

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

*	0	1
0	0	0
1	0	1

Multiplication

+	0	1
0	0	1
1	1	0

Addition

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:

0	=	(00)
1	=	(01)
x	=	(10)
x + 1	=	(11)

Finite Field Multiplication

Let $A = (a_{m-1}, a_{m-2}, \dots, a_0) = \sum_{i=0}^{m-1} a_i x^i$ and $B = (b_{m-1}, b_{m-2}, \dots, b_0) = \sum_{i=0}^{m-1} b_i x^i$

be any two field elements in $\text{GF}(2^m)$, where $a_i, b_i \in \{0,1\}$

Then the product $C = (c_{m-1}, c_{m-2}, \dots, c_0) = AB = \sum_{i=0}^{m-1} a_i x^i \sum_{j=0}^{m-1} b_j x^j \pmod{F(x)}$

This is what we want to implement

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

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

$B = (10) = x$

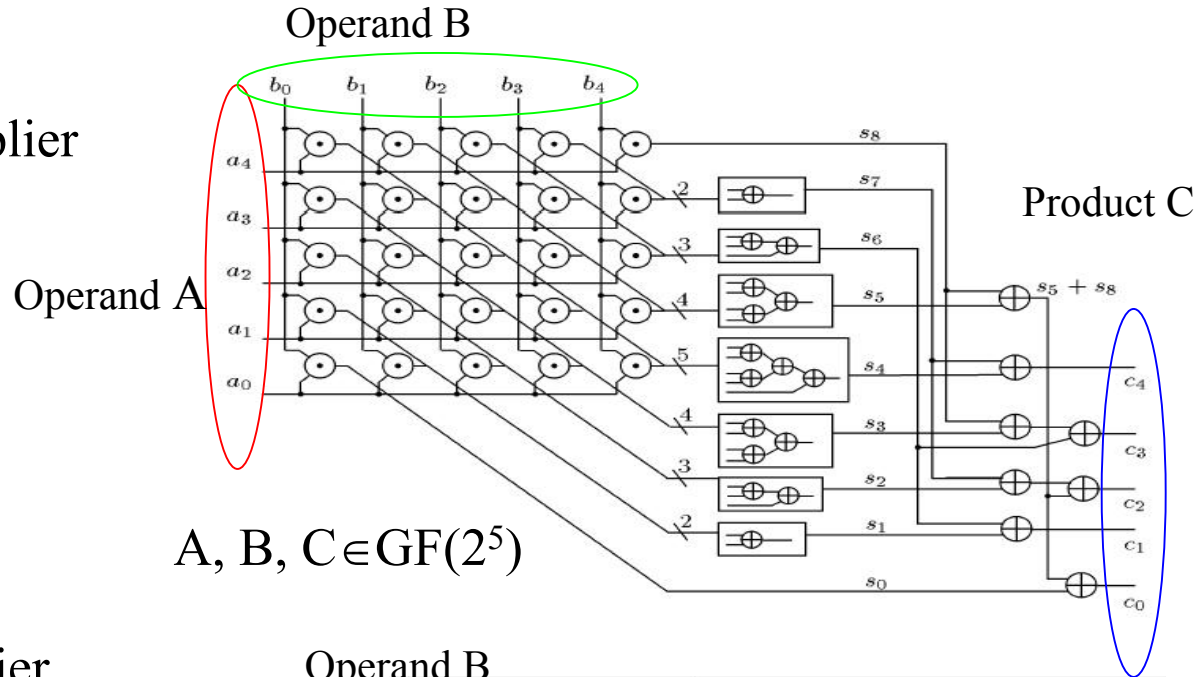
Then

$$\begin{aligned} C &= AB = (x+1)x \pmod{F(x)} \\ &= (x^2 + x) \pmod{F(x)} \\ &= (x^2 + x + 1) + 1 \pmod{F(x)} \\ &= 1 \\ &= (01) \end{aligned}$$

Finite field multipliers $C=AB$

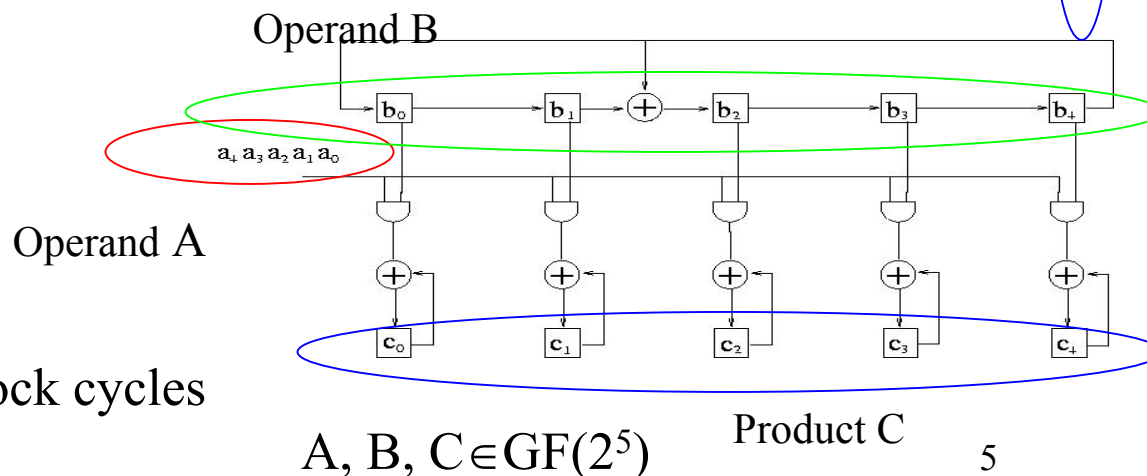
Bit-parallel finite field multiplier

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



Bit-serial finite field multiplier

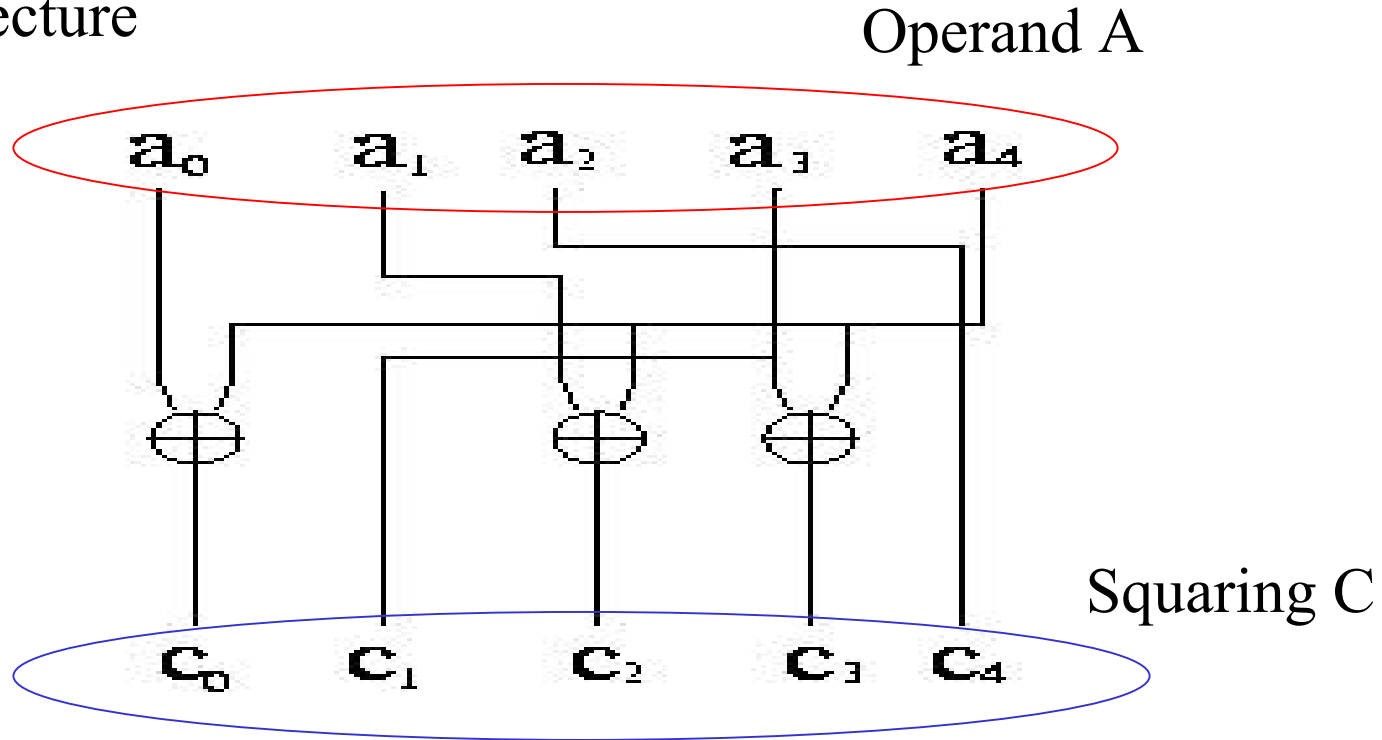
AND gates: m
 XOR gates: $m+1$
 m-bit registers: 2



One multiplication needs m clock cycles

Bit-parallel squarer $C=A^2$

- Architecture



Bit-parallel squarer in $GF(2^5)$

- 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

Degree	Polynomial
163	$F(x) = x^{163} + x^7 + x^6 + x^3 + 1$
233	$F(x) = x^{233} + x^{74} + 1$
283	$F(x) = x^{283} + x^{12} + x^7 + x^5 + 1$
409	$F(x) = x^{409} + x^{87} + 1$
571	$F(x) = x^{571} + x^{10} + x^5 + x^2 + 1$

Finite fields recommended by NIST for elliptic curve systems

Bit-Parallel Word-Serial (BPWS) Multiplier

Let $\{1, x, x^2, \dots, x^{232}\}$ be the polynomial basis for $GF(2^{233})$.

Let A and B be any two field elements and

$$A = \sum_{i=0}^{232} a_i x^i, \quad \text{where} \quad a_i \in GF(2) \quad (2)$$

$$B = \sum_{i=0}^{232} b_i x^i, \quad \text{where} \quad b_i \in GF(2) \quad (2)$$

The product is

$$\begin{aligned} C &= AB \bmod F(x) \\ &= \sum_{i=0}^{232} a_i x^i B \bmod F(x) \end{aligned}$$

Bit-Parallel Word-Serial (BPWS) Multiplier (Cont'd)

Algorithm:

$$A = (\underbrace{00000000}_{A_{29}} \underbrace{a_{232} a_{231} \dots a_{224}}_{A_{28}} \dots \underbrace{a_7 a_6 \dots a_0}_{A_0})$$

Let $A_j = a_{8j+7}x^7 + a_{8j+6}x^6 + \dots + a_{8j}$, for $j = 0, 1, \dots, 29$

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

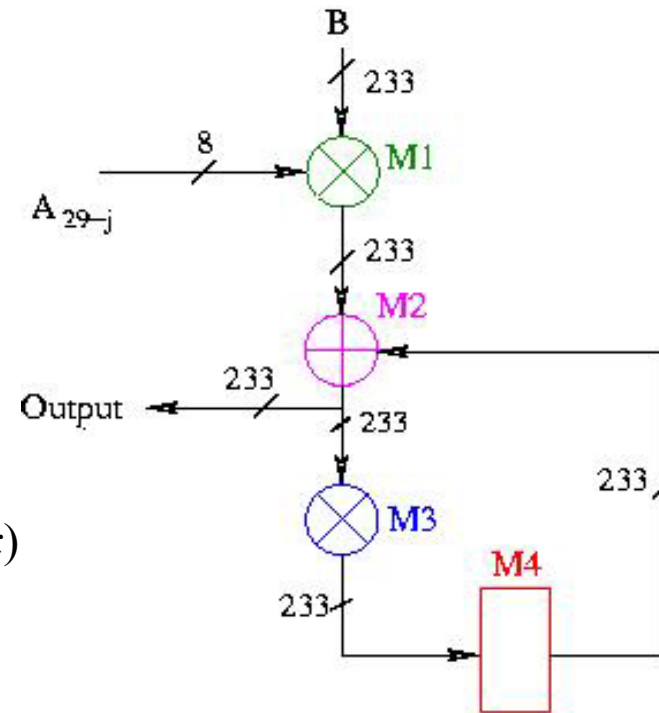
$$\begin{aligned} C &= AB \bmod F(x) \\ &= (\dots ((A_{29}Bx^8 + A_{28}B)x^8 + A_{27}B)x^8 + \dots + A_1B)x^8 + A_0B \bmod F(x) \end{aligned}$$

Let $D_j = A_{29-j}B$, for $j = 0, 1, \dots, 29$

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

Then $C = C_{29}$

Architecture:



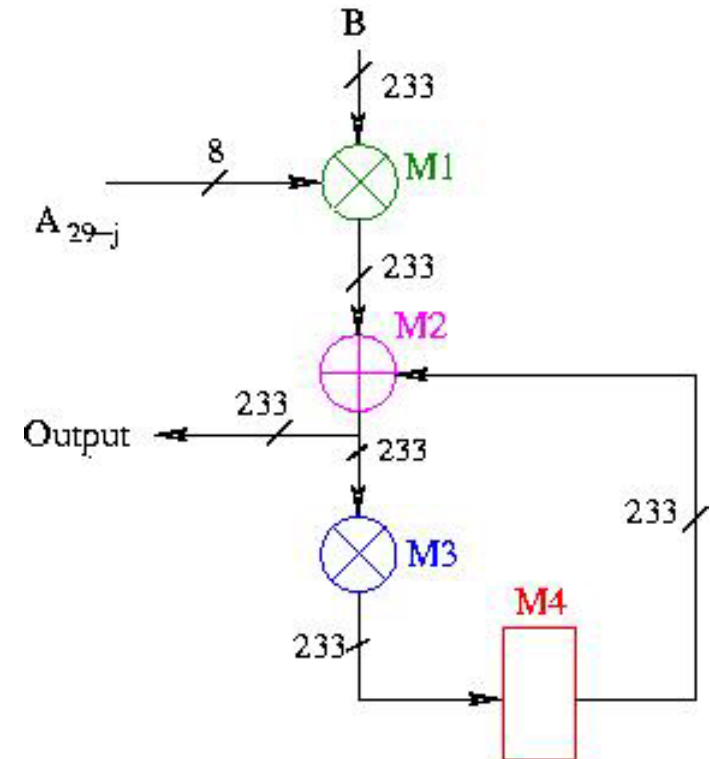
- M1: 8 x 233 Partial product generator
- M2: 233-bit Adder
- M3: Constant multiplier
- M4: 233-bit Register

Generating the Product

$$D_j = A_{29-j}B, \quad \text{for } j = 0, 1, \dots, 29$$

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

Clock cycle	Output of M1	Output of M4	Output
0	D_0	0	$C_0 = D_0$
1	D_1	C_0x^8	C_1
2	D_2	C_1x^8	C_2
...
28	D_{28}	$C_{27}x^8$	C_{28}
29	D_{29}	$C_{28}x^8$	$C_{29} = C$



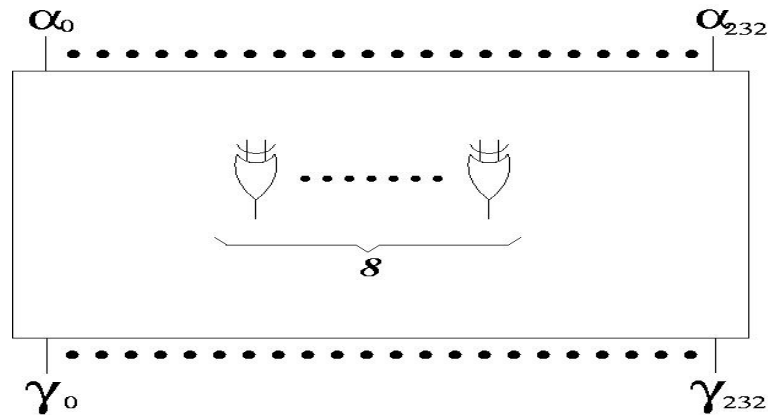
- M1: 8 x 233 Partial product generator
- M2: 233-bit Adder
- M3: Constant multiplier
- M4: 233-bit Register

M3: Constant multiplier $\gamma = x^8 \alpha$

- Logic equation

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

- Circuit



- Gate count

- 8 XOR gates

M1: 8 x 233 Partial product generator $A_j B$

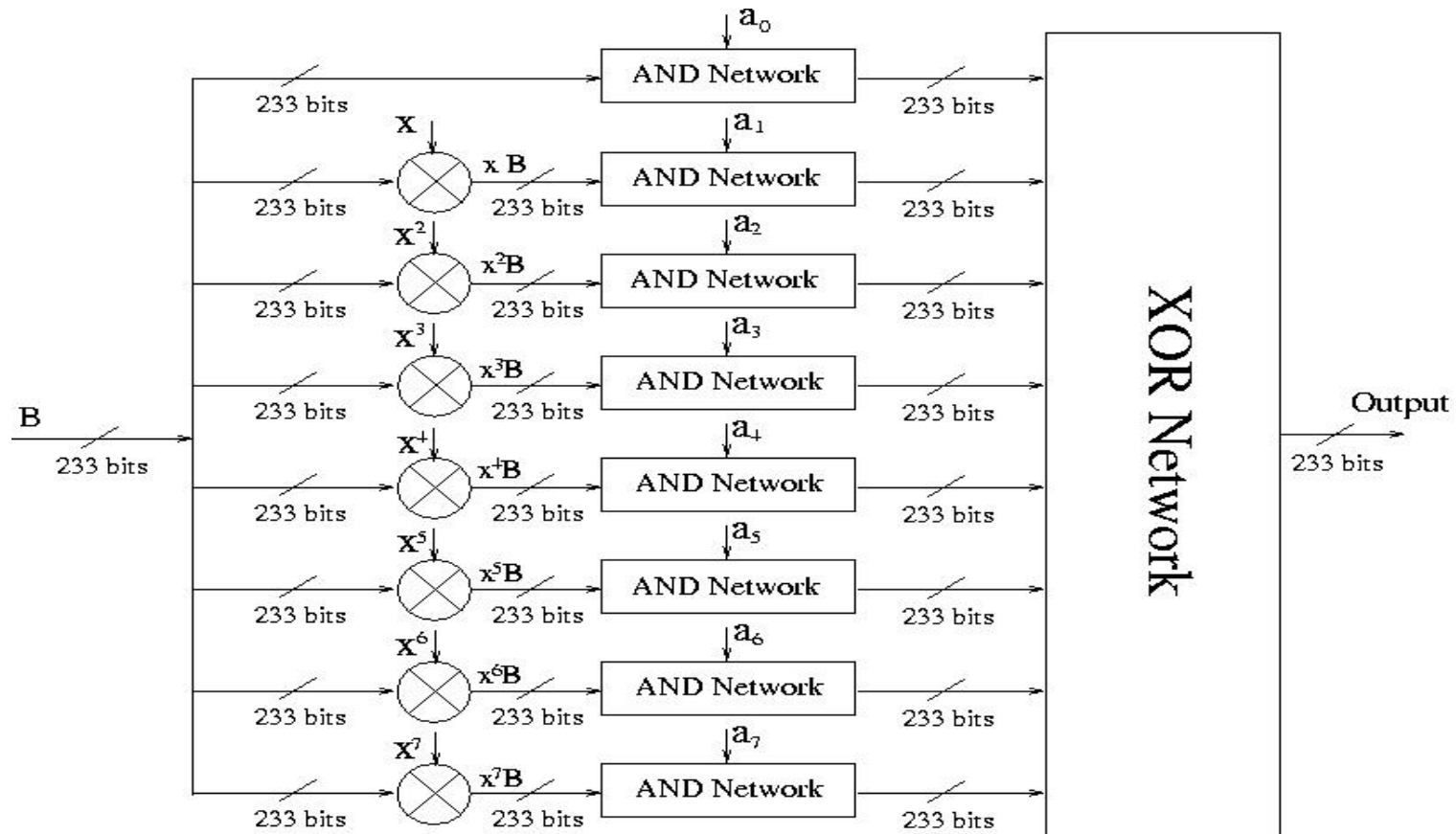
- Function

$$\begin{aligned} A_j B &= (a_0 + a_1 x + \dots + a_7 x^7) B \\ &= a_0 B + a_1 x B + \dots + a_7 x^7 B \end{aligned}$$

- Components
 - Seven constant multipliers
 - Eight AND networks
 - A XOR network

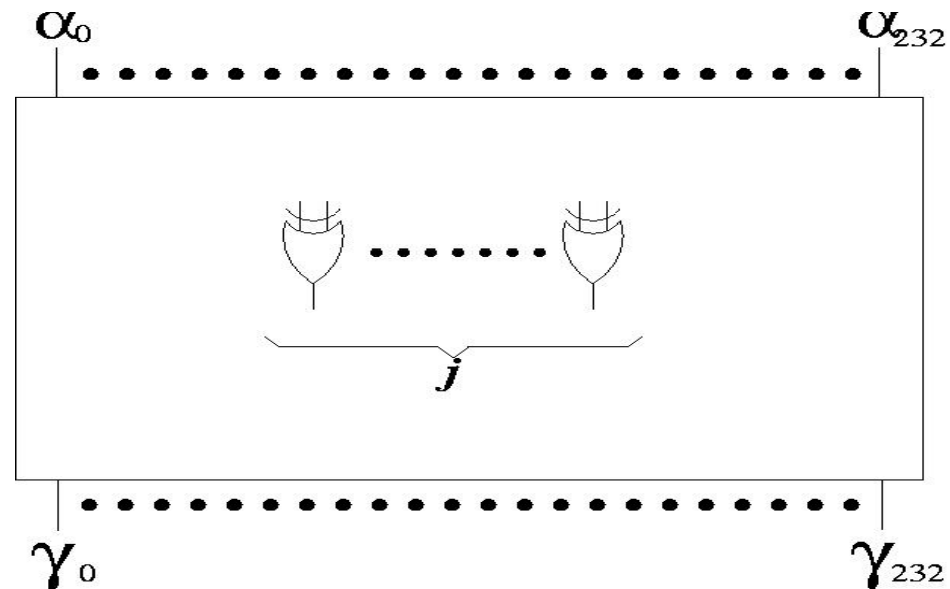
M1: 8 x 233 Partial product generator (Cont'd)

Architecture



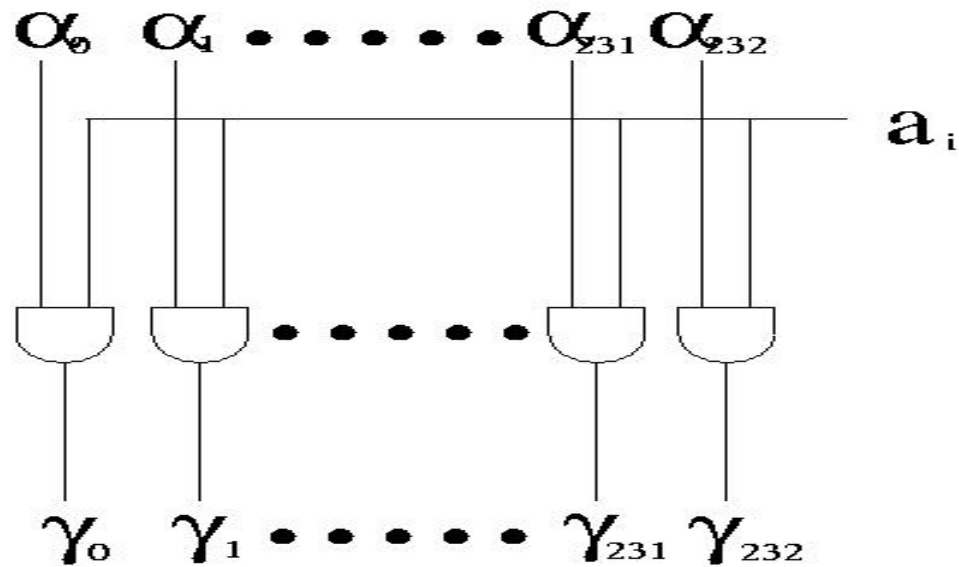
M1: 8 x 233 Partial product generator (Cont'd)

- Constant multipliers $x^j\alpha$, $j=1,2,\dots,7$.
 - Similar architecture as M3 ($x^8\alpha$)



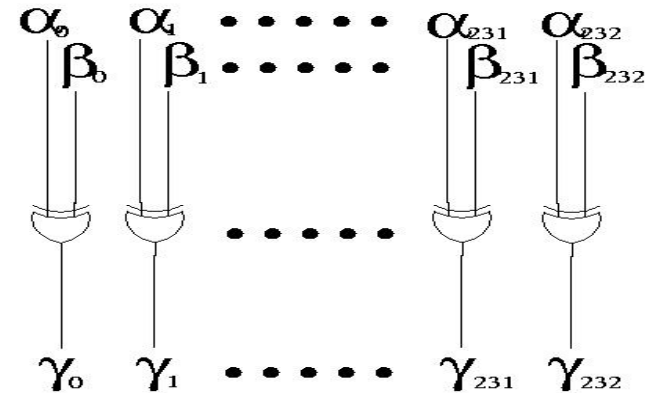
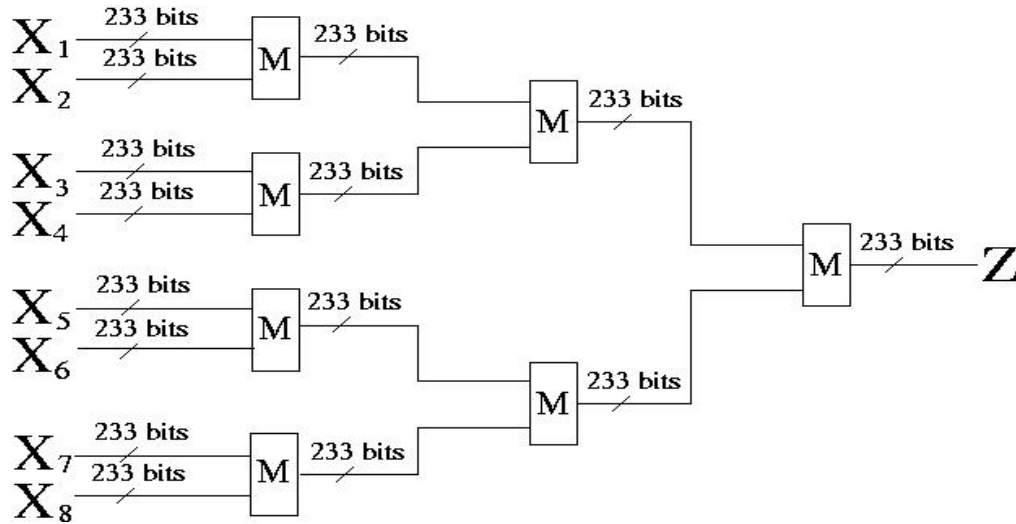
M1: 8 x 233 Partial product generator (Cont'd)

- AND network



M1: 8 x 233 Partial product generator (Cont'd)

- XOR network
 - 7 XOR sub networks

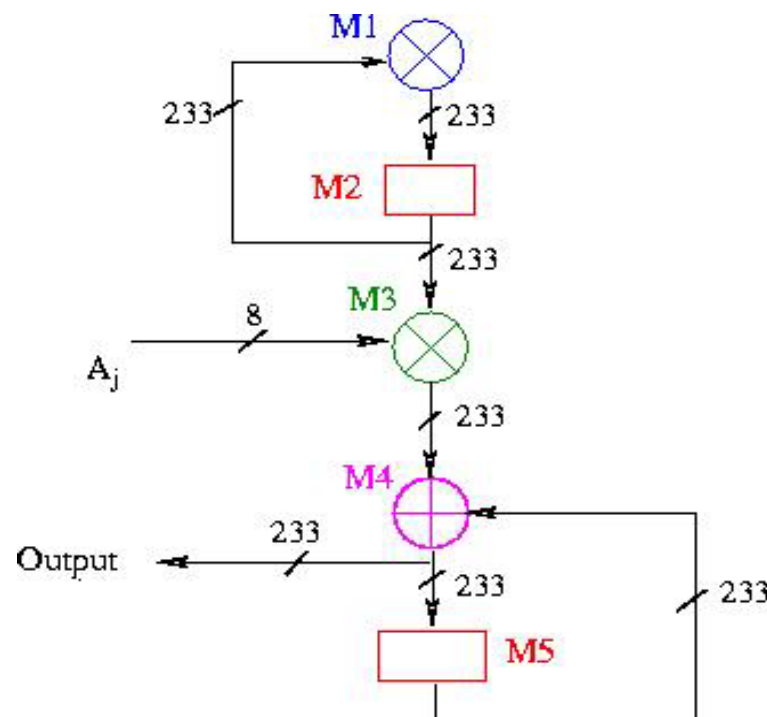


M: Sub XOR network

Alternative BPWS finite field multiplier

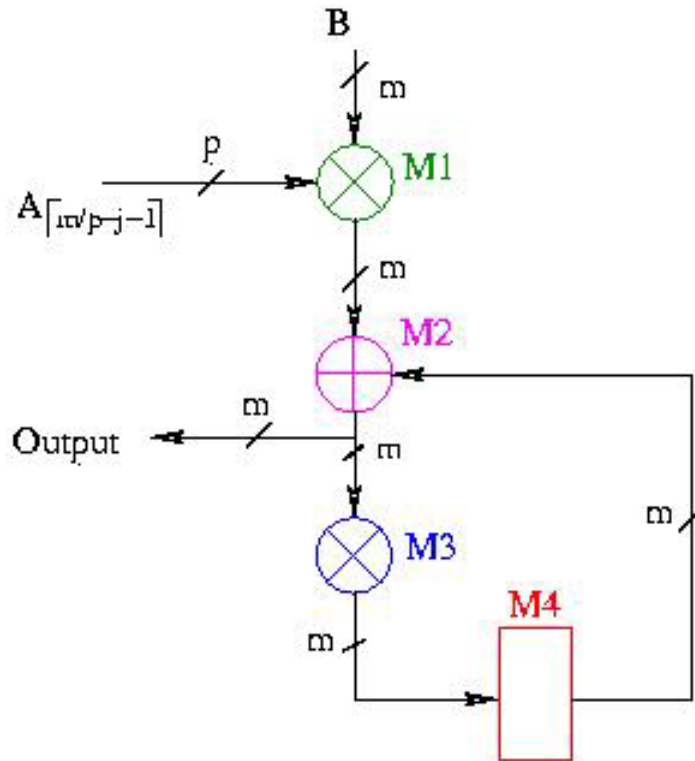
- Least significant word (LSW) first architecture
- One additional m-bit register needed
- One multiplication still needs 30 clock cycles

Architecture:



- M1: Constant multiplier
- M2: 233-bit Register
- M3: 8 x 233 Partial product generator
- M4: 233-bit Adder
- M5: 233-bit Register

General BPWS finite field multiplier



M1: $p \times m$ Partial product generator
M2: m -bit Adder
M3: Constant multiplier
M4: m -bit Register

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

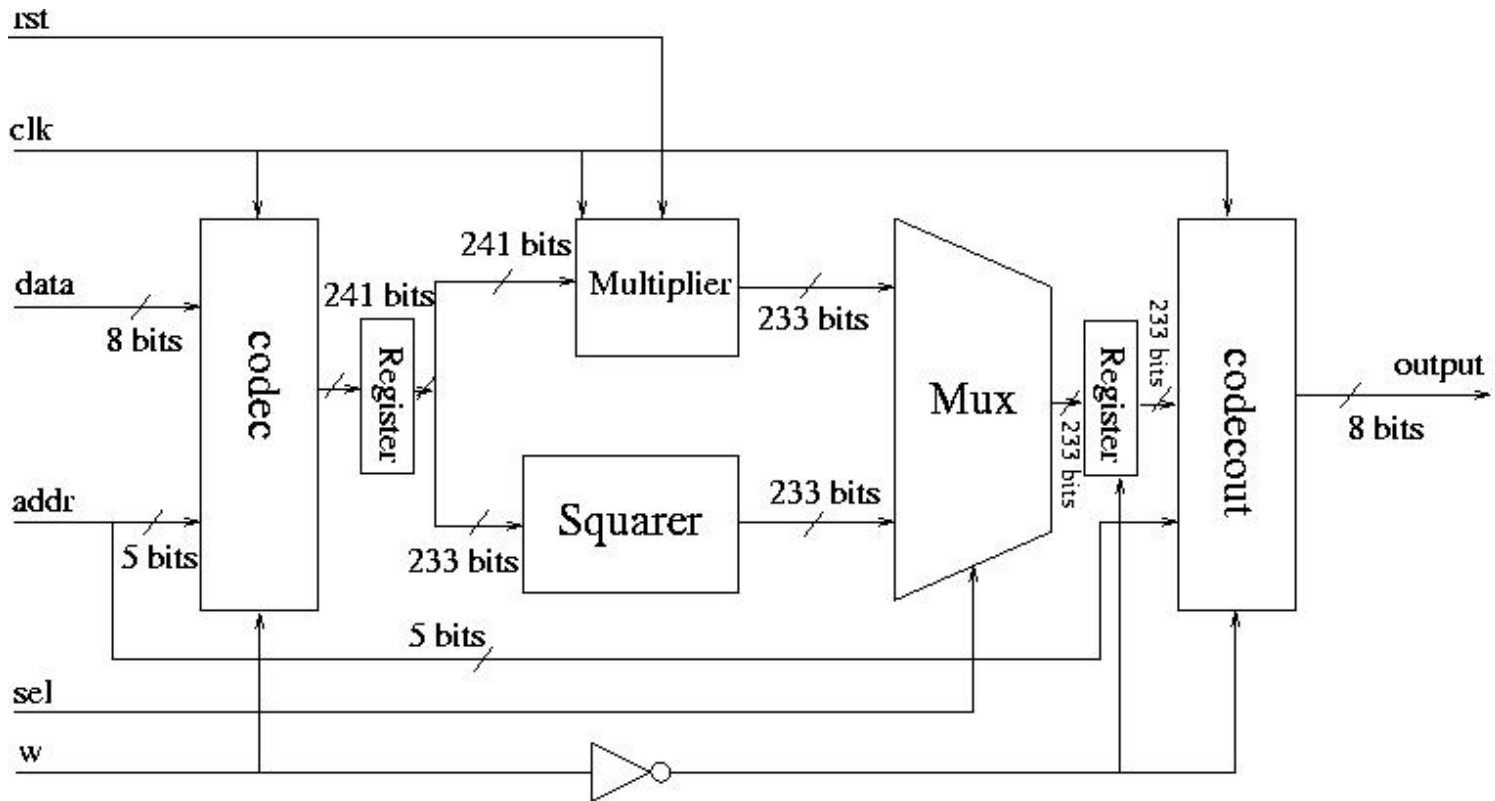
Comparisons

Multiplier	Finite field	Speed (Clock cycle)	Circuit complexity
Parallel	GF(2^{233})	1	233^2 AND gates 233^2-1 XOR gates
Serial		233	two 233-bit registers 233 AND gates 234 XOR gates
Proposed BPWS		30	$8*233$ AND gates $8*233+36$ XOR gates one 233-bit register
Alternative BPWS		30	$8*233$ AND gates $8*233 +36$ XOR gates Two 233-bit registers
General BPWS Trinomail ($1 < k < m/2$ p word width)	GF(2^m)	Ceiling function of (m/p)	$p*m$ AND gates $p*m+(p+1)p/2$ XOR gates One m-bit register

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

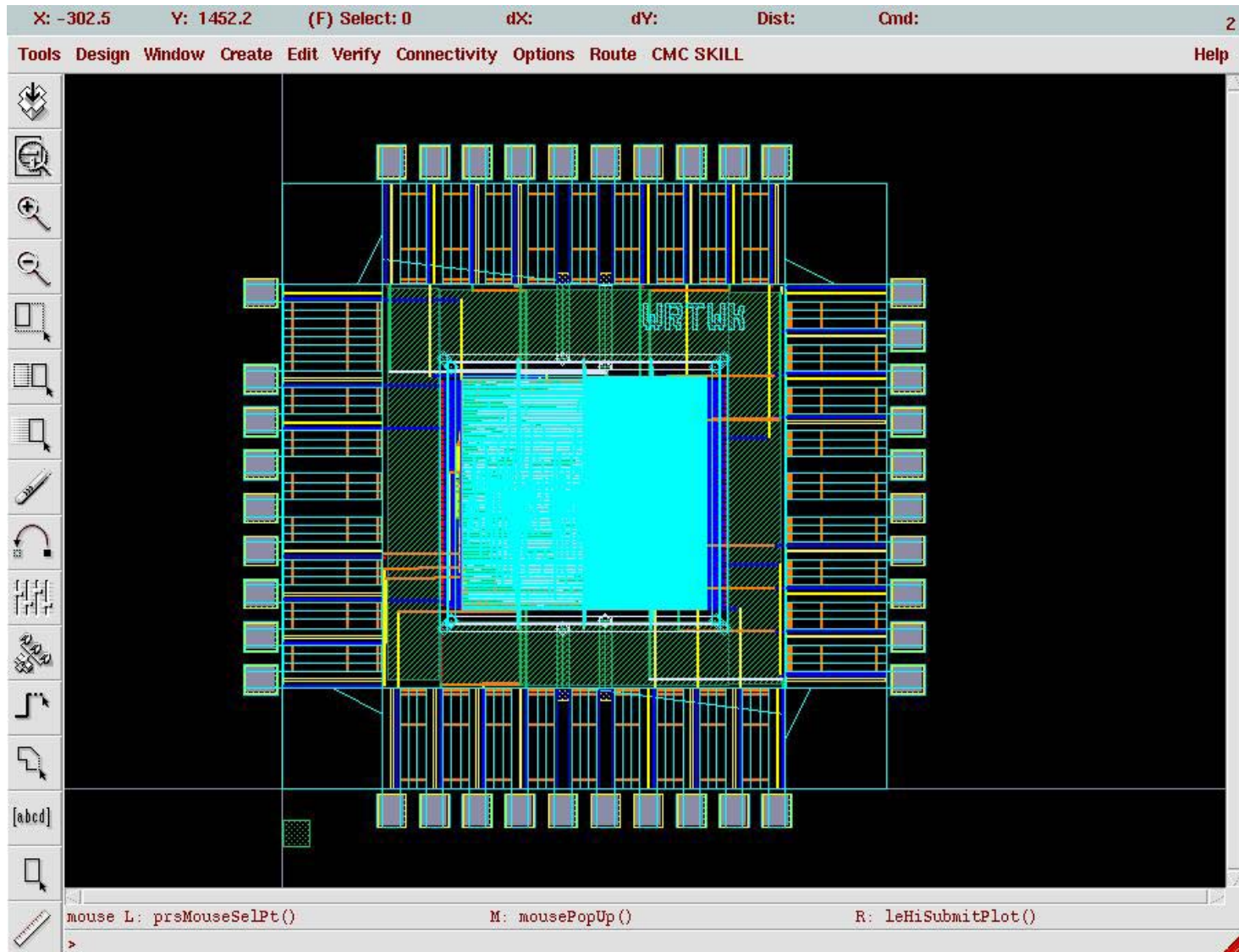
Hardware schematic



Final results and comparisons

Multiplier	Frequency (MHz)	Field size	# of cells	Gate counts	Area (μm^2)	VLSI technology
BPWS 8x233	50 (max. 130)	2^{233}	3029	4893	189297.06439	TSMC 0.18 μm CMOS
Squarer			293	293	6437.15746	
Classical 233x233 [1]	77	2^{233}	37296 LUTs 37552 FFs	528427	N/A	Xilinx FPGA XC2V6000- ff1517-4
Hans et al MSD 64x256 [2]	66.4	$\leq 2^{256}$	14797 LUTs 2948 FFs	136064	N/A	Xilinx FPGA Virtex-II XCV2000E-7
Souichi et al 8x288 [3]	3	$\leq 2^{576}$	2*8*288 ANDs 2*8*288 XORs 3*(8+288) FFs	14544	N/A	ALTERA FPGA EPF10K250AG C5992

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 8×233 partial product generator is designed.
- Future work expected is to use this multiplier in security processor for smart card.

References

- [1] Grabbe C., Bednara M., Teich J., Von Zur Gathen J., Shokrollahi J, “FPGA designs of parallel high performance $GF(2^{233})$ multipliers”, Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on , Volume: 2 , 25-28 May 2003
- [2] Hans Eberle, Sheueling Chang, Nils Gura, Sumit Gupta, Dniel Finchelstein, Edouard Goupy, Douglas Stebila, “ An End-to-End Systems Approach to Elliptic Curve Cryptography” Sun Microsystems Laboratories 2002-2003
- [3] Souichi Okada, Naoya Torii, Kouichi Itoh, Masahiko Takenaka, “Implementation of Elliptic Curve Cryptographic Coprocessor over $GF(2^m)$ on an FPGA”, C.K. Koc and C. Paar (Eds.): CHES 2000, LNCS 1965, pp. 25-40, 2000. Springer-Verlag Berlin Heidelberg 2000

Question ?

THANK YOU !