

Small-footprint ALU for public-key processors for pervasive security

K. Sakiyama, L. Batina, N. Mentens,
B. Preneel and I. Verbauwhede

Katholieke Universiteit Leuven
ESAT-SCD/COSIC

RFID security 06
Graz, Austria
July 12-14, 2006

Outline



- Introduction and Motivation
- Curve-based Cryptography (ECC/HECC)
- MALU
- Results: area, power, performance
- Conclusions
- Future work



Motivation

- Emerging new applications: wireless applications, sensor networks, RFIDs, car immobilizers, key chains...
 - resource limited: area, memory, power, bandwidth
 - low-cost, low-power, low-energy
- Pure hardware solutions are cost effective
- PKC allows for strong authentication

Introduction



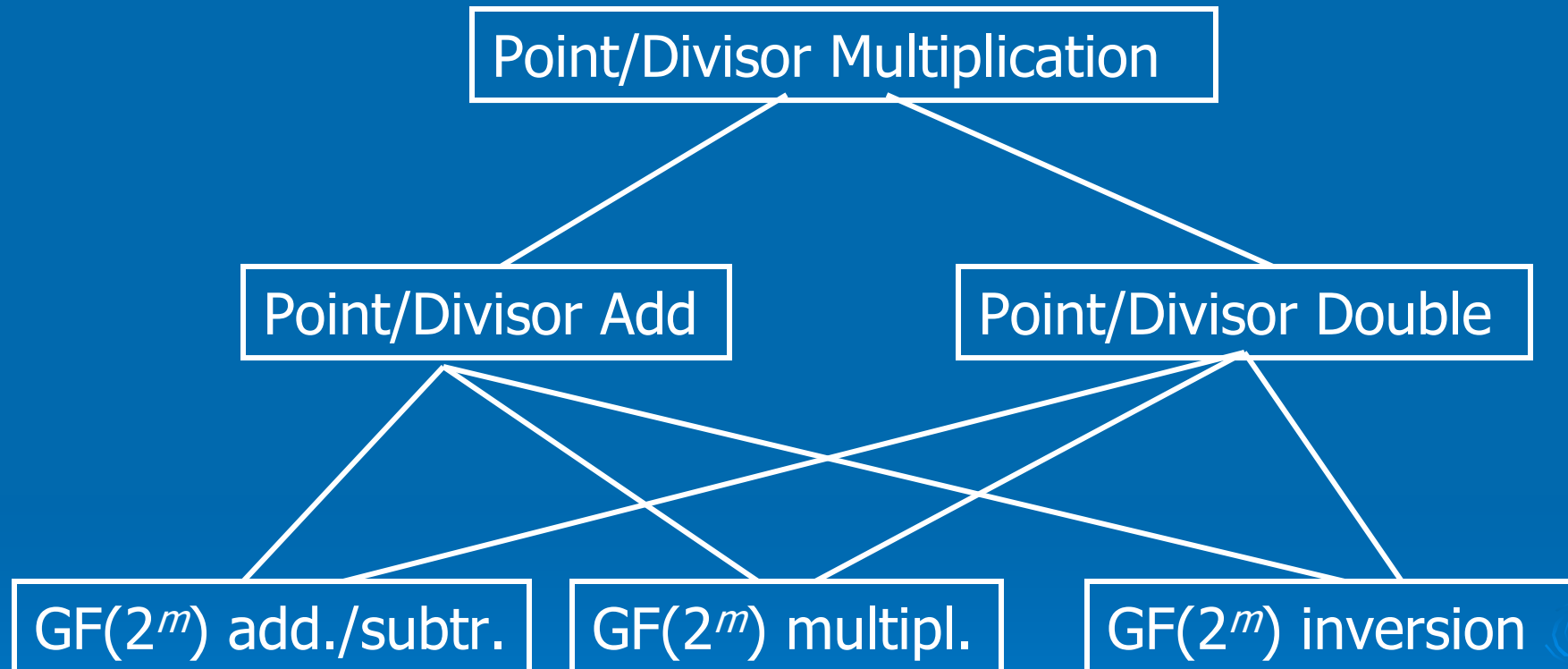
- Curve-based crypto vs. RSA:
 - (H)ECC offers shorter certificates, lower power consumption, more “security per bit”
 - More compact solutions, suitable for wireless applications
- Side-channel resistance

ECC/HECC over binary fields



- ECC is around for twenty years
- Only recently work on compact and low-power implementations
- EC is a special case of HEC (genus $g=1$)
- HECC allows one to work in even smaller field (80 bits for curves with $g=2$)

(H)ECC hierarchy

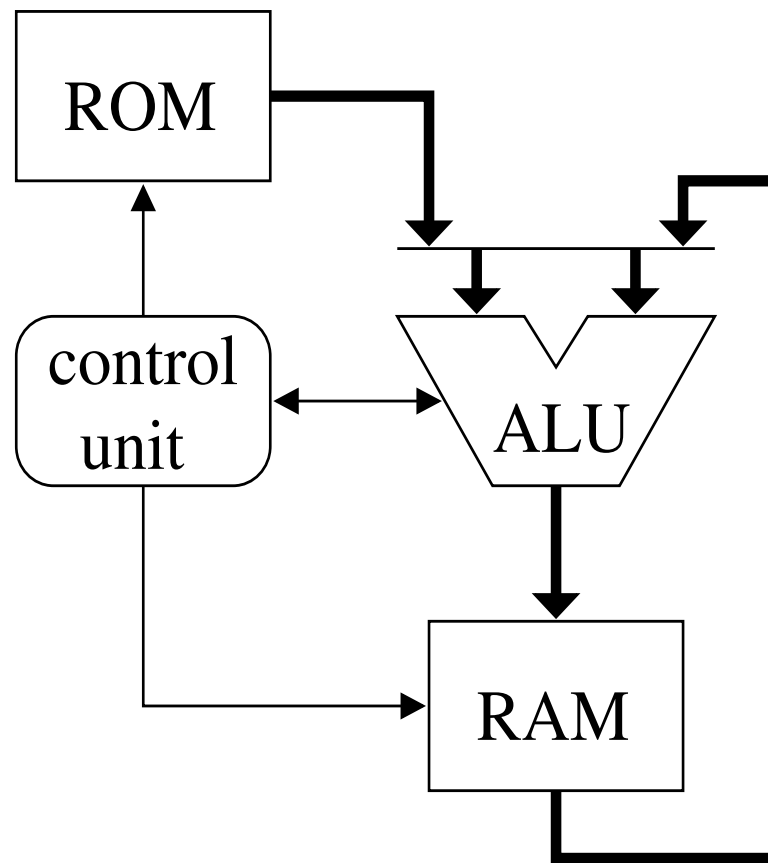


Low-power design



- Architectural decisions are important
- Frequency as low as possible
- Power consumption and energy efficiency are both crucial
- ECC arithmetic should be revisited to optimize those parameters
- The circuit size should be minimized
- Flexibility can be sacrificed

(H)ECC processor

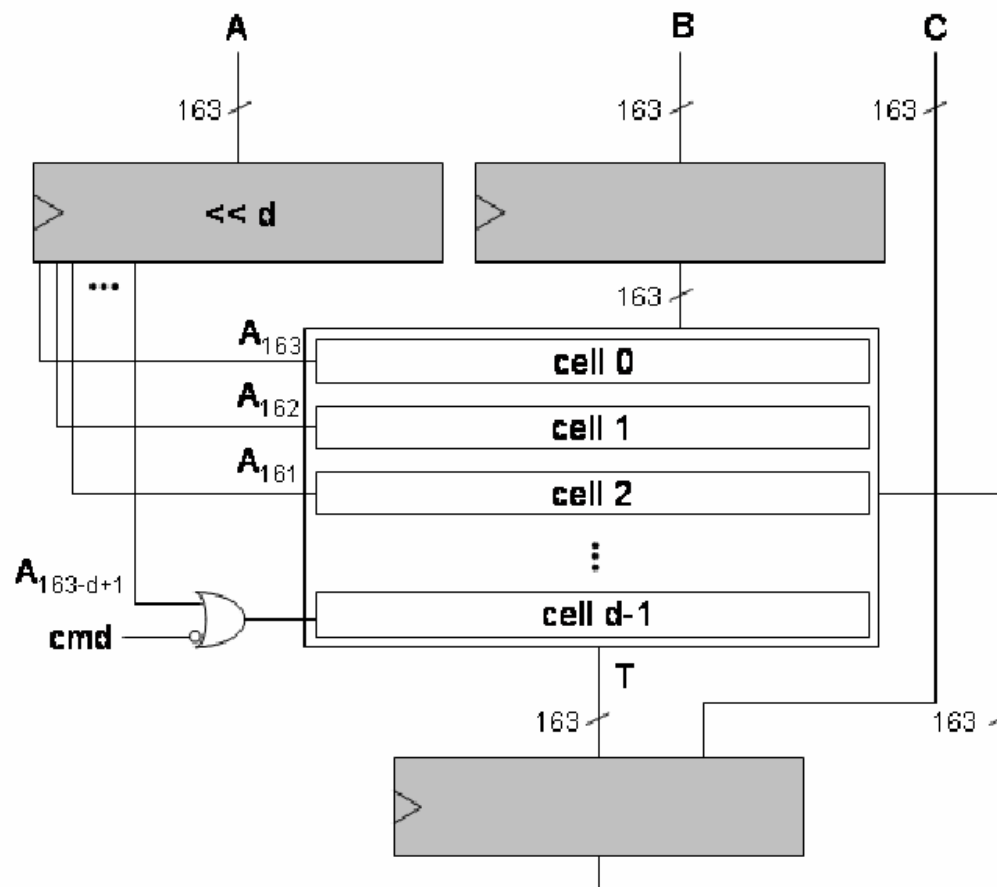


New compact MALU

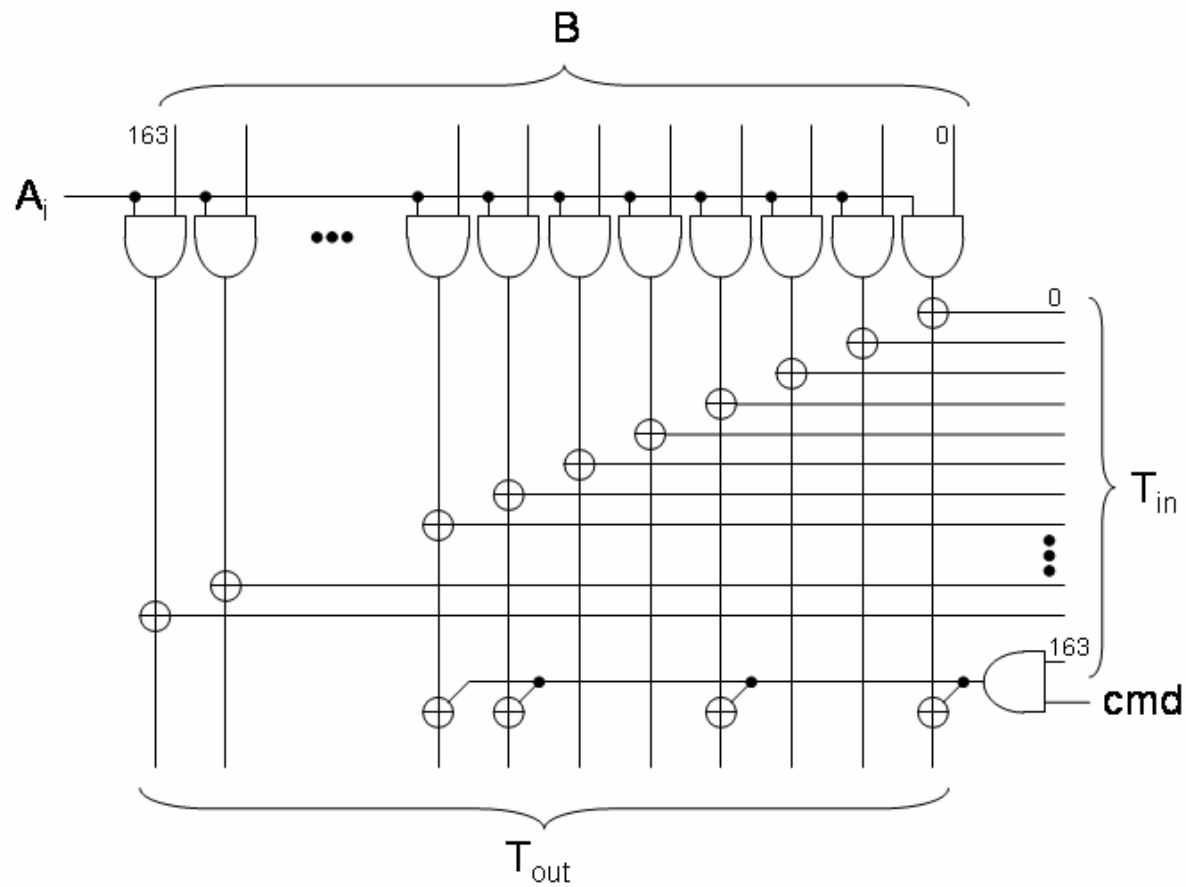


- Implements bit/digit serial modular multiplication and addition in a binary field
- Fixed irreducible polynomial
- Suitable for ECC and HECC
- Resource sharing of both modular operations required
- No separate squaring unit => simple side-channel resistance

Schematic of the MALU



Cell in MALU

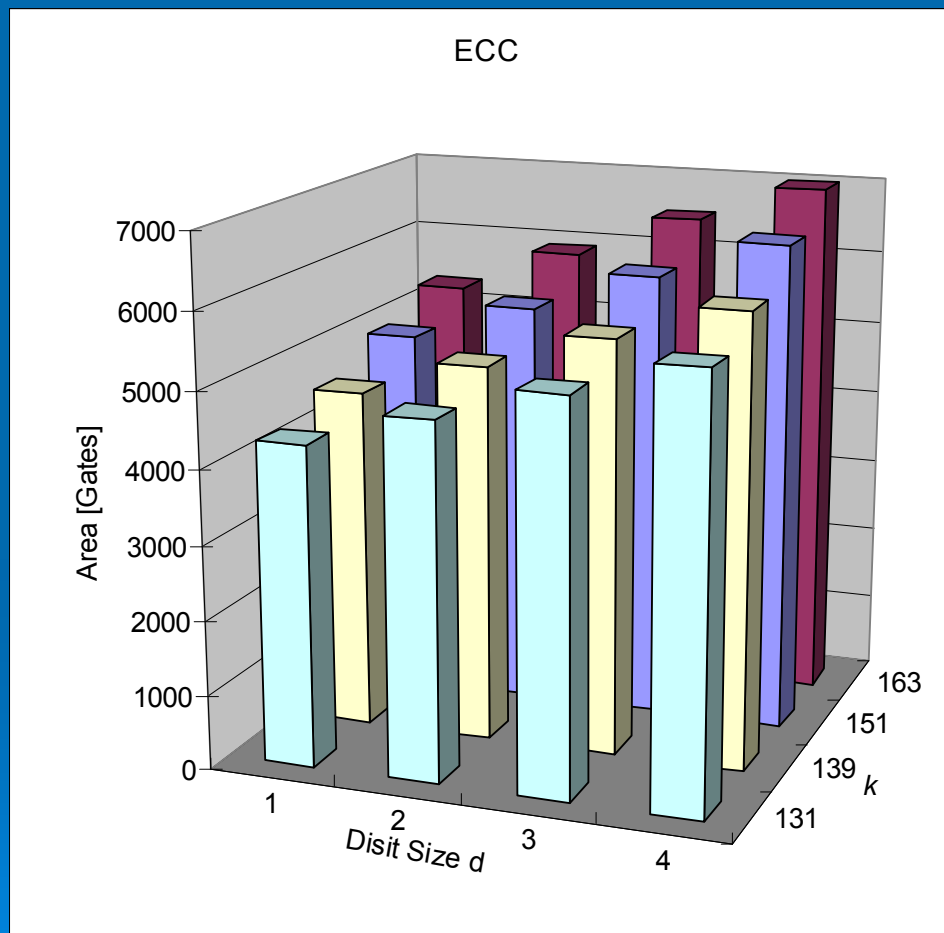


Results for area: MALU



Field size	$d=1$	$d=2$	$d=3$	$d=4$
131	4281	4758	5219	5685
139	4549	5043	5535	6028
151	4955	5472	6016	6540
163	5314	5900	6486	7052

Area of MALU for ECC over $GF(2^{163})$



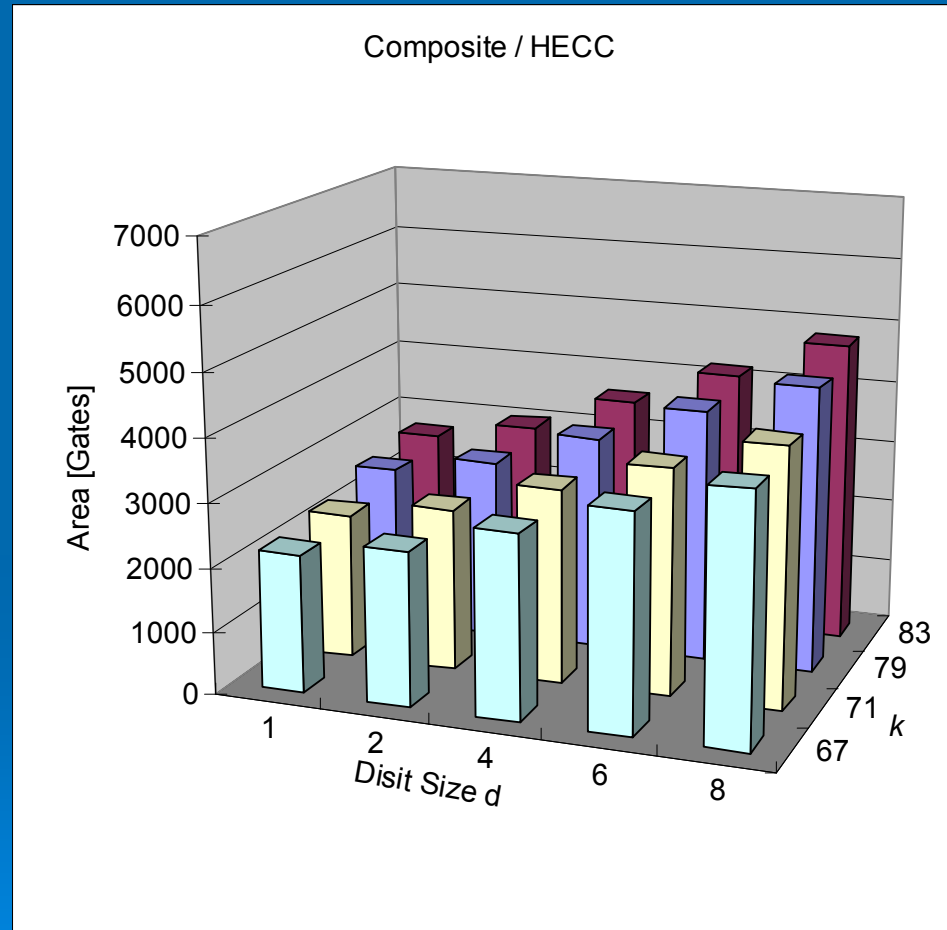


Results for area: MALU + control

Field size	$d=1$	$d=2$	$d=3$	$d=4$
131	6612	7079	7539	8005
139	7256	7650	7855	8348
151	7662	8173	8336	8860
163	8021	8601	9174	9738

Total area: RAM for storage of $5n$ bits should be added

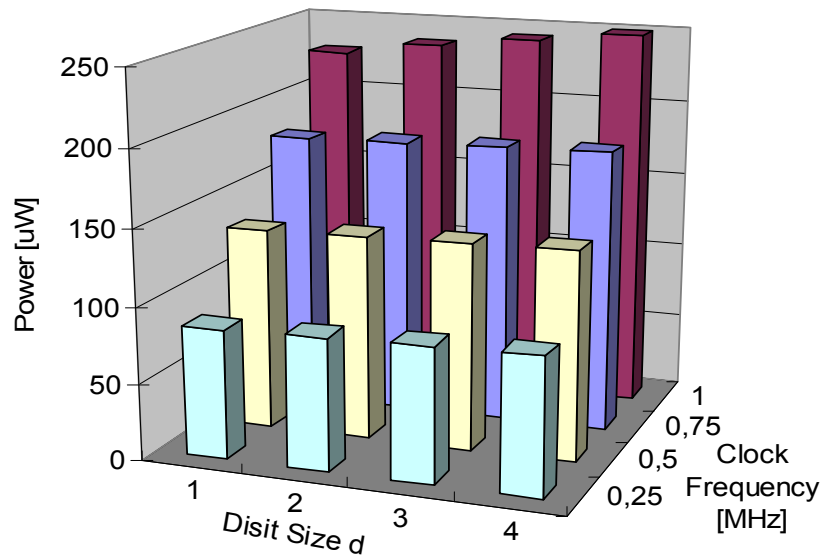
Area of MALU for HECC and ECC over composite fields



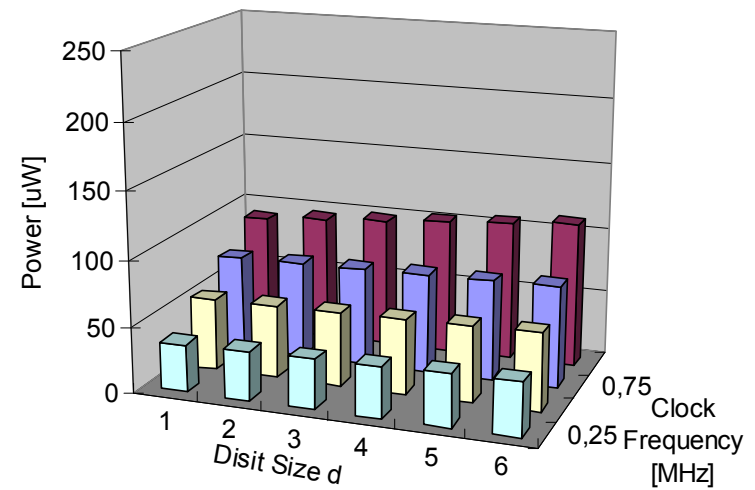
Results: Power consumed by MALU



GF(2¹⁶³)



COMPOSITE



Results: performance



Estimated performance for 1 point multiplication @ 175 kHz:

$t = 543$ ms in $GF(2^{163})$

$t = 576$ ms in $GF(2^{131})$

Conclusions and future work



- The presented MALU is the smallest possible solution for curve-based cryptography
- Our result is the most compact ECC solution so far
- HECC is work in progress
- Better power estimates regarding RAM and synthesis in 0.13 (0.18) μm library are required