ECC is Ready for RFID – A Proof in Silicon

RFIDsec 08 Presentation

Daniel Hein, daniel.hein@gmx.at
Johannes Wolkerstorfer, Johannes.Wolkerstorfer@iaik.tugraz.at
Norbert Felber, felber@iis.ee.ethz.ch

Outline I

- Radio Frequency Identification (RFID)
  - Product piracy
  - Authentication
- Elliptic Curve Cryptography (ECC)
  - Montgomery point multiplication
  - Binary extension field arithmetic
- ECCon processor architecture
  - RFID front-end
  - ECC processor
    - Small datapath Approach
    - Specialized ALU

Outline II

Digit level algorithms

- Multiplication
- Reduction
- Multiplication with interleaved reduction

Results

- Timing, Area, Power
- Comparison with related work

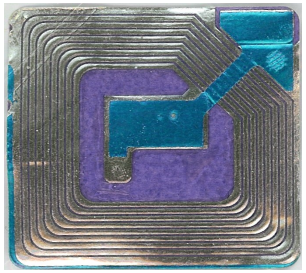
Radio Frequency Identification

Rapid automated item identification

Barcode replacement

Computer X-ray vision

- No line of sight
- No optical scanning



RFID Tag

- Antennae + IC
- Powered by EM field

Product Piracy

Causes considerable economic damage

Counterfeits inserted in legitimate supply chain

RFID tags

- Alleviate problem
- Easy to clone

Cryptography

- Authentication

Elliptic Curve Cryptography I

Public-key cryptography

- Short key => Small hardware footprint

Authentication with digital signature

- ECDSA

Security depends on point multiplication

Point multiplication

- scalar • point on elliptic curve
- Non-invertible

Elliptic Curve Cryptography II

Point multiplication

- Point addition
- Point doubling
- Montgomery point ladder algorithm

Side channel attack resistance

- Timing based attacks: MPLA
- Simple power analyses attacks: MPLA
- Differential power analyses attacks: ECDSA

Binary Extension Field Arithmetic

Elliptic Curve defined on finite field

Finite Fields

- Fixed size elements

Binary extension field

- Elements = binary polynomials
- Addition = XOR

Required Operations

- Addition
- Multiplication
- Reduction

Prerequisites of an RFID application

Small die area

- 15000 gate equivalents

Minuscule power consumption

- 15µA available mean current

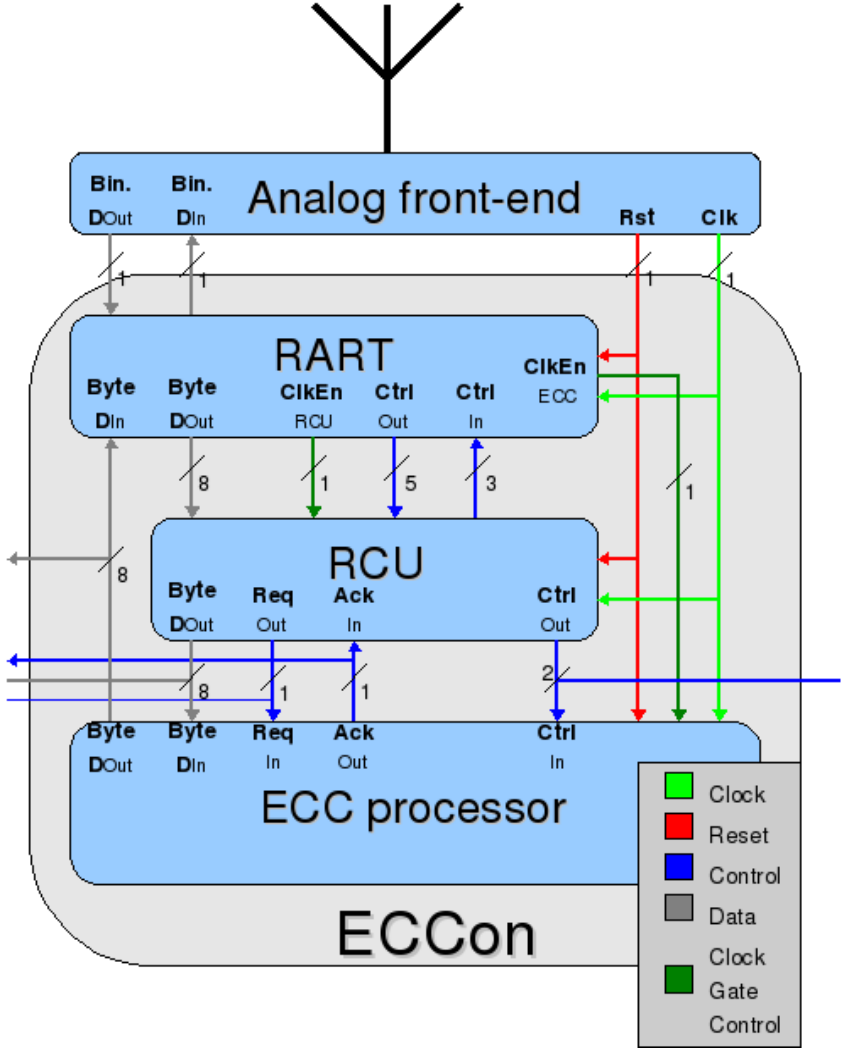
Constant power consumption

- “Accidental” load modulation

ECCon Top Level Architecture

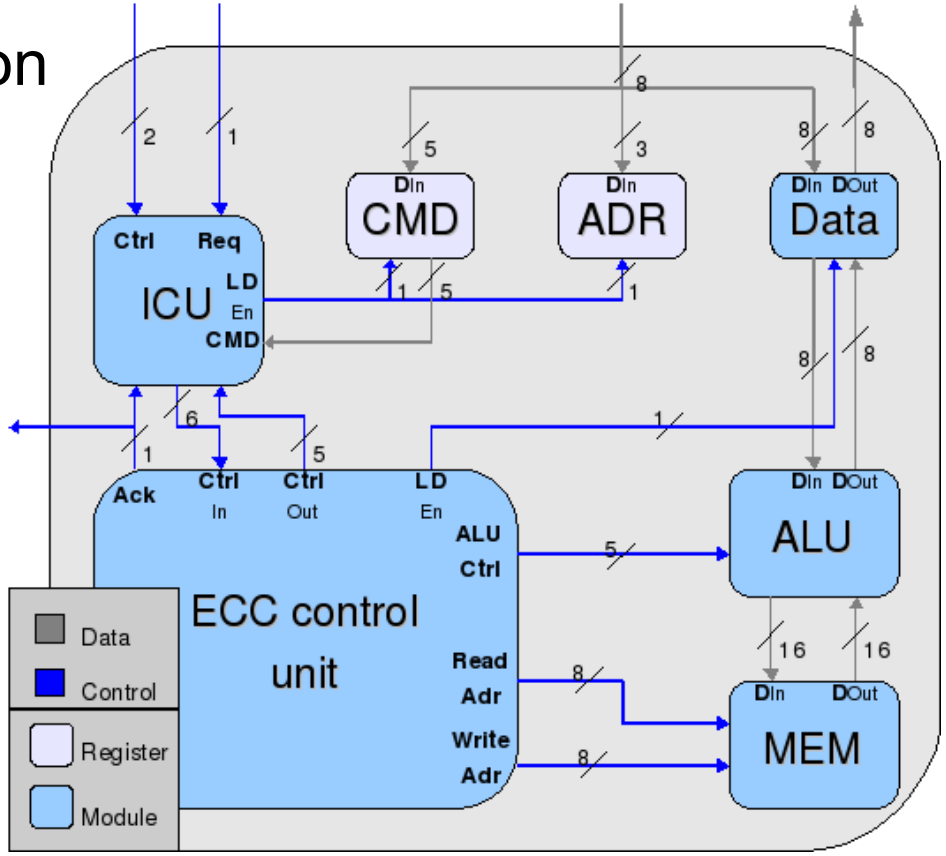
RFID front end

- ISO-18000-3-1 compliant
- Air Interface
  - Power supply
  - Clock generation
  - Signal modulation
- RART
  - Receive: bit stream to byte
  - Send: byte to bit stream
- RFID Control Unit (RCU)
  - Communication protocol
  - Manages ECC processor



ECC Processor Architecture I

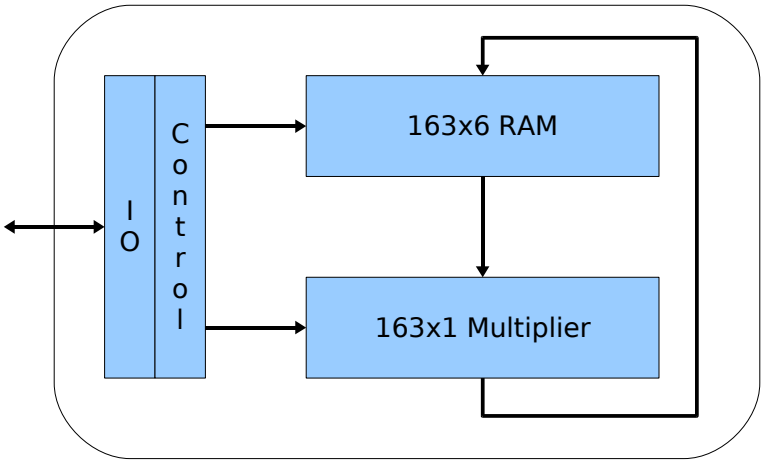
- Implements point multiplication
  - Fixed 163 bit NIST curve
- Supports two modes
  - RFID
  - Stand alone
- Interface
  - two-phase full handshake
  - 8 bit wide
- Control unit
  - hardwired FSM hierarchy



Low Power, Small Area ALU Architectures

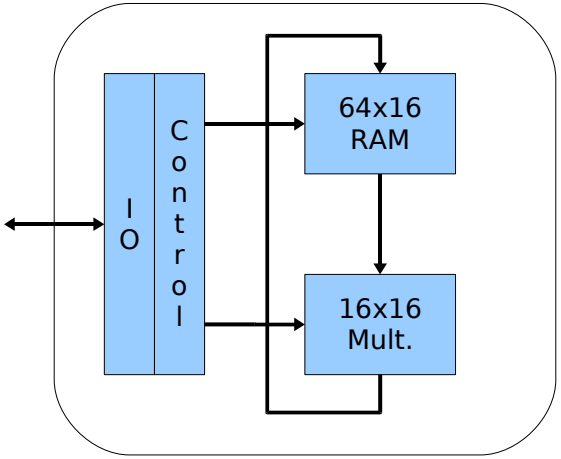
Bit-serial multiplier

- current state of the art
- 2x163 = 326 bits ALU storage
  - Lion's share of power used for clocking the storage



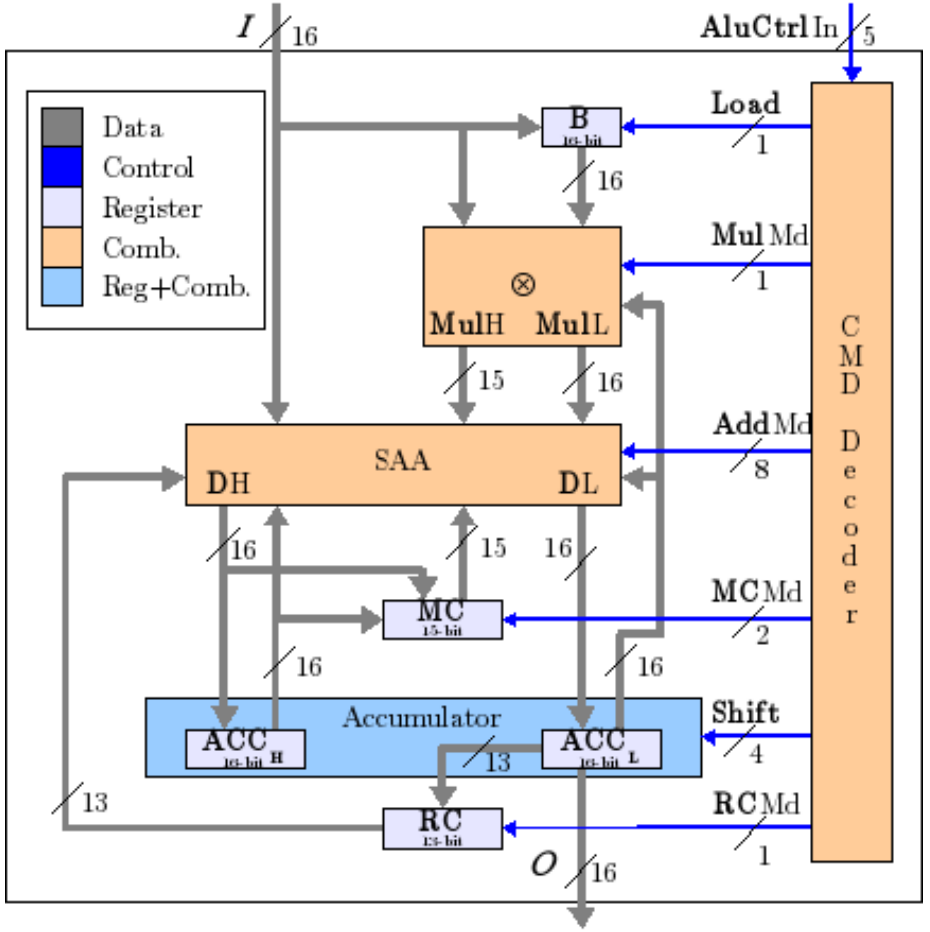
16-bit datapath

- Used for ISE [GK03a]
- Conceptually 48-bit ALU storage
  - More power for computation
- Total power consumption smaller
- Requires digit based algorithms

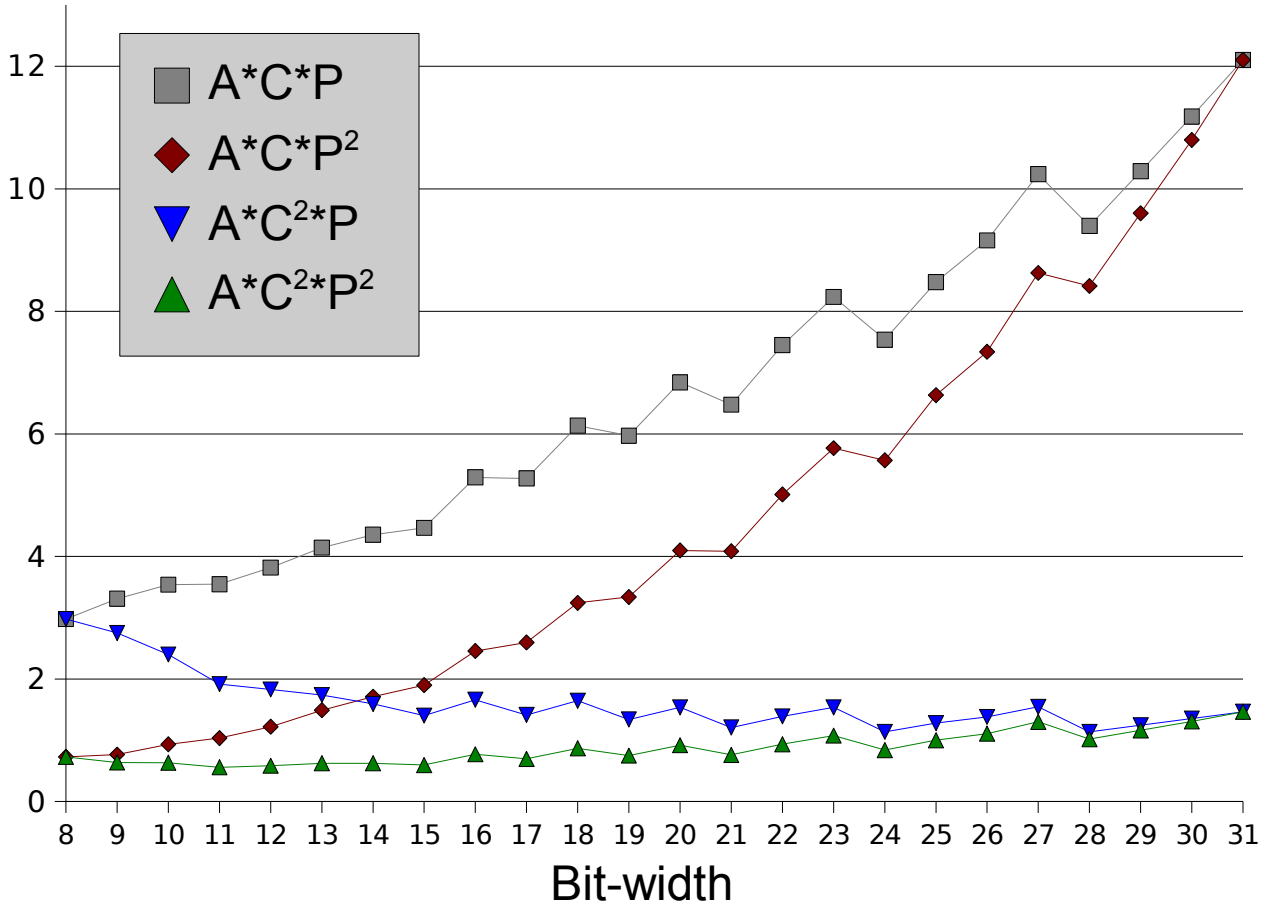


Arithmetic Logic Unit

- 16x16 GF(2) multiplier
- 2 Register input selection units
- 2 16-bit adders (XOR)
- Registers
  - 32-bit accumulator
  - interleaved reduction
    - 15-bit MC
    - 13-bit RC
  - clock gated



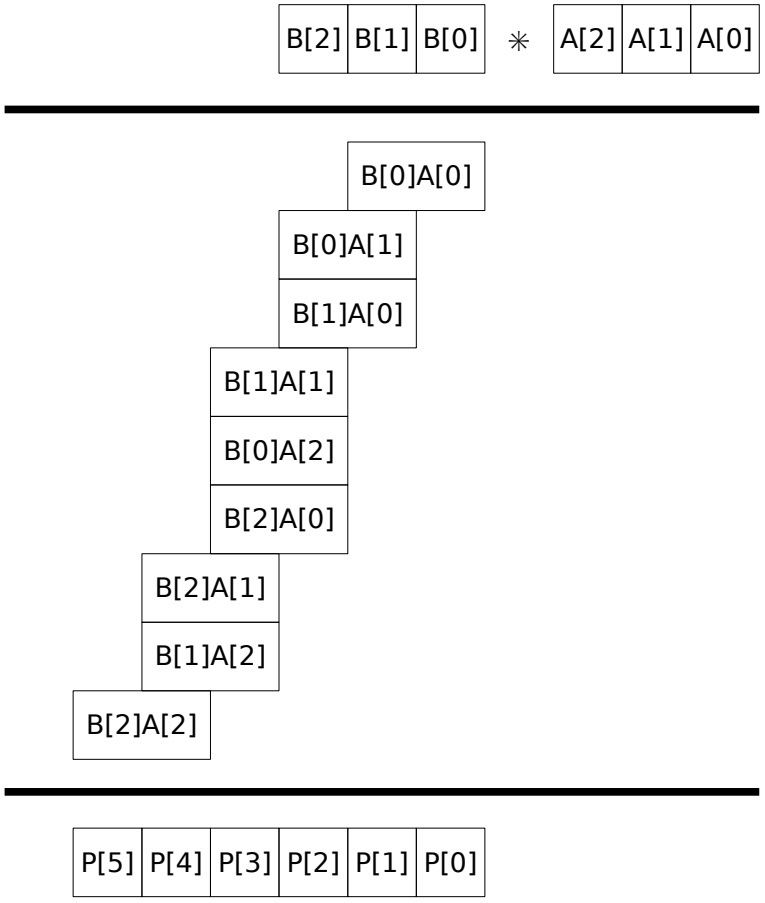
Word Size Selection



Comba Multiplication

Two possible digit multiplication algorithms
- Operand scanning form
- Product scanning form

Product Scanning Form
- A.k.a Comba Multiplication
- Computes result one result digit at the time
- Optimal operand order minimizes memory access



Modular Reduction in GF(2^{163})

Multiplication of 2 163-bit elements produces a 325-bit result: a(z)*b(z)=c(z); deg(c(z))=325

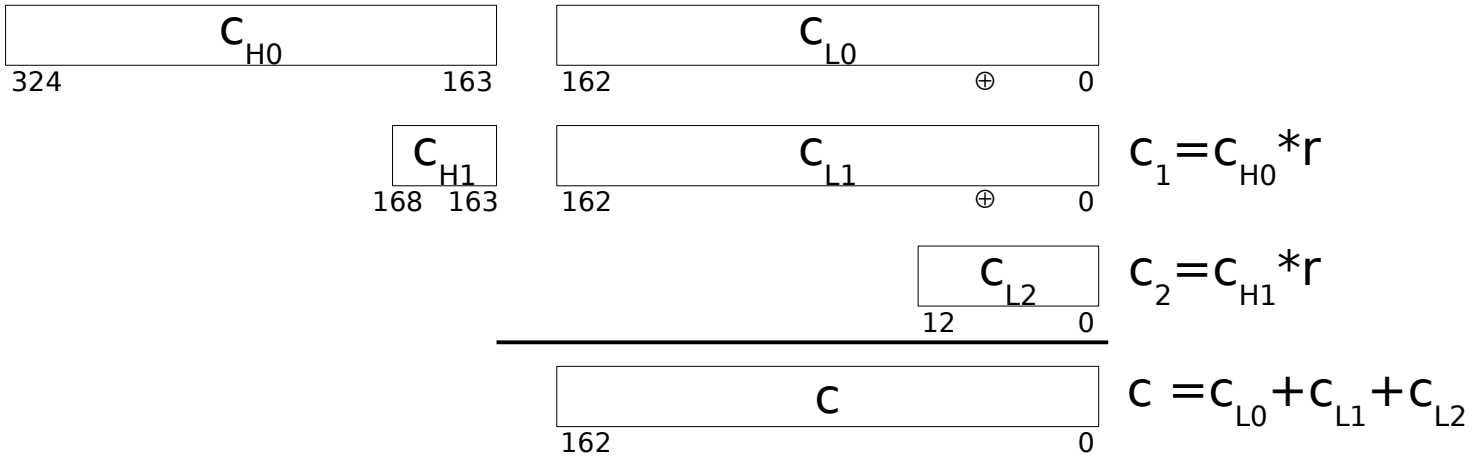
Common residue: $c(z) \equiv c(z) \pmod{f(z)}$

- $f(z) = z^{163}+z^7+z^6+z^3+1$... irreducible polynomial

The common residue is limited in size to 163 bits

The common residue is the remainder of a long division by f(z)

An Alternate Reduction Method

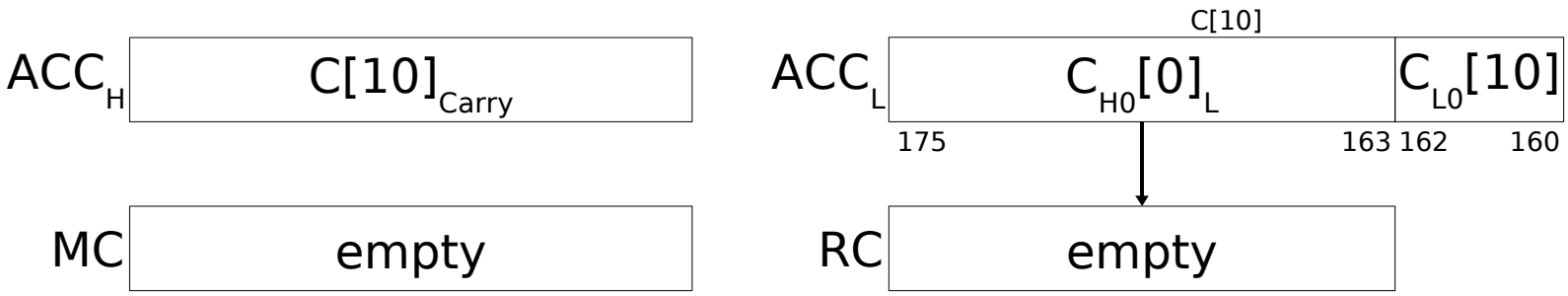


$$c(z)=c_{2m-2}z^{2m-2}+\ldots+c_m z^m+c_{m-1}z^{m-1}+\ldots+c_1 z+c_0$$

$$\equiv(c_{2m-2}z^{m-2}+\ldots+c^m)r(z)+c_{m-1}z^{m-1}+\ldots+c_1 z+c_0 \pmod{f(z)},$$

where the reduction polynomial $r(z)=f(z)-z^{163}=z^7+z^6+z^3+1$

Interleaved Reduction Step I



Computation of the first 10 digits of the product

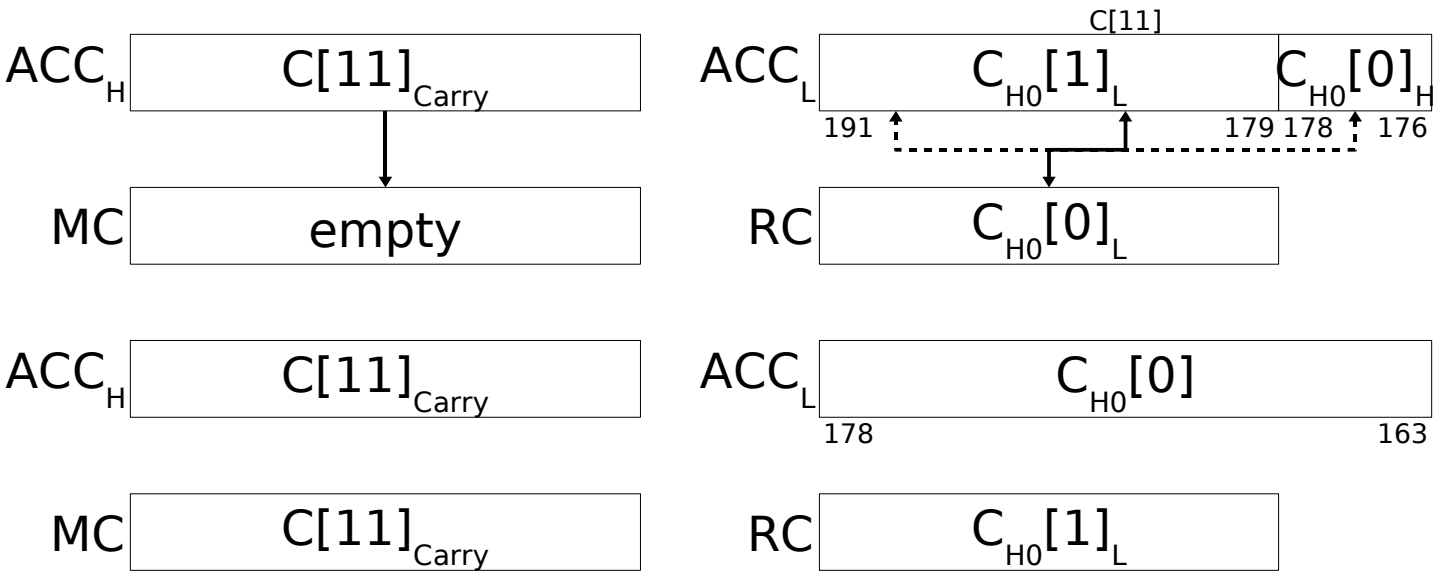
11th digit (C[10]) exceeds 163 bit limit

- Stored in ACC_L
- ACC_H contains multiplication carry for 12th digit C[11]

C[10] contains the first 13 bits of C_{H0}

- Saved to Reduction Carry register RC

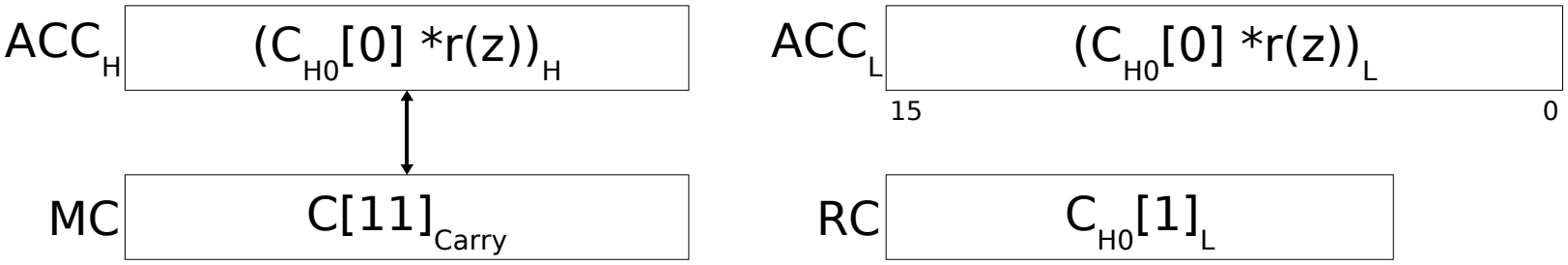
Interleaved Reduction Step II



Upon computation of 12th digit (C[11])

- Last 3 bits of $C_{H0}[0]$ become available
- $C_{H0}[0]$ is restored in ACC_L, lower 13 bit of $C_{H0}[0]$ saved to RC
- Multiplication carry is saved to Multiplication Carry register MC

Interleaved Reduction Step III

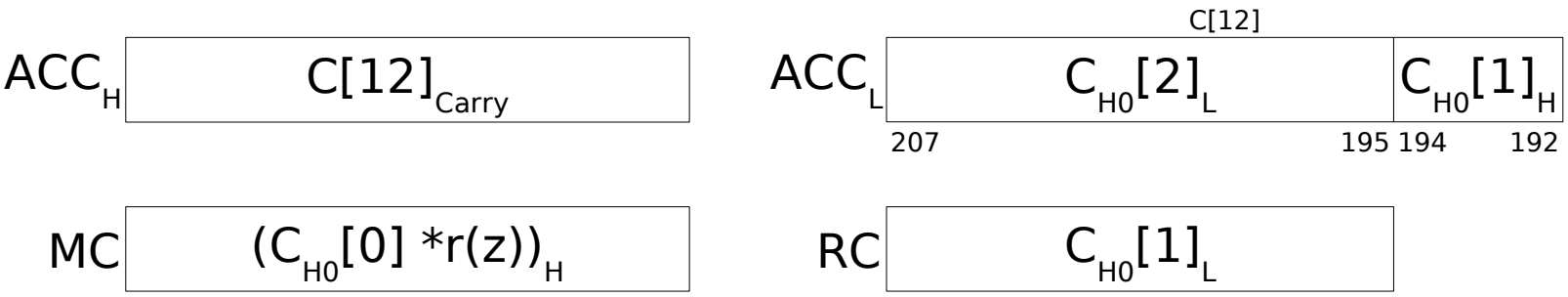


Multiplication of 1st digit of C_{H0} ($C_{H0}[0]$) with r(z) produces 1st digit of C_1 ($C_{L1}[0]$)

Addition of $C_{L1}[0]$ to $C_{L0}[0]$, Sum stored to result memory

Exchange of reduction multiplication carry and nominal multiplication carry

Interleaved Reduction Step IV



The next digit of the product (C[12]) is computed

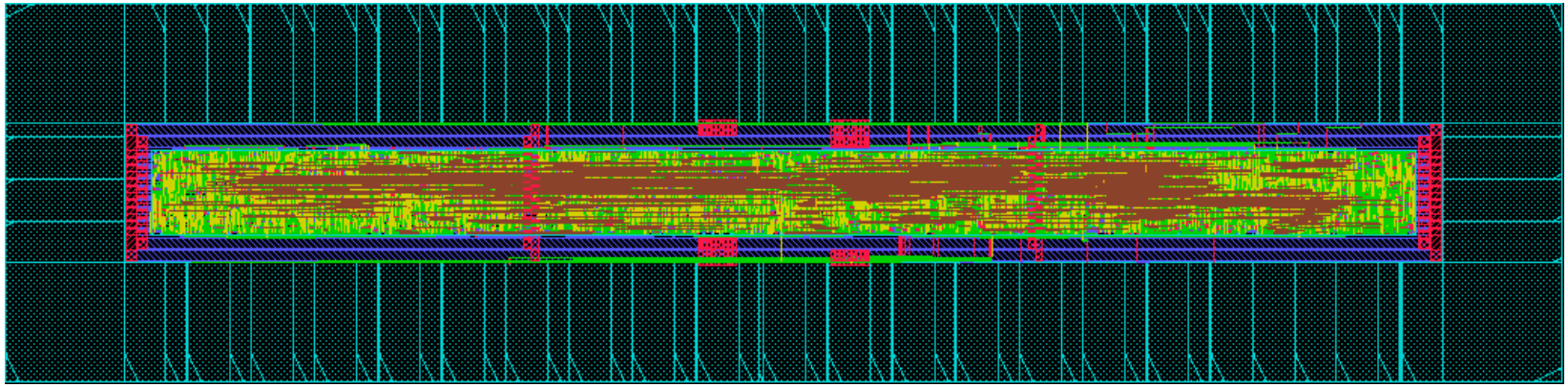
- Requires several MAC operations

Interleaved reduction steps I to IV repeat until all digits of C_1 are processed

Process is repeated for C_2

- Single multiplication and addition

ECCon



- Low power, small area ECC point multiplication device
- ISO-18000-3-1 compatible digital RFID front-end
- Technology: UMC L180 GII 1P/6M 1.8V/3.3V CMOS
- Core Size: 219897 µm2
- Clock Frequency: 46 MHz
- ECC processor power consumption at 106 kHz: 10.8 µW
- Built-in memory self-test/Full scan using one scan chain

Results I - Timing

Maximum frequencies:

- UMC 180: 46 MHz (unconstrained)
- AMS c35: 20 MHz (constrained)

Carrier frequency: f_c=13.56 MHz

RFID front-end

- RART: 6.78 MHz
- RCU: 106 kHz (f_c/128, clock gated)

ECC processor

- 850 kHz (f_c/16, clock gated)

Area & Power

Component	Area [µm²]	Area [GE]	Area [%]	Power [µW] @ 6,78 MHz	Power [µW] @ 848 kHz	Power [µW] @ 106 kHz
ECCon	144,823	14,976	100.00%	176	87	11.4
RCU	8,290	857	5.72%	10	1	0.2
RART	8,054	833	5.56%	20	3	0.4
ECC core	128,098	13,247	88.45%	146	83	10.8
Memory	91,117	9,423	62.92%	56	32	4.3
ALU	16,863	1,744	11.64%	44	40	5.0
Control (est.)	20,118	2,080	13.89%	46	11	1.5

Power Simulation

Comparison with related work

Source	Area [GE]	Runtime [kCycles]	Field	Technology	
[FWR05]	3.400		1 AES	AMS	350nm
ECCon w/o key	**11.904**		**296 GF(2^{163})**	**UMC**	**180nm**
[BBD+08]	12.876		80 GF(2^{163})	INF	220nm
[LSBV08]	12.168		272 GF(2^{163})	TSMC	130nm
[LV07]	13.182		314 GF(2^{163})	TSMC	180nm
[KP06]	15.094		430 GF(2^{163})	AMI	350nm
[Wol05]	23.000		426 GF(2^{191})	AMS	350nm
[FFW07]	23.656		502 GF(2^{192})	AMS	350nm

Source	Power [µW]	I_{mean}[µA]	f [MHz]	Technology	
[FWR05]	4,50	3,00	106 kHz	AMS	350nm
[BBD+]	79,00	?	847 kHz	INF	220nm
[LSBV08]	51,85	?	1.364 MHz	TSMC	130nm
ECCon	**10,80**	**6,00**	**106 kHz**	**UMC**	**180nm**
ECCon	**54,70**	**21,88**	**106 kHz**	**AMS**	**350nm**
ECCon	**83,00**	**46,11**	**847 kHz**	**UMC**	**180nm**
[FFW07]	141,00	42,73	106 kHz	AMS	350nm

Comparison with related work II

	ECCon	[BBD+]	[%]
Memory	8080	5273	65,26%
ALU	1744	6171	353,84%
Control	2080	1432	68,85%
Total	11904	12876	108,17%

ECCon

- Memory
  - higher requirements due to
    - Register based approach
    - Additional 163 bits storage
- ALU
  - Very compact due to small datapath
- Control
  - Increased complexity due to digit based algorithms

Thank you for your attention. Questions?

References I

[GK03a] Johann Großschädl and Guy-Armand Kamendje. Instruction set extension for fast elliptic curve cryptography over binary finite fields GF(2^m). In Proc. IEEE International Conference on Application-Specific Systems, Architectures, and Processors, pages 455–468, 2003.

[FWR05] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. Aes implementation on a grain of sand. *IEEE Proceedings Information Security*, 152(1):13–20, 2005.

[BBD+08] Holger Bock, Michael Braun, Markus Dichtl, Erwin Hess, Johann Heyszl, Walter Kargl, Helmut Koroschetz, Bernd Meyer and Hermann Seuschek. A milestone towards rfid products offering asymmetric authentication based on elliptic curve cryptography. In Workshop on RFID Security, 2008

References II

[LSBV08] Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, and Ingrid Verbauwhede. A compact ECC processor for pervasive computing. *Presentation at Secure Component and System Identification (SECSI)*, 2008

[LV07] Yong Ki Lee, Ingrid Verbauwhede. A compact architecture for Montgomery elliptic curve scalar multiplication processor. *In Proc. International Workshop on Information Security Applications (WISA)*, 2007.

[KP06] S.Kumar and C. Paar. Are standards compliant elliptic curve cryptosystems feasible on RFID? *Printed handout of Workshop on RFID Security (RFIDSec06)*, 2006

[Wol05] Johannes Wolkerstorfer. Is elliptic-curve cryptography suitable to to secure RFID tags? *In Workshop on RFID and Lightweight Crypto*, 2005

References III

[FW07] F. Fürbaß, and J. Wolkerstorfer. ECC processor with low die size for RFID applications. *In Proc. IEEE International Symposium on Circuits and Systems ISCAS 2007,* pages 1835–1838, 2007.

[OScE04] E. Öztürk, B. Sunar, and Savaç, E. Low-power elliptic curve cryptography using scaled modular arithmetic. In Cryptographic Hardware and Embedded System (CHES), 2004