Bit-Parallel Word-Serial Multiplier in GF(2^{233}) and Its VLSI Implementation

Supervisors: Dr. Huapeng Wu
Dr. M. Ahmadi

Student: Wenkai Tang
Contents

• Introduction to Finite Field
• Research Motivations
• Proposed Multipliers
• VLSI Design
• Conclusions
• References
Introduction to Finite Field

• Finite field
  - A set of finite number of elements where addition and multiplication are defined, denoted as GF

Example 1: \( GF(2) = \{0, 1, "+", "*"\} \)

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Example 2: \( GF(2^2) \) can be generated by \( F(x) = x^2 + x + 1 \) where \( \{1, x\} \) is called a polynomial basis

Four elements are:

\[
\begin{align*}
0 &= (00) \\
1 &= (01) \\
x &= (10) \\
x + 1 &= (11)
\end{align*}
\]
Finite Field Multiplication

Let \( A = (a_{m-1}, a_{m-2}, \ldots, a_0) = \sum_{i=0}^{m-1} a_i x^i \) and \( B = (b_{m-1}, b_{m-2}, \ldots, b_0) = \sum_{i=0}^{m-1} b_i x^i \) be any two field elements in GF\((2^m)\), where \( a_i, b_i \in \{0,1\} \)

Then the product
\[
C = (c_{m-1}, c_{m-2}, \ldots, c_0) = AB = \sum_{i=0}^{m-1} a_i x^i \sum_{j=0}^{m-1} b_j x^j \mod F(x)
\]

This is what we want to implement

Example: GF\((2^2)\) is generated by \( F(x)=x^2+x+1 \)

Let \( A = (11) = x + 1 \)

\( B = (10) = x \)

Then
\[
C = AB = (x+1)x \mod F(x)
= (x^2 + x) \mod F(x)
= (x^2 + x + 1) + 1 \mod F(x)
= 1
= (01)\]
Finite field multipliers $C = AB$

**Bit-parallel finite field multiplier**

AND gates: $m^2$
XOR gates: $m^2 - 1$

**Bit-serial finite field multiplier**

AND gates: $m$
XOR gates: $m + 1$
m-bit registers: 2

One multiplication needs $m$ clock cycles

$A, B, C \in \text{GF}(2^5)$
Bit-parallel squarer $C = A^2$

- Architecture

Bit-parallel squarer in $\text{GF}(2^5)$

- Gate counts: 3 XOR gates
Research Motivations

• Smart card and applications
  – Usually a plastic card that contains a security processor and has many security related applications
    • E-Commerce
    • Personal finance
    • Health care
    • Campus badges and access
    • Telecommuting and corporate network security
    • GSM cell phones
  – Limitations
    • Low frequency, limit memory size
    • Software implementation of security application is slow and insecure
    • Area constraint
Smart card and public key cryptosystem

• Public key cryptosystem
  – key exchange, digital signature and encryption/decryption

• Elliptic Curve (EC) over RSA
  – Shorter key length than RSA with the same security strength
  – Very suitable for VLSI implementation
  – EC is more suitable for smart card

• EC operations
  – Finite field multiplication
  – Finite field squaring
  – Finite field addition

• We will design a finite field multiplier for smart card
Proposed Multipliers

• Choose a finite field

<table>
<thead>
<tr>
<th>Degree</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>163</td>
<td>$F(x) = x^{163} + x^7 + x^6 + x^3 + 1$</td>
</tr>
<tr>
<td>233</td>
<td>$F(x) = x^{233} + x^{74} + 1$</td>
</tr>
<tr>
<td>283</td>
<td>$F(x) = x^{283} + x^{12} + x^7 + x^5 + 1$</td>
</tr>
<tr>
<td>409</td>
<td>$F(x) = x^{409} + x^{87} + 1$</td>
</tr>
<tr>
<td>571</td>
<td>$F(x) = x^{571} + x^{10} + x^5 + x^2 + 1$</td>
</tr>
</tbody>
</table>

Finite fields recommended by NIST for elliptic curve systems
Bit-Parallel Word-Serial (BPWS) Multiplier

Let \( \{1, x, x^2, \ldots, x^{2^{32}}\} \) be the polynomial basis for \( \text{GF}(2^{233}) \).

Let \( A \) and \( B \) be any two field elements and

\[
A = \sum_{i=0}^{2^{32}} a_i x^i, \quad \text{where} \quad a_i \in \text{GF} \quad (2)
\]

\[
B = \sum_{i=0}^{2^{32}} b_i x^i, \quad \text{where} \quad b_i \in \text{GF} \quad (2)
\]

The product is

\[
C = A B \mod F(x)
\]

\[
= \sum_{i=0}^{2^{32}} a_i x^i B \mod F(x)
\]
Bit-Parallel Word-Serial (BPWS) Multiplier (Cont’d)

Algorithm:

\[ A = \left( \begin{array}{c}
0000000 \\
A_{29}
\end{array} \right) \begin{array}{c}
a_{232} \\
A_{28}
\end{array} \ldots \begin{array}{c}
a_{231} \\
A_{23}
\end{array} \ldots \begin{array}{c}
a_{224} \\
A_{16}
\end{array} \ldots \begin{array}{c}
a_{7} \\
A_{0}
\end{array} \right) \]

Let \[ A_j = a_{8j+7}x^7 + a_{8j+6}x^6 + \ldots + a_{8j} , \quad \text{for} \quad j = 0,1,\ldots,29 \]

Then \[ A = \sum_{i=0}^{232} a_i x^i = ( (A_{29}x^8 + A_{28})x^8 + \ldots + A_1)x^8 + A_0 \]

\[ C = AB \mod F(x) = ( (A_{29}Bx^8 + A_{28}B)x^8 + A_{27}B)x^8 + \ldots + A_1B)x^8 + A_0B \mod F(x) \]

Let \[ D_j = A_{29-j}B , \quad \text{for} \quad j = 0,1,\ldots,29 \]

\[ C_j = C_{j-1}x^8 + D_j , \quad \text{for} \quad j = 0,1,\ldots,29, \quad \text{and} \quad C_{-1} = 0 \]

Then \[ C = C_{29} \]
Generating the Product

\[ D_j = A_{29-j} B \text{, for } j = 0,1,\ldots, 29 \]

\[ C_j = C_{j-1}x^8 + D_j \text{, for } j = 0,1,\ldots, 29 \text{, and } C_{-1} = 0 \]

<table>
<thead>
<tr>
<th>Clock cycle</th>
<th>Output of M1</th>
<th>Output of M4</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>D_0</td>
<td>0</td>
<td>C_0=D_0</td>
</tr>
<tr>
<td>1</td>
<td>D_1</td>
<td>C_0x^8</td>
<td>C_1</td>
</tr>
<tr>
<td>2</td>
<td>D_2</td>
<td>C_1x^8</td>
<td>C_2</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>28</td>
<td>D_{28}</td>
<td>C_{27}x^8</td>
<td>C_{28}</td>
</tr>
<tr>
<td>29</td>
<td>D_{29}</td>
<td>C_{28}x^8</td>
<td>C_{29}=C</td>
</tr>
</tbody>
</table>

M1: 8 x 233 Partial product generator
M2: 233-bit Adder
M3: Constant multiplier
M4: 233-bit Register
M3: Constant multiplier $\gamma=x^8\alpha$

- Logic equation

$$\gamma_i = \begin{cases} 
\alpha_{225} + i & i = 0, 1, \ldots, 7 \\
\alpha_{i-8} & i = 8, 9, \ldots, 73 \\
\alpha_{i-8} + \alpha_{151} + i & i = 74, 75, \ldots, 81 \\
\alpha_{i-8} & i = 82, 83, \ldots, 232 
\end{cases}$$

- Circuit

- Gate count
  - 8 XOR gates
M1: 8 x 233 Partial product generator $A_j B$

- **Function**

$$A_j B = (a_0 + a_1 x + ... + a_7 x^7)B$$
$$= a_0 B + a_1 x B + ... + a_7 x^7 B$$

- **Components**
  - Seven constant multipliers
  - Eight AND networks
  - A XOR network
M1: $8 \times 233$ Partial product generator (Cont’d)

Architecture

[Diagram showing the architecture of the partial product generator with AND and XOR networks]
M1: 8 x 233 Partial product generator (Cont’d)

• Constant multipliers $x^j \alpha$, $j=1,2,…,7$.
  – Similar architecture as $M3 (x^8 \alpha)$
M1: 8 x 233 Partial product generator (Cont’d)

- AND network
M1: 8 x 233 Partial product generator (Cont’d)

- XOR network
  - 7 XOR sub networks

M: Sub XOR network
Alternative BPWS finite field multiplier

- Least significant word (LSW) first architecture
- One additional m-bit register needed
- One multiplication still needs 30 clock cycles
General BPWS finite field multiplier

Finite field: $GF(2^m)$
Word size: $p$

Components:
- One $p \times m$ partial product generator
- One adder ($m$ XOR gates)
- One constant FFM
- One $m$-bit register
## Comparisons

<table>
<thead>
<tr>
<th>Multiplier</th>
<th>Finite field</th>
<th>Speed (Clock cycle)</th>
<th>Circuit complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallel</td>
<td>GF($2^{233}$)</td>
<td>1</td>
<td>$233^2$ AND gates, $233^2-1$ XOR gates</td>
</tr>
<tr>
<td>Serial</td>
<td></td>
<td>233</td>
<td>two 233-bit registers, 233 AND gates, 234 XOR gates</td>
</tr>
<tr>
<td>Proposed BPWS</td>
<td></td>
<td>30</td>
<td>8<em>233 AND gates, 8</em>233+36 XOR gates, one 233-bit register</td>
</tr>
<tr>
<td>Alternative BPWS</td>
<td></td>
<td>30</td>
<td>8<em>233 AND gates, 8</em>233+36 XOR gates, Two 233-bit registers</td>
</tr>
<tr>
<td>General BPWS Trinomial (1&lt;k&lt;m/2 p word width)</td>
<td>GF($2^m$)</td>
<td>Ceiling function of ($m/p$)</td>
<td>$p<em>m$ AND gates, $p</em>m+(p+1)p/2$ XOR gates, One m-bit register</td>
</tr>
</tbody>
</table>
VLSI Design

• Target
  – ASIC chip which can perform multiplication and squaring in GF($2^{233}$)

• Specifications
  – Frequency: 50MHz
  – Gate counts: 14000

• Design flow
  – CMC digital design flow

• Technology
  – TSMC 0.18 μm CMOS technology
Hardware schematic
## Final results and comparisons

<table>
<thead>
<tr>
<th>Multiplier</th>
<th>Frequency (MHz)</th>
<th>Field size</th>
<th># of cells</th>
<th>Gate counts</th>
<th>Area (µm²)</th>
<th>VLSI technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPWS 8x233</td>
<td>50 (max. 130)</td>
<td>$2^{233}$</td>
<td>3029</td>
<td>4893</td>
<td>189297.06439</td>
<td>TSMC 0.18µm CMOS</td>
</tr>
<tr>
<td>Squarer</td>
<td></td>
<td>293</td>
<td>293</td>
<td></td>
<td>6437.15746</td>
<td></td>
</tr>
<tr>
<td>Classical 233x233 [1]</td>
<td>77</td>
<td>$2^{233}$</td>
<td>37296 LUTs</td>
<td>528427</td>
<td>N/A</td>
<td>Xilinx FPGA XC2V6000-ff1517-4</td>
</tr>
<tr>
<td>Hans et al MSD 64x256 [2]</td>
<td>66.4</td>
<td>$\leq 2^{256}$</td>
<td>14797 LUTs</td>
<td>136064</td>
<td>N/A</td>
<td>Xilinx FPGA Virtex-II XCV2000E-7</td>
</tr>
<tr>
<td>Souichi et al 8x288 [3]</td>
<td>3</td>
<td>$\leq 2^{576}$</td>
<td>2<em>8</em>288 ANDs</td>
<td>14544</td>
<td>N/A</td>
<td>ALTERA FPGA EPF10K250AG C5992</td>
</tr>
</tbody>
</table>
Chip Layout
Conclusions

• Bit-parallel word-serial multiplier architectures are proposed.
• The proposed architectures are not only useful for smart card but also beneficial to other security processors.
• An ASIC chip which has the proposed BPWS multiplier and bit parallel squarer is implemented.
• A novel $8 \times 233$ partial product generator is designed.
• Future work expected is to use this multiplier in security processor for smart card.
References


Question ?
THANK YOU!