A Racetrack Memory Based In-memory Booth Multiplier for Cryptography Application

Tao Luo[1], Wei Zhang[2], Bingsheng He[1], Douglas Maskell[1]

[1]School of Computer Engineering, Nanyang Technological University

[2]Department of Electronic & Computer Engineering, Hong Kong University of Science and Technology

26th Jan 2016

Outline

- Motivations
- Background and Related Work
- Proposed Racetrack Memory Based Adder
- Proposed Booth Multiplier
- Experimental Results
- Conclusions

Outline

- Motivations
- Background and Related Work
- Proposed Racetrack Memory Based Adder
- Proposed Booth Multiplier
- Experimental Results
- Conclusions

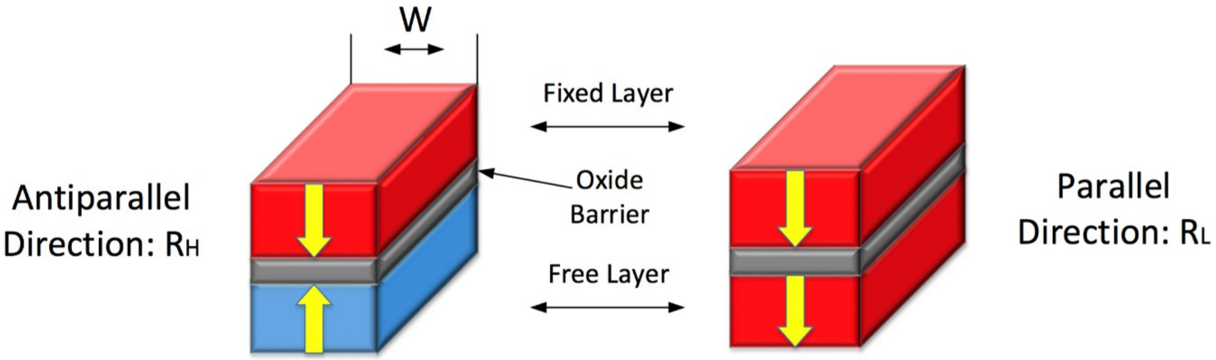
Motivation

- Big-data scaled data center for cloud computing
  - Data density
  - Data security
- Asymmetric encryption schemes
  - Internet-based applications
  - Time and resource consuming
- Racetrack memory
  - High data density, non-volatility, low static power and high speed
  - Data storage medium in data center
- In-memory encryption for racetrack memory
  - Avoid racetrack memory access time
  - Reduce the I/O requirement

Outline

- Motivations
- Background and Related Work
- Proposed Racetrack Memory Based Adder
- Proposed Booth Multiplier
- Experimental Results
- Conclusions

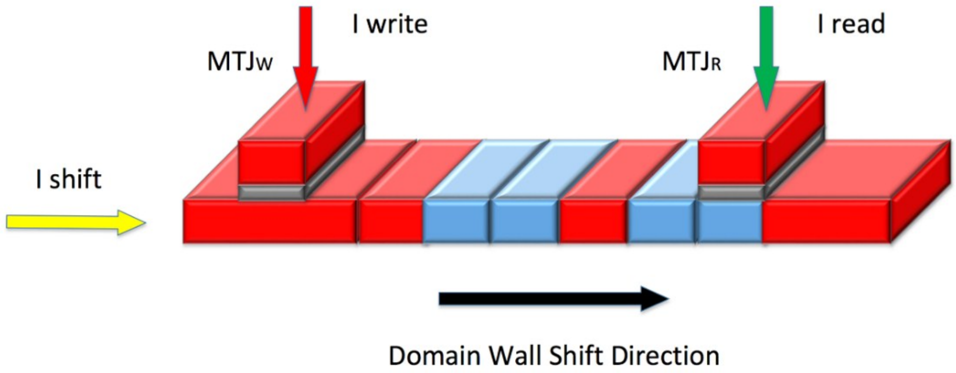
Background: Racetrack Memory



Basic structure of vertical magnetic tunnel junction

- Magnetic tunnel junction (MTJ)
  - One ferromagnetic (FM) layer with fixed magnetization direction
  - One FM layer with free magnetization direction
  - An oxide barrier between the two FM layers
- Resistance of the MTJ
  - High resistance R_H: The two FM layers have antiparallel direction
  - Low resistance R_L: The two FM layers have parallel direction
  - Two different states: “0” and “1”

Background: Racetrack Memory



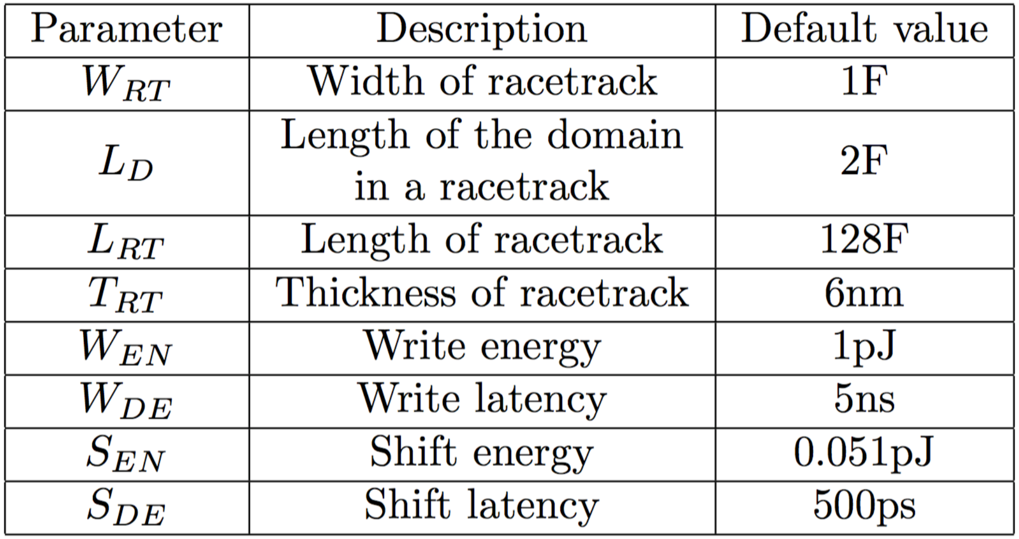
Basic structure of stripe of the racetrack memory

- Storage format
  - Each unit stores one bit
  - 50-100 nm wide for each unit
  - The stripe can be as long as 256 bits
- Read, write, shift
- Advantage: High data density
- Disadvantage: Long access time

Background: Racetrack Memory

- Racetrack memory has very small characteristic parameters:
  - 1 F = 45nm
- Write and shift
  - Write latency is 10X as shift latency
  - Write energy is 20X as shift energy

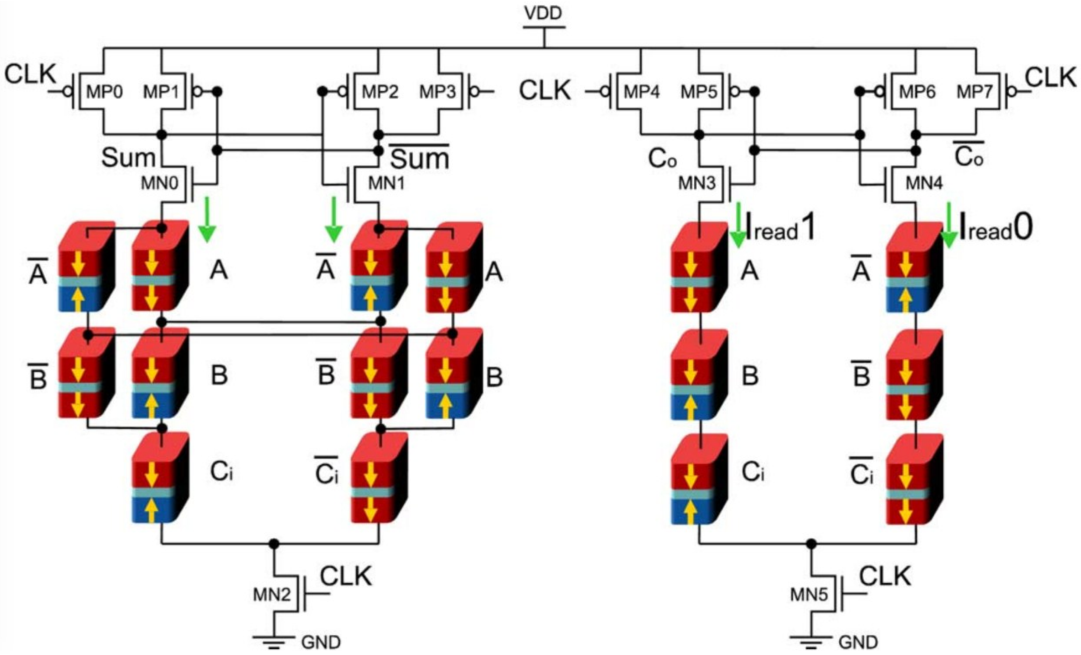
Main Parameters in the racetrack memory model



Parameter	Description	Default value
W_{RT}	Width of racetrack	1F
L_D	Length of the domain in a racetrack	2F
L_{RT}	Length of racetrack	128F
T_{RT}	Thickness of racetrack	6nm
W_{EN}	Write energy	1pJ
W_{DE}	Write latency	5ns
S_{EN}	Shift energy	0.051pJ
S_{DE}	Shift latency	500ps

Related Work: Magnetic Full Adder

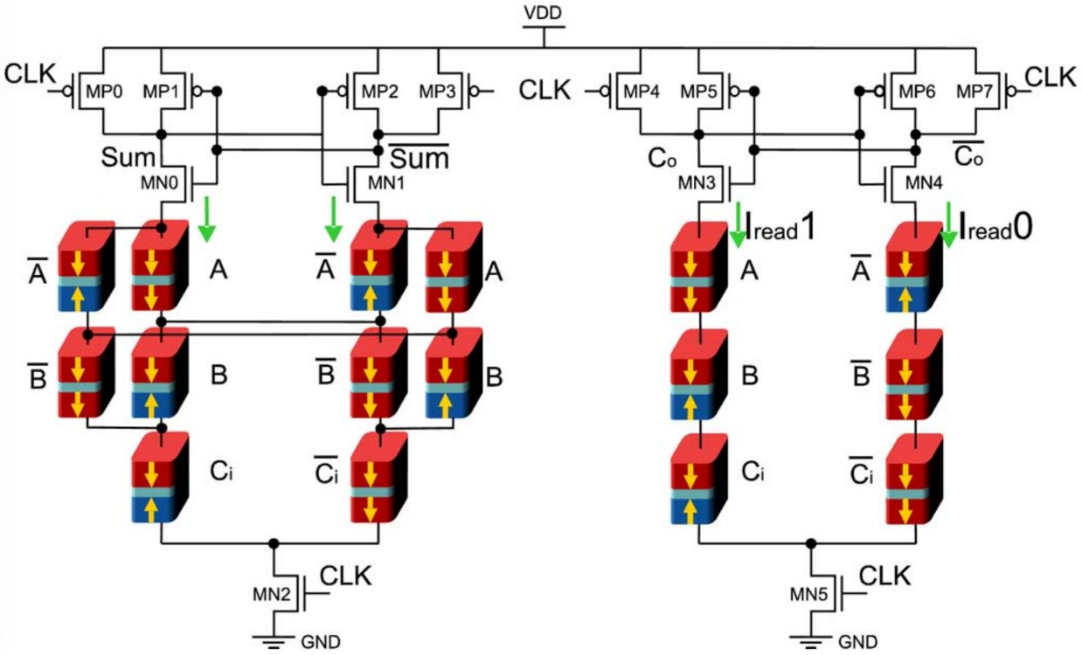
- Magnetic full adder
  - A spintronic full adder [Meng et al., EDL’05]
  - A non-volatile full adder [Matsunaga et al., APE’08]
  - Racetrack memory based adder [Trinh et al., TCAS-I’13]



Magnetic full adder

Related Work: Magnetic Full Adder

- The previous MFA [Trinh et al., TCAS-I'13]
  - MTJ logic tree
  - *"Sum"* signal and *"Co"* signal are realized separately
- Drawbacks
  - Too many MTJs
  - Too many write operations lead to high power consumption



Magnetic full adder

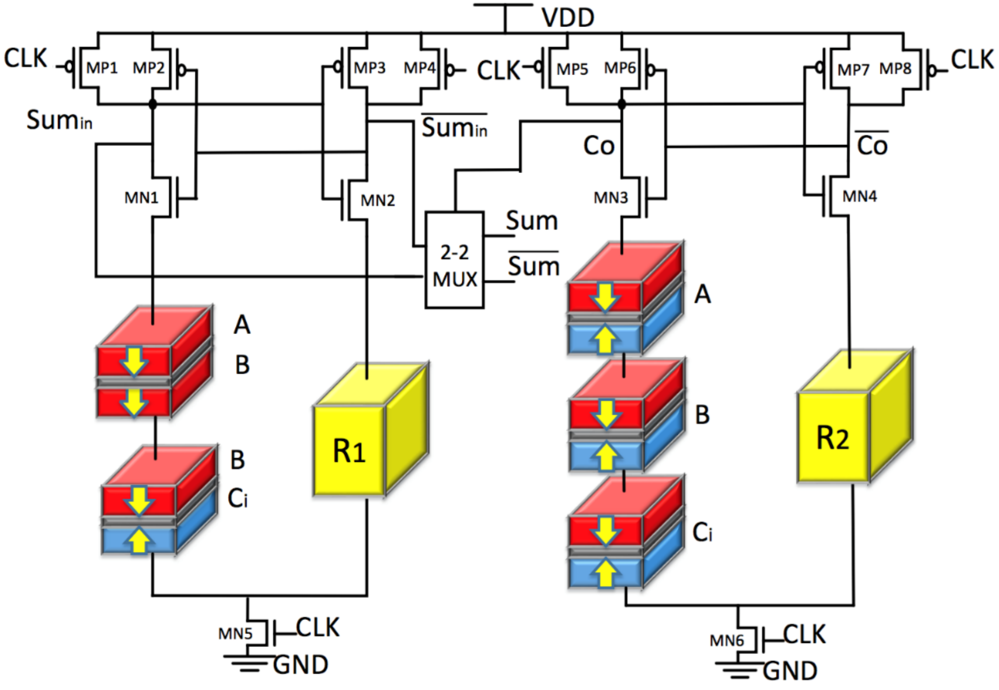
Outline

- Motivations
- Background and Related Work
- Proposed Racetrack Memory Based Adder
- Proposed Booth Multiplier
- Experimental Results
- Conclusions

NANYANG TECHNOLOGICAL UNIVERSITY

Proposed Racetrack Memory Based Adder: Generation of Carry Out Signal

- Pre-charge sense amplifier (PCSA) is used to read the data out
  - Best sensing reliability
  - High power efficiency
  - High speed performance
- Generation of carry out signal
  - $Co = A \cdot B + A \cdot Ci + B \cdot Ci$
  - A majority function

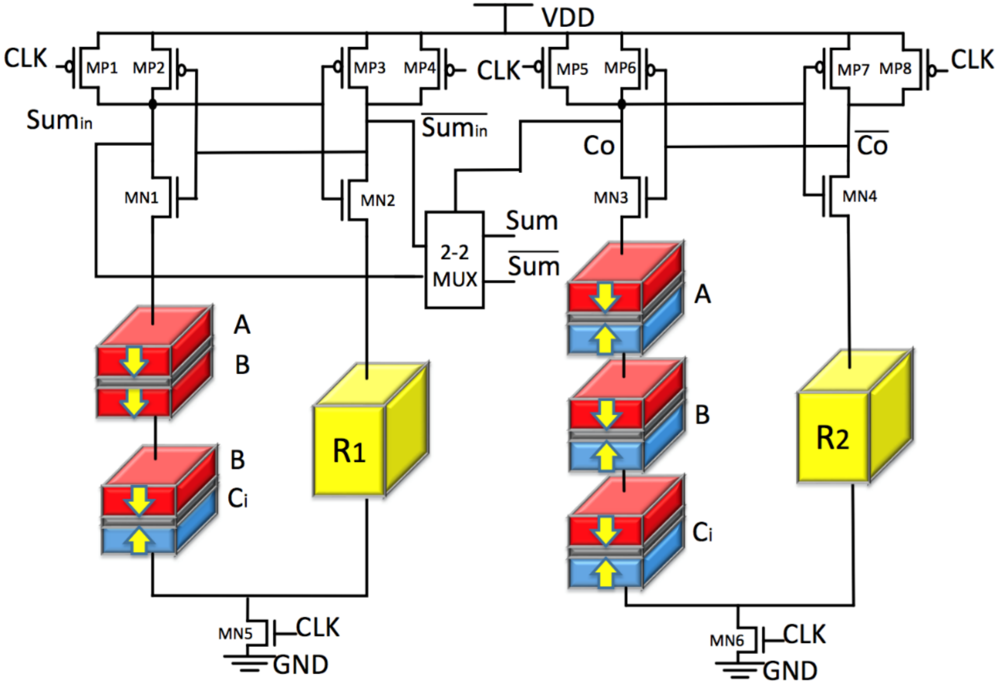


Proposed magnetic full adder

Proposed Racetrack Memory Based Adder: Generation of Carry Out Signal

Truth table of carry out signal

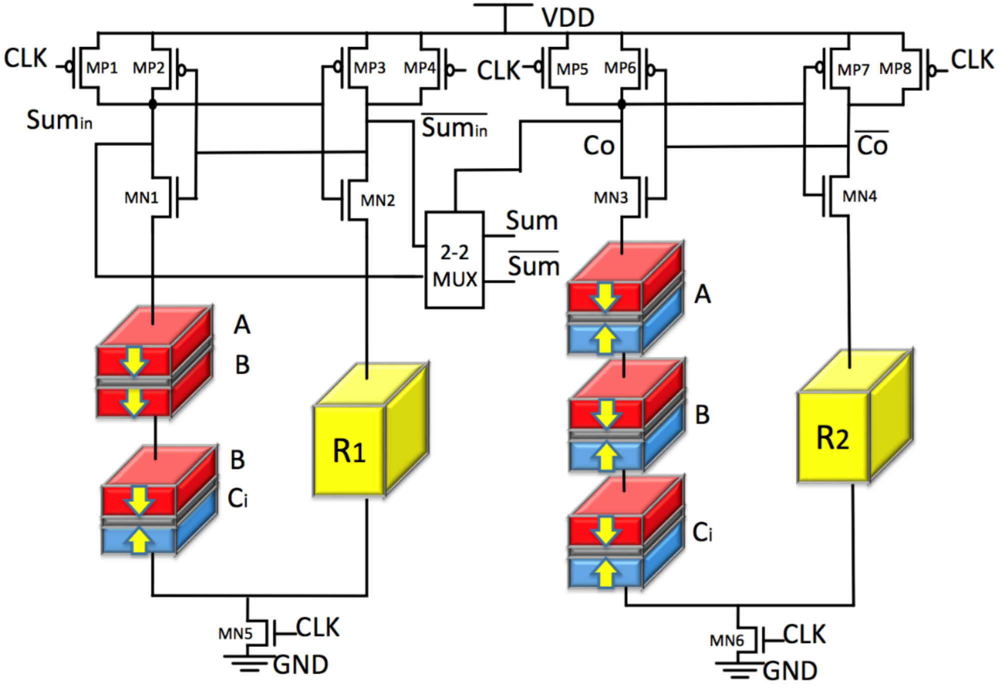
A	B	C_i	R_{left}	R_{right}	C_o
0	0	0	$3R_L$	$2R_H$	0
0	0	1	$2R_L + R_H$	$2R_H$	0
0	1	0	$2R_L + R_H$	$2R_H$	0
0	1	1	$R_L + 2R_H$	$2R_H$	1
1	0	0	$2R_L + R_H$	$2R_H$	0
1	0	1	$R_L + 2R_H$	$2R_H$	1
1	1	0	$R_L + 2R_H$	$2R_H$	1
1	1	1	$3R_H$	$2R_H$	1



Proposed magnetic full adder

Proposed Racetrack Memory Based Adder: Generation of *“Sum”* Signal

- Generation of *“Sum”* signal
  - $Sum = A \oplus B \oplus Ci$
  - A complicated logic function
- Combination with signal *“Co”*
  - The logic function of *“Co”* is a majority function
  - *A/B* and *B/Ci* to form the left branch
  - A MUX is added in the adder
  - *“Co”* is used as a select signal

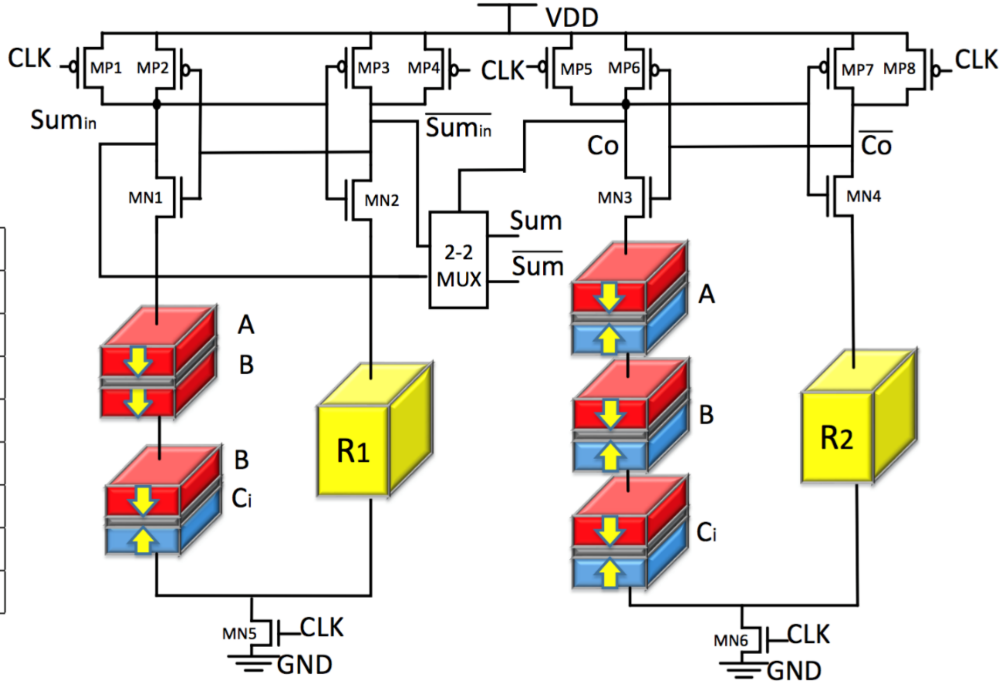


Proposed magnetic full adder

Proposed Racetrack Memory Based Adder: Generation of *"Sum"* Signal

Truth table of *"Sum"* signal

A	B	C_i	R_{left}	R_{right}	C_o	Sum_{in}	Sum
0	0	0	$2R_L$	R_H	0	0	0
0	0	1	$R_L + R_H$	R_H	0	1	1
0	1	0	$2R_H$	R_H	0	1	1
0	1	1	$R_L + R_H$	R_H	1	1	0
1	0	0	$R_L + R_H$	R_H	0	1	1
1	0	1	$2R_H$	R_H	1	1	0
1	1	0	$R_L + R_H$	R_H	1	1	0
1	1	1	$2R_L$	R_H	1	0	1



Proposed magnetic full adder

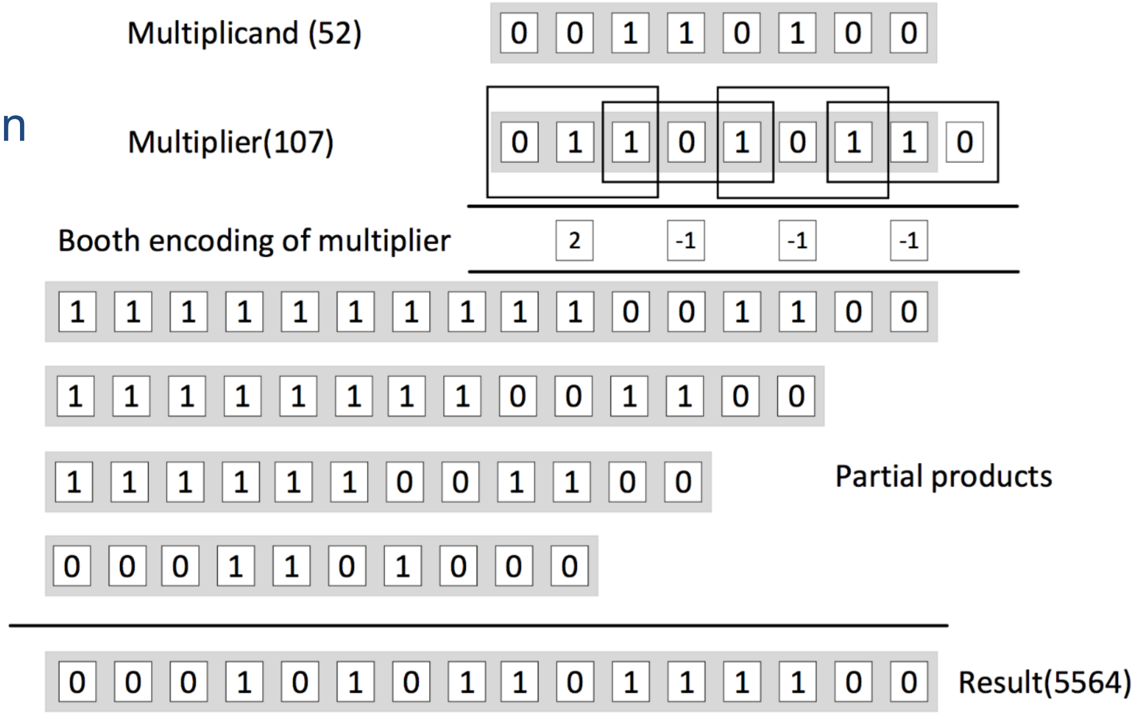
Outline

- Motivations
- Background and Related Work
- Proposed Racetrack Memory Based Adder
- Proposed Booth Multiplier
- Experimental Results
- Conclusions

NANYANG
TECHNOLOGICAL
UNIVERSITY

Proposed Booth Multiplier: The Operation of The Booth Multiplication

- Multiplication
  - Partial products generation
  - Partial products addition
- Booth algorithm
  - Recoding of the multiplier
  - Radix-4 Booth algorithm
- Advantages
  - Reduction of the number of partial products
  - Improvement of the performance, area and power



Multiplicand (52) 0 0 1 1 0 1 0 0

Multiplier(107) 0 1 1 0 1 0 1 1 0

Booth encoding of multiplier 2 -1 -1 -1

1 1 1 1 1 1 1 1 1 1 0 0 1 1 0 0

1 1 1 1 1 1 1 1 0 0 1 1 0 0

1 1 1 1 1 1 0 0 1 1 0 0 Partial products

0 0 0 1 1 0 1 0 0 0

0 0 0 1 0 1 0 1 1 0 1 1 1 1 0 0 Result(5564)

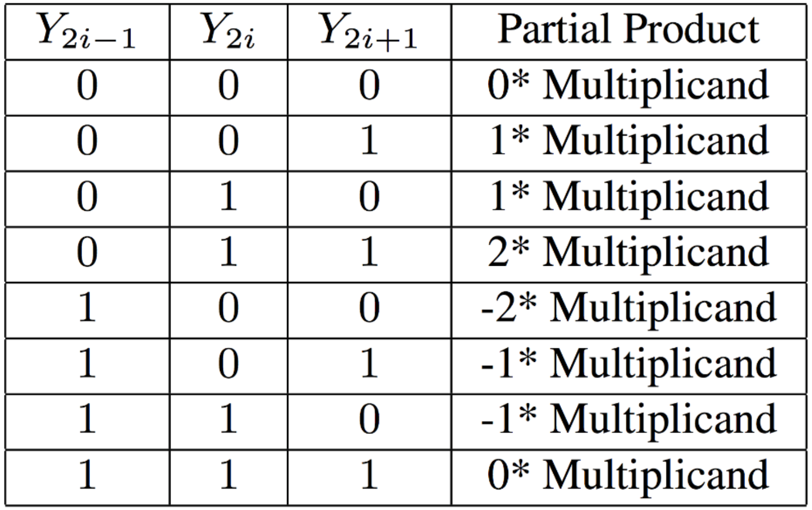
The operation of the Booth multiplication

NANYANG TECHNOLOGICAL UNIVERSITY

Proposed Booth Multiplier: Partial Products Generation

- Encoding and decoding
  - Y_{2i-1}, Y_{2i} and Y_{2i+1} are digits of the input blocks of the multiplier
  - "0*" means the partial product equals to zero multiplying the multiplicand.
  - It is the same for "1*", "2*", "-1*" and "-2*".

Encoding and decoding regarding to block inputs



Y_{2i-1}	Y_{2i}	Y_{2i+1}	Partial Product
0	0	0	0* Multiplicand
0	0	1	1* Multiplicand
0	1	0	1* Multiplicand
0	1	1	2* Multiplicand
1	0	0	-2* Multiplicand
1	0	1	-1* Multiplicand
1	1	0	-1* Multiplicand
1	1	1	0* Multiplicand

Proposed Booth Multiplier: Partial Products Generation

- Control signals
  - *“zero”* corresponds to “0*”
  - *“one”* corresponds to “1*”
  - *“two”* corresponds to “2*”
  - *“ne_two”* corresponds to “-2*”
  - *“ne_one”* corresponds to “-1*”

Control signals for the partial products generation

$$zero = Y_{2i-1} \cdot Y_{2i} \cdot Y_{2i+1} + \overline{Y_{2i-1}} \cdot \overline{Y_{2i}} \cdot \overline{Y_{2i+1}}$$

$$one = \overline{Y_{2i-1}} \cdot \overline{Y_{2i}} \cdot Y_{2i+1} + \overline{Y_{2i-1}} \cdot Y_{2i} \cdot \overline{Y_{2i+1}}$$

$$two = \overline{Y_{2i-1}} \cdot Y_{2i} \cdot Y_{2i+1}$$

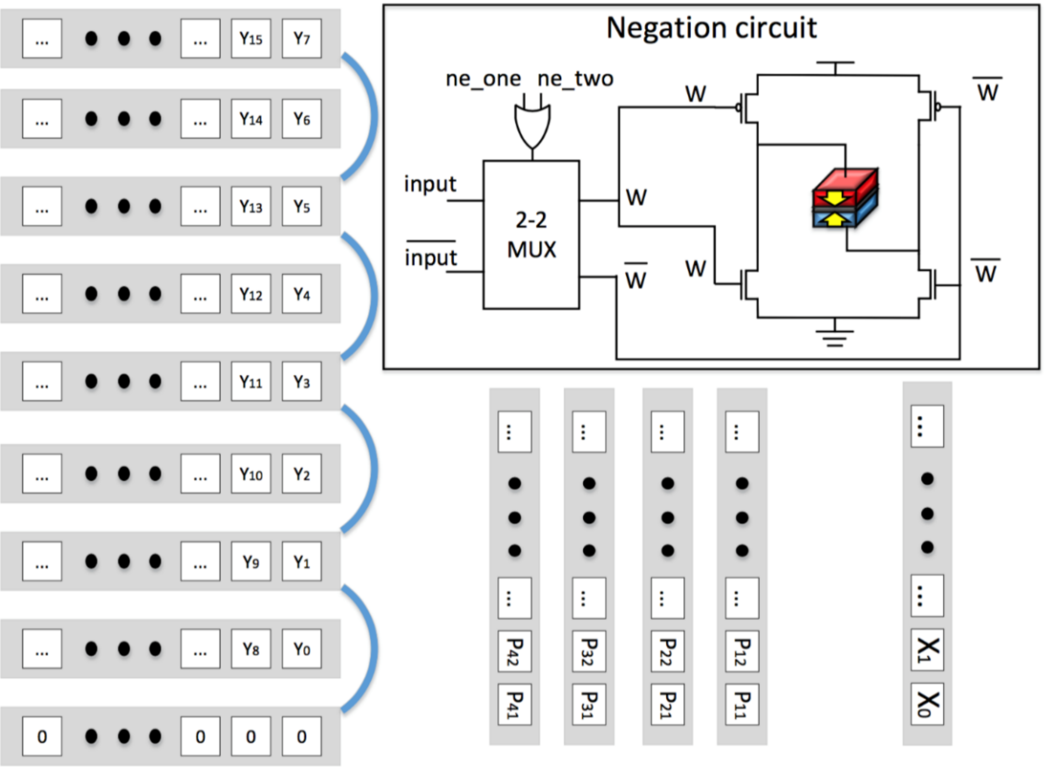
$$ne\_two = Y_{2i-1} \cdot \overline{Y_{2i}} \cdot \overline{Y_{2i+1}}$$

$$ne\_one = Y_{2i-1} \cdot \overline{Y_{2i}} \cdot Y_{2i+1} + Y_{2i-1} \cdot Y_{2i} \cdot \overline{Y_{2i+1}}$$

NANYANG
TECHNOLOGICAL
UNIVERSITY

Proposed Booth Multiplier: Partial Products Generation

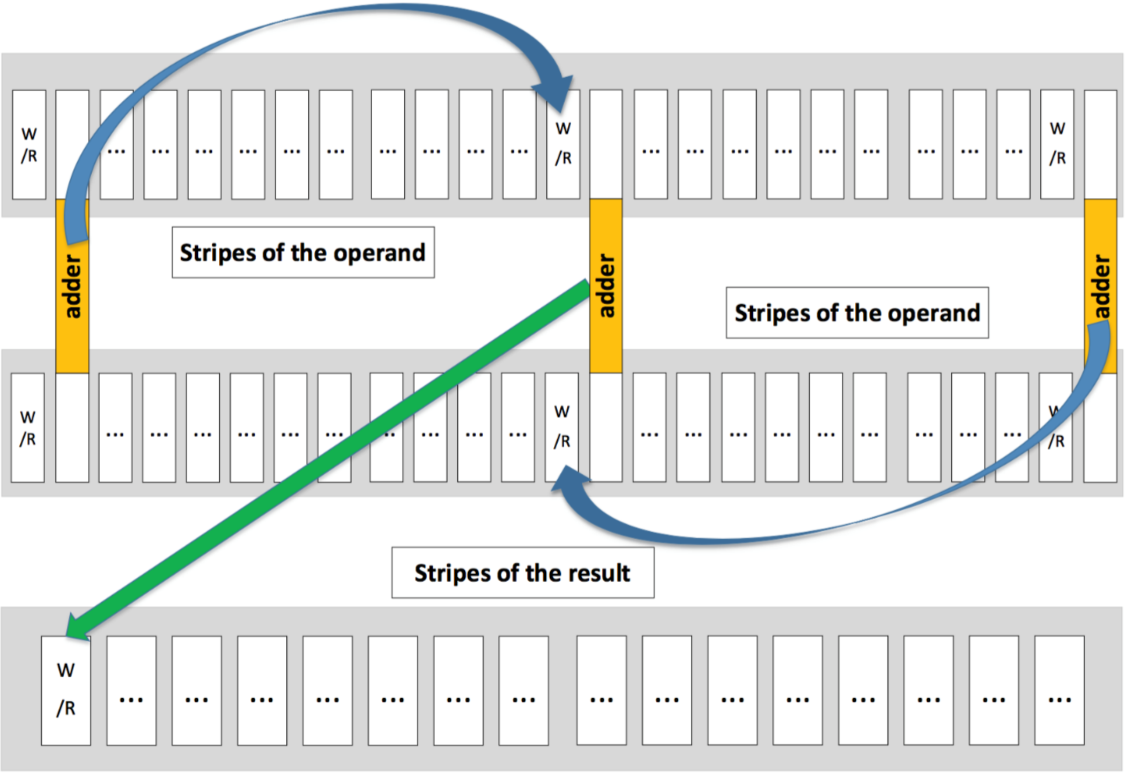
- Partial products are generated in parallel
- Five kinds of transformations
  - "remain"
  - "left-shifting"
  - "plusing-one"
  - "setting-to-zero"
  - "negation"
- Realization of the five transformations



Data organization for generation of partial products

Proposed Booth Multiplier: Addition of Partial Products

- Pipelined structure
  - Racetrack memory is used as the stage register
  - Pipeline can be very deep
- Advantages
  - Easy to realize
  - Efficient in terms of racetrack memory resource
  - High scalability



The pipelined addition based on racetrack memory

Outline

- Motivations
- Background and Related Work
- Proposed Racetrack Memory Based Adder
- Proposed Booth Multiplier
- Experimental Results
- Conclusions

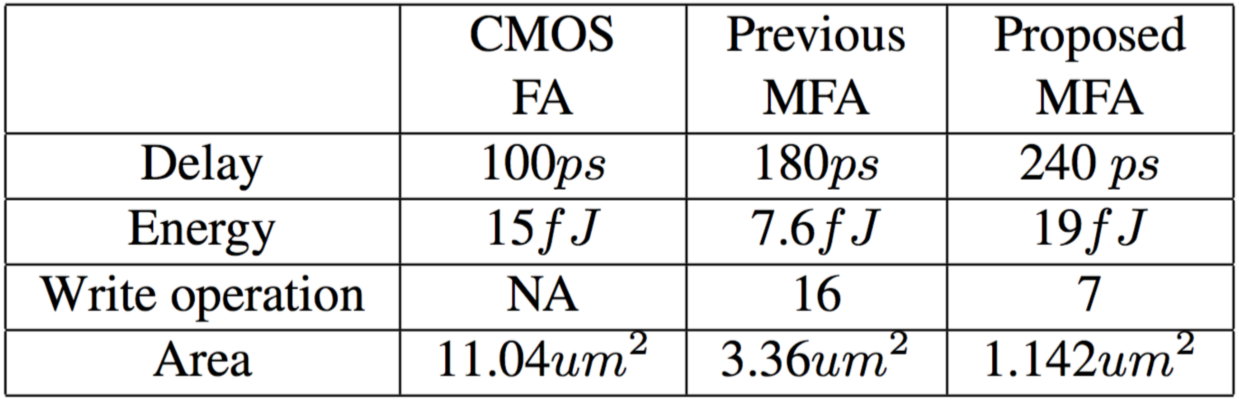
NANYANG TECHNOLOGICAL UNIVERSITY

Experimental Result:

1-bit magnetic full adder

- CMOS 45*nm* design kit
- A model of perpendicular magnetic anisotropy (PMA) racetrack memory based on CoFeB/MgO structure

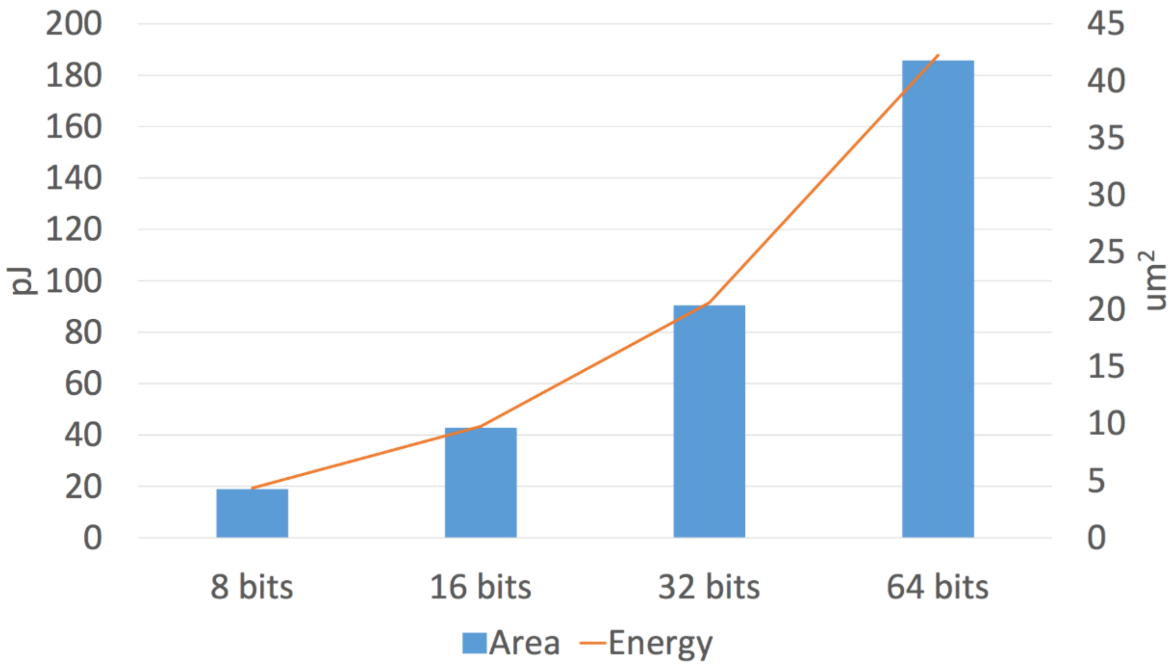
Comparison of the three adders



	CMOS FA	Previous MFA	Proposed MFA
Delay	$100ps$	$180ps$	$240\ ps$
Energy	$15fJ$	$7.6fJ$	$19fJ$
Write operation	NA	16	7
Area	$11.04um^2$	$3.36um^2$	$1.142um^2$

Experimental Result:

Racetrack memory based Booth multiplier



Energy per bit and area of our proposed multipliers with different input length

Conclusions

- Propose a compact racetrack memory based adder to reduce the number of write operation
- Design Booth encoder and decoder of the in-memory Booth multiplier for generating the partial products in parallel
- Implement a pipelined in-memory Booth multiplier for the encryption application in racetrack memory based data center

Thank you!

Questions?