Institute for Applied Information Processing and Communications

Graz University of Technology

Dual-Field Arithmetic Unit for GF(p) and GF(2^m) *

CHES 2002

Workshop on Cryptographic Hardware and Embedded Systems

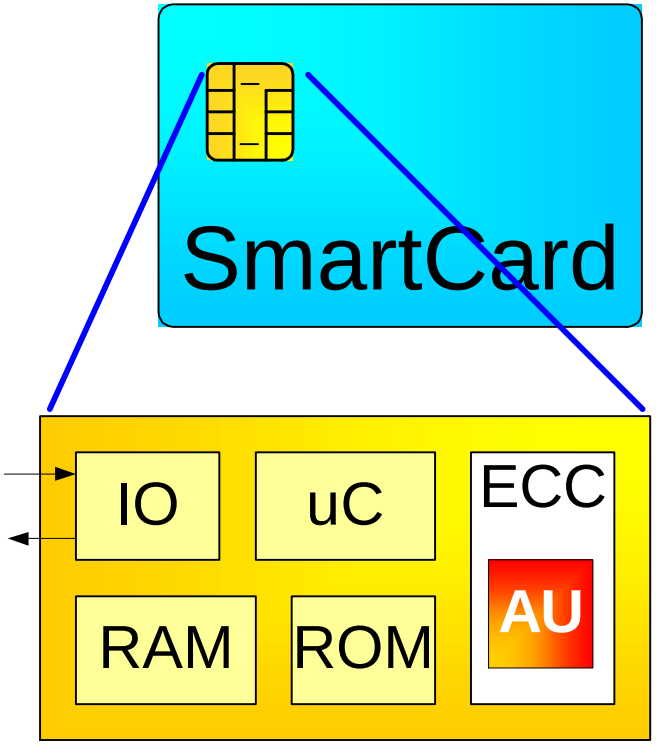
August 2002, Redwood Shores, CA.

*** This work origins from the European Commission funded project USB_CRYPT established under contract IST-2000-25169 in the Information Society Technology (IST) Program**

IAIK TUG

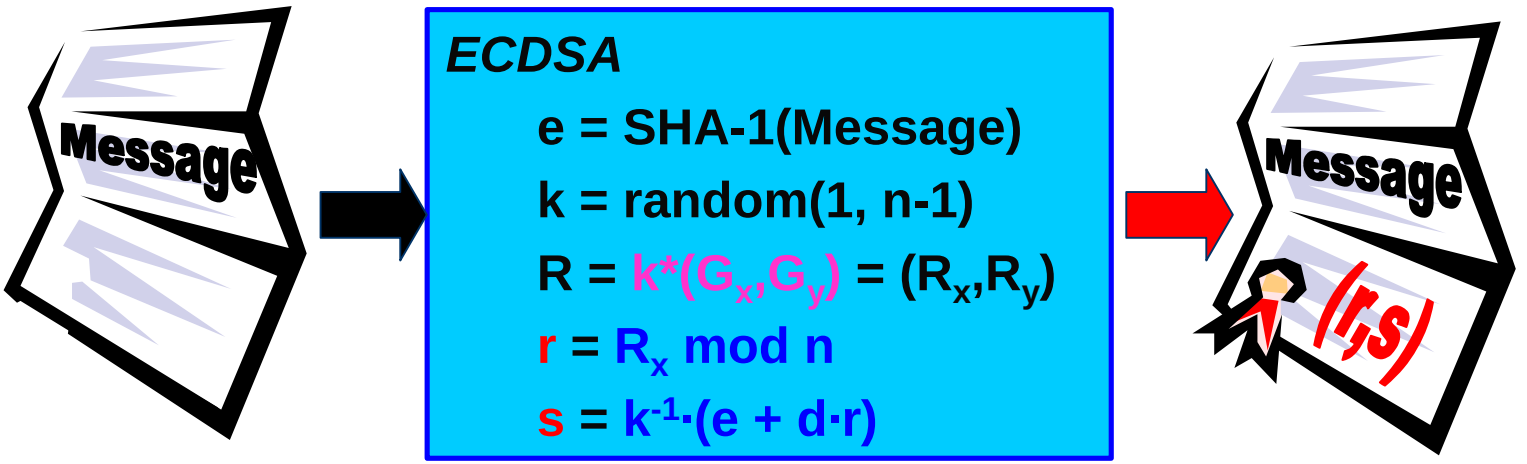
Motivation

- **Coprocessor**
  - For smartcards
- **Application**
  - ECDSA
- **Aims**
  - Small size
  - Low power
  - Medium throughput



IAIK TUG

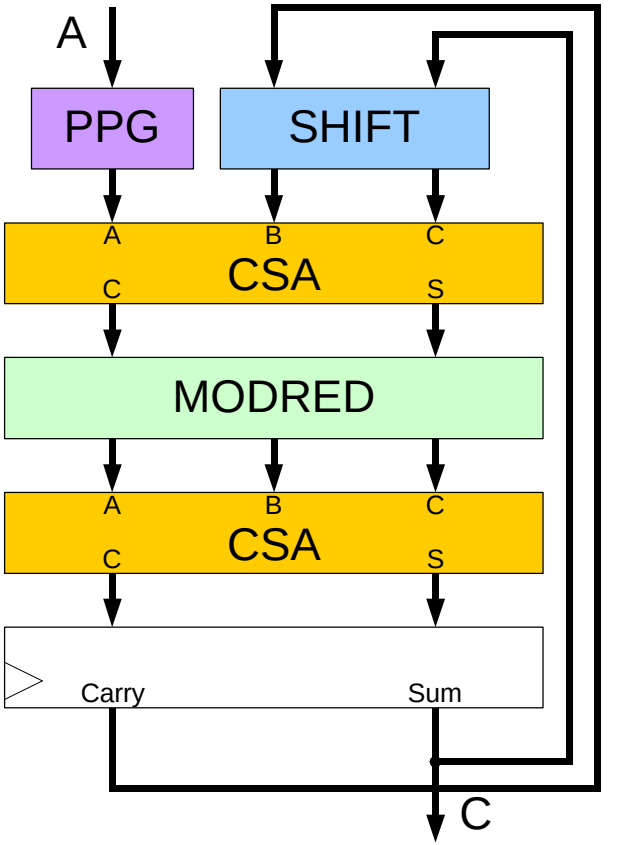
Motivation
EC signature over GF(2^m)



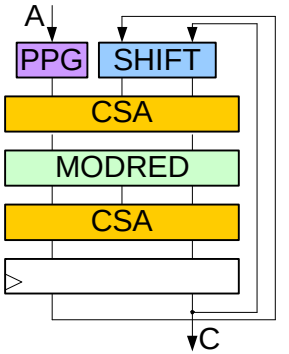
- **ECDSA**
  - Elliptic-Curve Digital-Signature Algorithm
  - Operations in GF(p) and GF(2^m)
    - Addition, Multiplication, Inversion, Comparison

Proposed architecture

- **PPG**
  - Partial product generator
- **SHIFT**
  - Shift unit
- **CSA**
  - Carry-save adder
- **MODRED**
  - Modular reduction unit

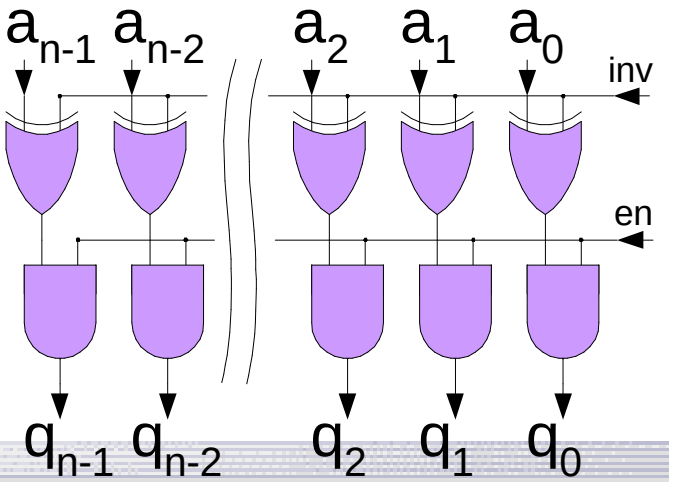


PPG - Partial product generator

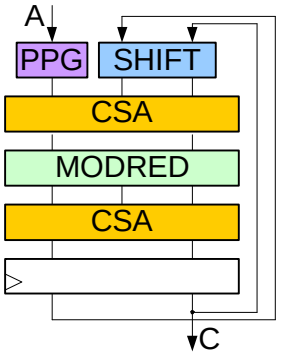


- **Generates**
  - Partial products $A \cdot b_i$ for multiplication
  - Negative numbers for subtraction

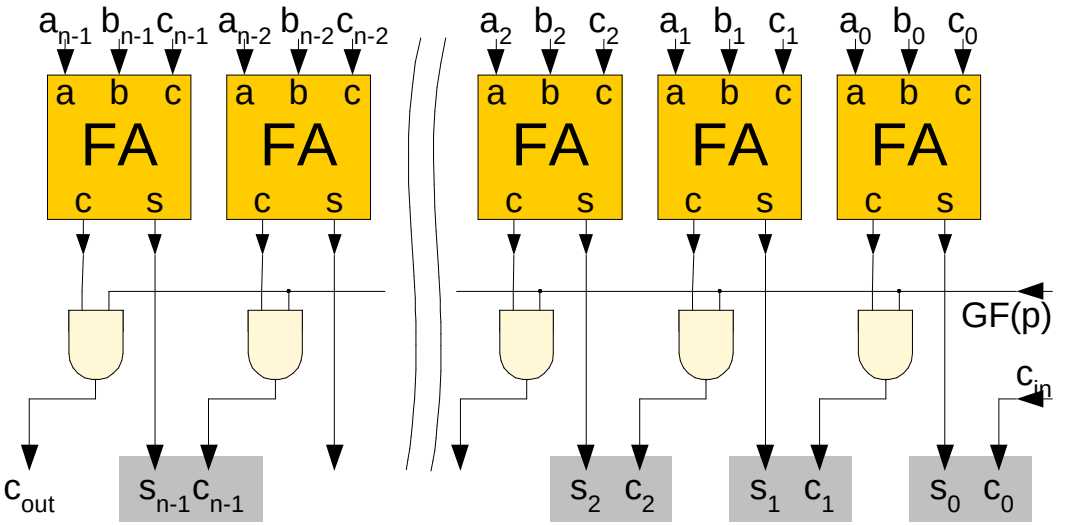
Inv	*En*	*Q*
x	0	0
0	1	A
1	1	-A-1



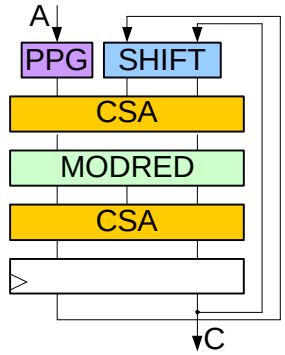
CSA
Carry-save adder



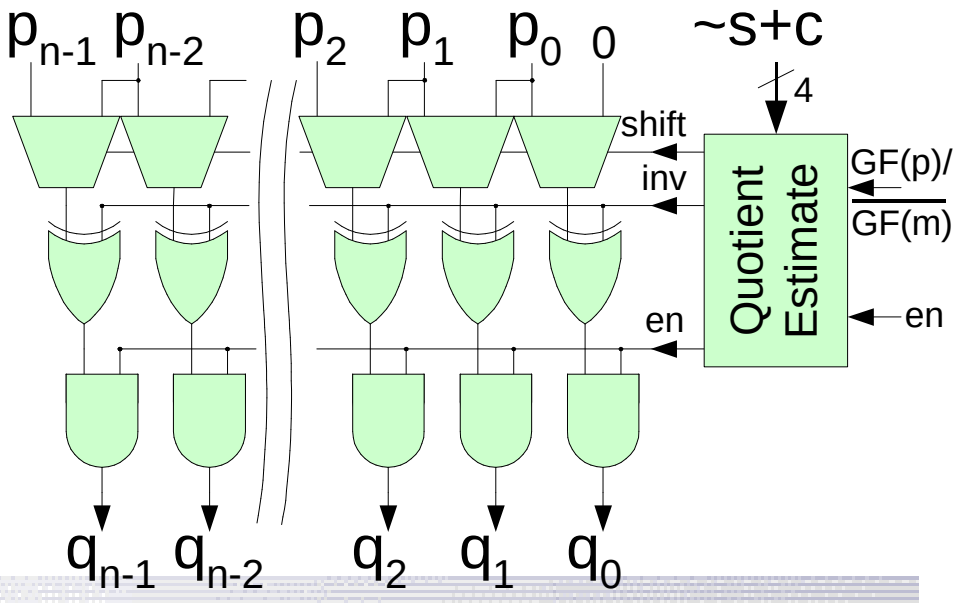
- **Fast addition**
  - Independent of wordsize *n*
- **GF(2^m)**
  - A xor B = CSA(A,B,0)



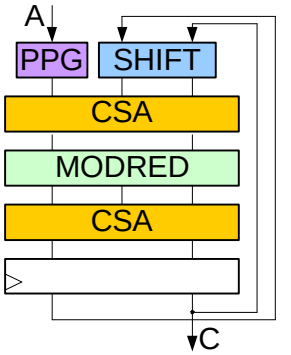
MODRED – modular reduction unit



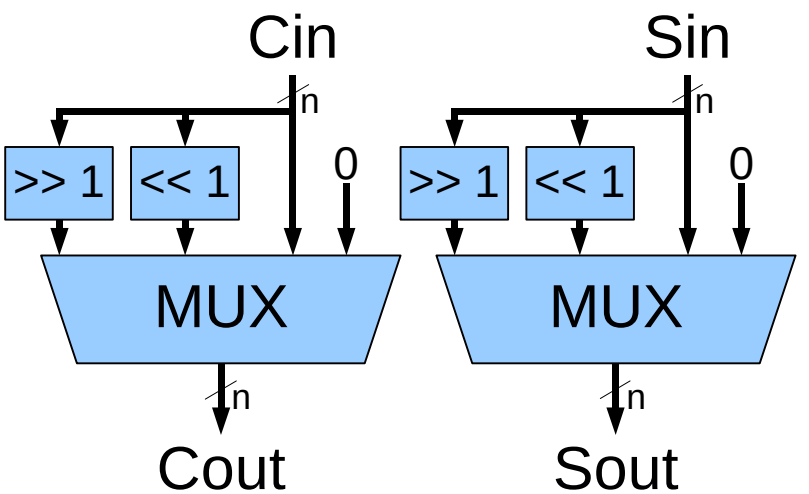
- **Limits intermediate results to *n+2* bit**
- **GF(p)**
  - Quotient estimated
  - q in {-2, -1, 0, 1, 2}
- **GF(2^m)**
  - Exact quotient
  - q in {0, 1}
- **Q = q·P**
- **Similar to PPG**



SHIFT
Feedback selector

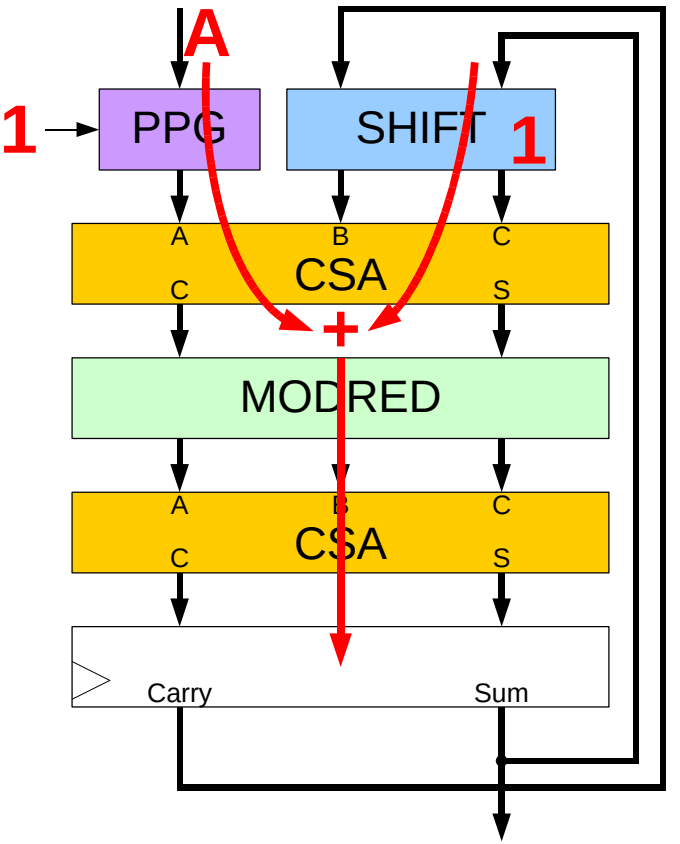


- **Selects feedback**
  - (Cout, Sout) =
    - (0, 0)
    - (Cin, Sin)
    - (Cin shl 1, Sin shl 1)
    - (Cin shr 1, Sin shr 1)



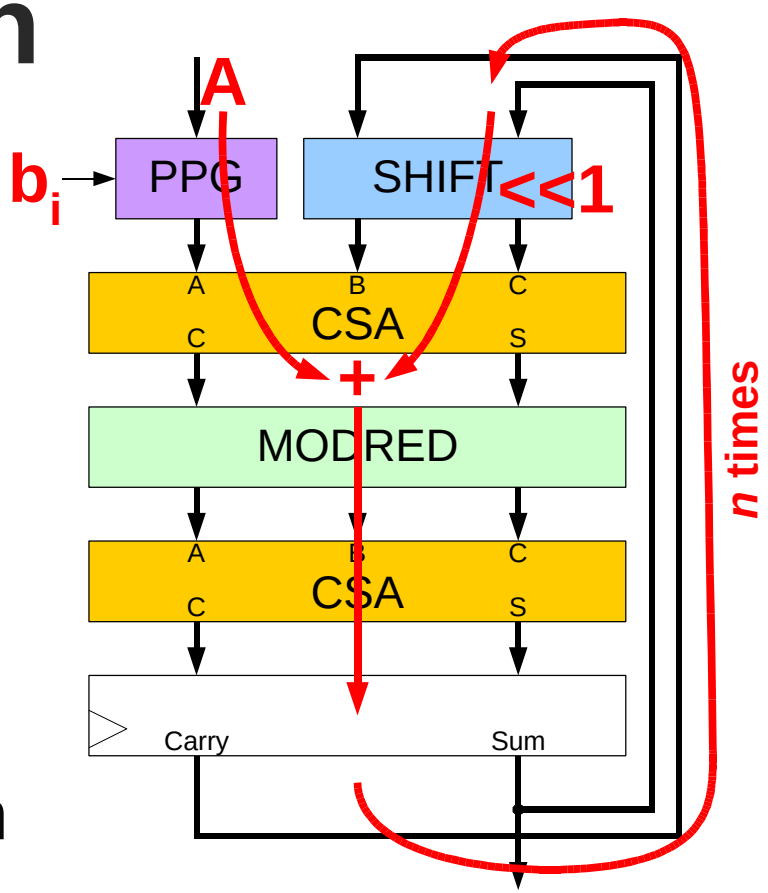
Operations Addition

- **Input A added to last result**
- **GF(p)**
  - CSA: Full-adder
- **GF(2^m)**
  - CSA: XOR-gate



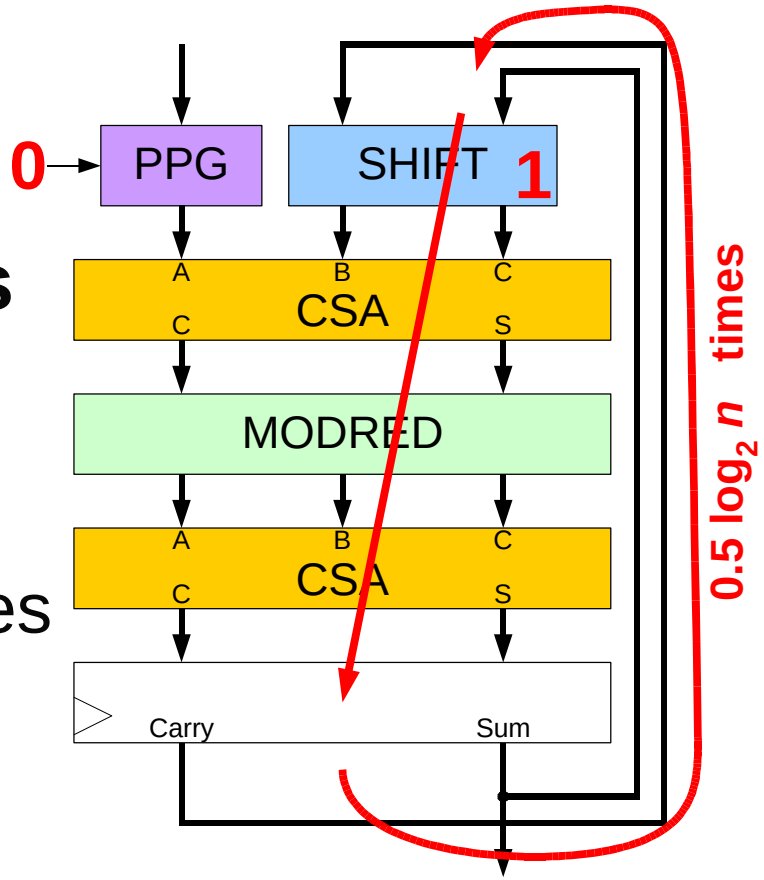
Operations Multiplication

- **Bitserial Multipl.**
  - Double & Add
  - *n* clock cycles
  - Interleaved modular reduction
- **Squaring**
  - Done by multiplication



Operations – Redundant to binary

- **Conversion of redundant numbers**
  - Into binary numbers
- **Hold operation**
  - CSAs eliminate carries
    - Approx. 4 cycles for 256-bit architecture



IAIK TUG

Operations
Inverse

- **Multiplicative inverse**
  - $a \cdot a^{-1} = 1 \bmod p$ in GF(p)
  - $A(x) \cdot A^{-1}(x) = 1 \bmod P(x)$ in GF(2^m)
- **Using Extended Euclidean Algorithm**
  - Compound multi-cycle operation
    - GF(p): Shift right, Subtraction, Comparison
    - GF(2m): Shift right, Addition, Comparison

IAIK TUG

Operations Summary

- **GF(p)**
  - Addition
  - Subtraction
  - Incrementation
  - Multiplication
  - Shift left
  - Shift right
- **Comparison**
  - Less than 0
- **GF(2^m)**
  - Addition / Subtraction
  - Multiplication
  - Times x
  - Div x
- **Integer**
  - Addition
  - Subtraction
  - Incrementation
  - Multiplication
- **Others**
  - Clear / Load 0
  - Load A
  - Load !A
  - Load -A
  - Hold
  - XOR
- **Compound**
  - Inversion
    - in GF(p)
    - in GF(2m)

IAIK TUG

Results Performance

- GF(p) performance

Bit-length	*MUL [cycles]*	*INV [cycles]*	*ECC pr. [cycles]*
192-bit	192	14.0k	720k
224-bit	224	16.5k	900k
256-bit	256	19.4k	1,150k

- GF(2^m) performance

Bit-length	*MUL [cycles]*	*INV [cycles]*	*ECC pr. [cycles]*
163-bit	163	11.0k	490k
233-bit	233	16.2k	905k
283-bit	283	20.7k	1,405k

IAIK TUG

Results
Circuit complexity

- **Number of gates**
- **Estimated die size**

Bit-length	*AND*	*XOR*	*MUX2*	*MUX4*	*FA*	*REG*	*Area on 0,35 µm CMOS process*
163-bit	660	330	165	330	330	660	0.57 mm²
224-bit	904	452	226	452	452	904	0.78 mm²
283-bit	1140	570	285	570	570	1140	0.99 mm²
n-bit	4*n*+8	2*n*+4	*n*+2	2*n*+4	2*n*+4	4*n*+8	

Conclusion

- **Dual-field arithmetic unit**
  - For GF(p) and GF(2^m)
  - Processing at full precision
  - Scaleable
    - CSAs prevent carry-propagation
  - Signed number representation
  - Short critical path
  - Regular (simple) structure
  - Low gate count
    - Only a little bit larger than a mere GF(p)-multiplier