 1)/r$
- For  $(p^9 - 1)(p^3 + 1)$  one can use Frobenius and remain with the hard exponent  $(p^6 - p^3 + 1)/r$
- The idea here is to use the Frobenius for  $f^{p^i}$

Modify the final exponentiation on your code for using the frobenius map:

```
Frobenius(f, Field, i);
```

- One way to go around on this is to express  $\lambda = (p^6 - p^3 + 1)/r$  to the base  $p$
- For example  $\lambda = \lambda_0 + \lambda_1 p + \lambda_2 p^2 + \dots + \lambda_{\phi(k)-1} p^{\phi(k)-1}$
- Then we can reduce this expensive exponentiation with some multiplications and squarings of cheaper exponentiations.

See <http://eprint.iacr.org/2008/490>

We have the Tate pairing and a reduction of the miller-loop thanks to the ate pairing (and Eta pairing). However, there is a new pairing, the  $r$ -ate pairing that has an even shorter miller-loop, but a complex implementation.

Miller-length in iterations		
Tate	$e_r(P, Q)$	377
Ate	$e_t(P, Q)$	254
R-ate	$e_{A,B}(P, Q)$	61

Table: Comparison of miller-loop length

for a  $\text{Log}_2(p) \approx 512$

20/ 21

Ezekiel J  
Kachisa, Luis  
J Domínguez  
PKSS family of  
curvesCurve  
generation  
Finding  $p$  and  $r$ Tate Pairing  
Miller loopTwist of a  
curve  
Twistsate pairing  
DefinitionFinal Expo-  
nentiation  
Frobenius  
Hard part

Conclusion

Implement the ate pairing for the BN Curves ( $k = 12$ )...

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

$$t(x) = 6x^2 + 1$$

For a level of security of AES-128.

21 / 21

Ezekiel J  
Kachisa, Luis  
J Domínguez  
P

KSS family of  
curves

Curve  
generation  
Finding  $p$  and  $r$

Tate Pairing  
Miller loop

Twist of a  
curve  
Twists

ate pairing  
Definition

Final Expo-  
nentiation  
Frobenius  
Hard part

Conclusion

## Questions?