OpenCores

www.opencores.org

Tate Bilinear Pairing Core
Specification

Author: Homer Xing

homer.xing@gmail.com

Rev. 0.1

February 2, 2012

This page has been intentionally left blank.

Revision History

Rev.	Date	Author	Description
0.1	01/31/2012 02/02/2012	Homer Xing Homer Xing	First Draft Detailed input data capture time in the section “Input timing pattern”

Contents

1 Introduction

The Tate Bilinear Pairing core is for calculating Tate bilinear pairing especially on super-singular elliptic curve $E: y^2 = x^3 - x + 1$ in affine coordinates defined over a Galois field $GF(3^m), m = 97$, whose irreducible polynomial is $x^{97} + x^{12} + 2$. (For improving security, an irreducible polynomial with higher degree might be used in the future.)

The above elliptic curve contains a large cyclic subgroup of prime order l. Also l divides $3^{6m} - 1$ and not any $3^{j\times m} - 1, j < 6$, and l^2 does not divide $\#E$. Now $E\big(GF(3^m)\big)$ contains an l-torsion group $E[l]\big(GF(3^m)\big)$ and $E\big(GF(3^{6m})\big)$ also contains an l-torsion group $E[l]\big(GF(3^{6m})\big)$. The Tate bilinear pairing (of order l) is a bilinear map between $E[l]\big(GF(3^m)\big)$ and $E[l]\big(GF(3^{6m})\big)$ to an element of the multiplicative group $GF(3^{6m})^*$, i.e.

$$e_l: E[l]\big(GF(3^m)\big) \times E[l]\big(GF(3^{6m})\big) \to GF(3^{6m})^* \qquad (1)$$

It is necessary to raise the value on the right hand side to the power $\epsilon = (3^{6m} - 1) / l$ to obtain a unique value in $GF(3^{6m})$. Consider $P = (x_1, y_1), Q = (x_2, y_2) \in E[l]\big(GF(3^m)\big)$ i.e. $x_1, y_1, x_2, y_2 \in GF(3^m)$ and define a distortion map ϕ as

$$\phi(Q) = \phi(x_2, y_2) = (\rho - x_2, \sigma y_2) \qquad (2)$$

, where $\rho, \sigma \in GF(3^{6m})$ satisfying $\rho^3 - \rho - 1 = 0$ and $\sigma^2 + 1 = 0$. Then the Tate pairing is defined on points $P, Q \in E[l]\big(GF(3^m)\big)$ as

$$\hat{e}(P, Q) = e_l\big(P, \phi(Q)\big)^{\epsilon} = \tau \in GF(3^{6m})^* \qquad (3)$$

Generally speaking, the Tate pairing is a transformation that takes in two elements in the elliptic curve point group and outputs a nonzero element in the extension field $GF(3^{6m})$.

The Tate pairing performs in two stages:

Stage 1: calculation of $\phi(Q) \in E[l]\big(GF(3^{6m})\big)$ in the rational function f_P on $E\big(GF(3^m)\big)$ such that $div(f_P) \sim l[P] - l[O]$, i.e. $e_l\big(P, \phi(Q)\big) = f_P\big(\phi(Q)\big) = t \in GF(3^{6m})^*$. This is by Algorithm 1 (Modified Duursma-Lee algorithm) below.

Stage 2: raising t to the power $\epsilon_1 = \epsilon / 3^{3m} = 3^{3\mathrm{m}} - 1$

Algorithm 1 (Modified Duursma-Lee algorithm)

Input: $P = (x_1, y_1), Q = (x_2, y_2) \in E[l]\big(GF(3^m)\big)$

Output: $t = e_l\big(P, \phi(Q)\big) \in GF(3^{6m})^*$

1: $t = 1 \in GF(3^{6m})^*, \alpha = x_1, \beta = y_1, x = x_2^3, y = y_2^3, \mu = 0 \in GF(3^m), d = m \ mod \ 3$

2: for i from 0 to $m - 1$ do

3: $\alpha = \alpha^9, \beta = \beta^9, \mu = \alpha + x + d$

4: $\gamma = -\mu^2 - \beta y\sigma - \mu\rho - \rho^2, t = t^3\gamma, y = -y, d = d - 1 \ mod \ 3$

5: next i

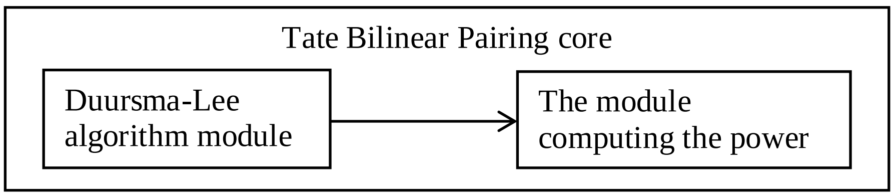
6: return t

For more information about the Tate pairing please refer to [1], [2].

2

Architecture

The Tate Bilinear Pairing core consists of two fundamental modules, where the first module running Duursma-Lee algorithm, and the second module calculating the power.



3

Interface

The Tate Bilinear Pairing core implements the signals shown in the table below.

Input signals are synchronous and sampled at the rising edge of the clock.

Output signals are driven by flip-flops, and not directly connected to input signals by combinational logic.

For signals wider than 1 bit, the range is most significant bit down to least significant bit.

Table 1: Interface signals

Signal name	Width	In/Out	Description
clk	1	In	clock
reset	1	In	*active high synchronous* reset
x1	194	In	one of input data
y1	194	In	one of input data
x2	194	In	one of input data
y2	194	In	one of input data
done	1	Out	The termination signal. It is inactive low after the *reset* signal asserted, and is active high only if the Tate pairing computation is done.
out	1164	Out	Output data. Its value is valid when the *done* signal is asserted.

4

Timing diagrams

Input timing pattern

When the *reset* signal is asserted, valid input data should be on the input signals and keep valid until the computation termination. The input data is captured at the moment when the rising edge of the *clk* signal meets the high value of the *reset* signal as shown by the blue arrow in Figure 1.

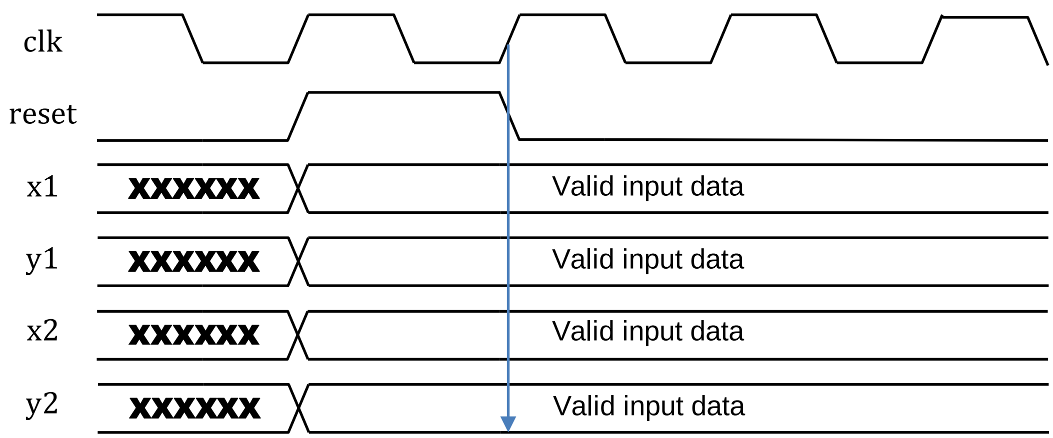


Figure 1: Input timing pattern

Output timing pattern

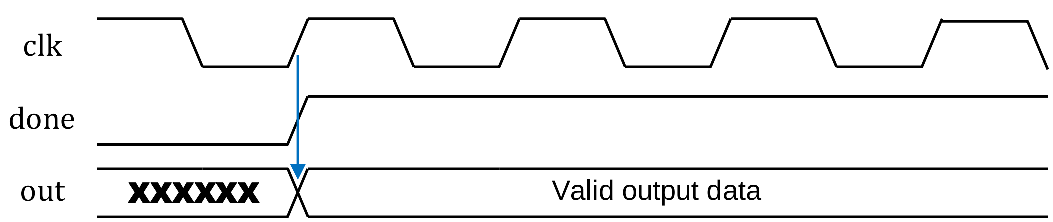


Figure 2: Output timing pattern

5

FPGA Implementation

The core has only been verified on a Xilinx Virtex 4 XC4VLX200 FPGA. For this setup related configuration files is in the directory synthesis/xilinx.

The code is vendor independent in Verilog 2001.

Synthesis results on Xilinx Virtex 4 XC4VLX200-11FF1513, synthesized with Xilinx ISE 13.3:

- Number of occupied slices: 30,149
- Number of 4 input LUTs: 47,083
- Number of flip-flops: 31,383
- Minimal period: 7.632 ns
- Max achievable frequency: 131 MHz

The number of clock cycles for one Tate pairing is 75,839. It means the core computes one Tate pairing in 0.76 milliseconds if with a 100MHz clock.

6

Test bench

Some self-checking test benches are provided in the testbench directory. The test benches include test vectors and expected results. The object being tested of each file is listed in the table below.

Table 2: the object being tested by each test bench

File name	the object being tested
test_f3_*.v	arithmetic modules in $GF(3)$, i.e. addition, negation, multiplication
test_f3m_*.v	arithmetic modules in $GF(3^m)$, i.e. cubic, multiplication, inversion
test_f32m_*.v	multiplication module in $GF(3^{2m})$
test_f33m_*.v	multiplication and inversion module in $GF(3^{3m})$
test_f36m*.v	multiplication and cubic module in $GF(3^{6m})$
test_duursma_lee_algo.v	module running Modified Duursma Lee algorithm
test_second_part.v	module raising t to the power ϵ_1
test_tate_pairing.v	the outermost core

7

References

[1] I. Duursma, H.S. Lee. Tate pairing implementation for hyper-elliptic curves $y^2 = x^p - x + d$.

[2] T. Kerins, W. P. Marnane, E. M. Popovici, and P.S.L.M. Barreto. Efficient hardware for the Tate pairing calculation in characteristic three.