



HAL
open science

Hardware and Arithmetic for Hyperelliptic Curves Cryptography

Gabriel Gallin, Arnaud Tisserand, Nicolas Veyrat-Charvillon

► **To cite this version:**

Gabriel Gallin, Arnaud Tisserand, Nicolas Veyrat-Charvillon. Hardware and Arithmetic for Hyperelliptic Curves Cryptography. RAIM: 7ème Rencontre Arithmétique de l'Informatique Mathématique, Apr 2015, Rennes, France. , 2015. hal-01134020

HAL Id: hal-01134020

<https://inria.hal.science/hal-01134020v1>

Submitted on 29 Mar 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

1. Elliptic Curve Cryptography (ECC)

protocol level

encryption, signature, key gen., etc.

$E : y^2 = x^3 + 4x + 20$ over $GF(1009)$
 Points on E : $P, Q = (x, y)$ or (x, y, z)
 Coordinates: $x, y, z \in GF(\cdot)$
 $GF(p), GF(2^m), t : 160-600$ bits
 $k = (k_{t-1}k_{t-2} \dots k_1k_0)_2 \in \mathbb{N}$

curve level

Scalar multiplication operation
 for i from 0 to $t-1$ do
 if $k_i = 1$ then $Q = \text{ADD}(P, Q)$
 $P = \text{DBL}(P)$

field level

Point addition/doubling operations
 sequence of finite field operations
 DBL: $V_1 = Z_1^2, V_2 = X_1 - V_1, \dots$
 ADD: $W_1 = Z_1^2, W_2 = Z_1 \times W_1, \dots$

$GF(p)$ or $GF(2^m)$ operations
 operation modulo large prime ($GF(p)$)
 or irreducible polynomial ($GF(2^m)$)

2. Side Channel Attacks (SCAs)

Side channels:

- Power consumption
- Electromagnetic radiation
- Computation timings

Attacks:

- Simple analysis
- Differential analysis (statistics)
- Templates and learning

3. Protections & Counter-Measures Against SCAs

- Uniform comp. durations
- Uniform power/EM profile
- Random behavior
- Circuit reconfiguration
- detection/correction codes
- Add noise (!)

Example: use redundant number systems

Random recoding: $\forall i \quad [R_i(k)]P = [k]P$

4. From ECC to HECC

	field size	ADD	DBL
ECC	ℓ bits	Cost: 12M + 2S	Cost: 6M + 5S
HECC	$\frac{\ell}{2}$ bits	Cost: 47M + 4S	Cost: 38M + 6S

Examples of computation expressions for projective coordinates

5. HAH Project Objectives

- Efficient algorithms and representations for HECC
- HECC protections against SCAs (passive and active)
- Fast, low-power and secure hardware implementations (open source hardware code and programming tools)
- Intensive security evaluation using our SCA setup

6. Developed Crypto-Processor(s) from PAVOIS ANR Project

- Arithmetic Units (AUs): \pm, \times, \div over $GF(p)/GF(2^m)$
 various configurations (area vs speed, internal protection)
- Various key recoding methods (and dedicated units)
- Configuration: field size, internal word size, #AUs, type(AUs)
- Circuit/architecture level protections

7. Programming Tools for Our Crypto-Processor(s)

HW modules, crypto. lib., compiler, Sage, user, assembler, API/TLS-SSL, CAD tools, implementation, binary code, commands.

8. Implementation Results on FPGA

XC6SLX75 FPGA, $GF(p)$, 256-bit ECC or 128-bit HECC, internal word size $w = 32$ bits

Recoding units:

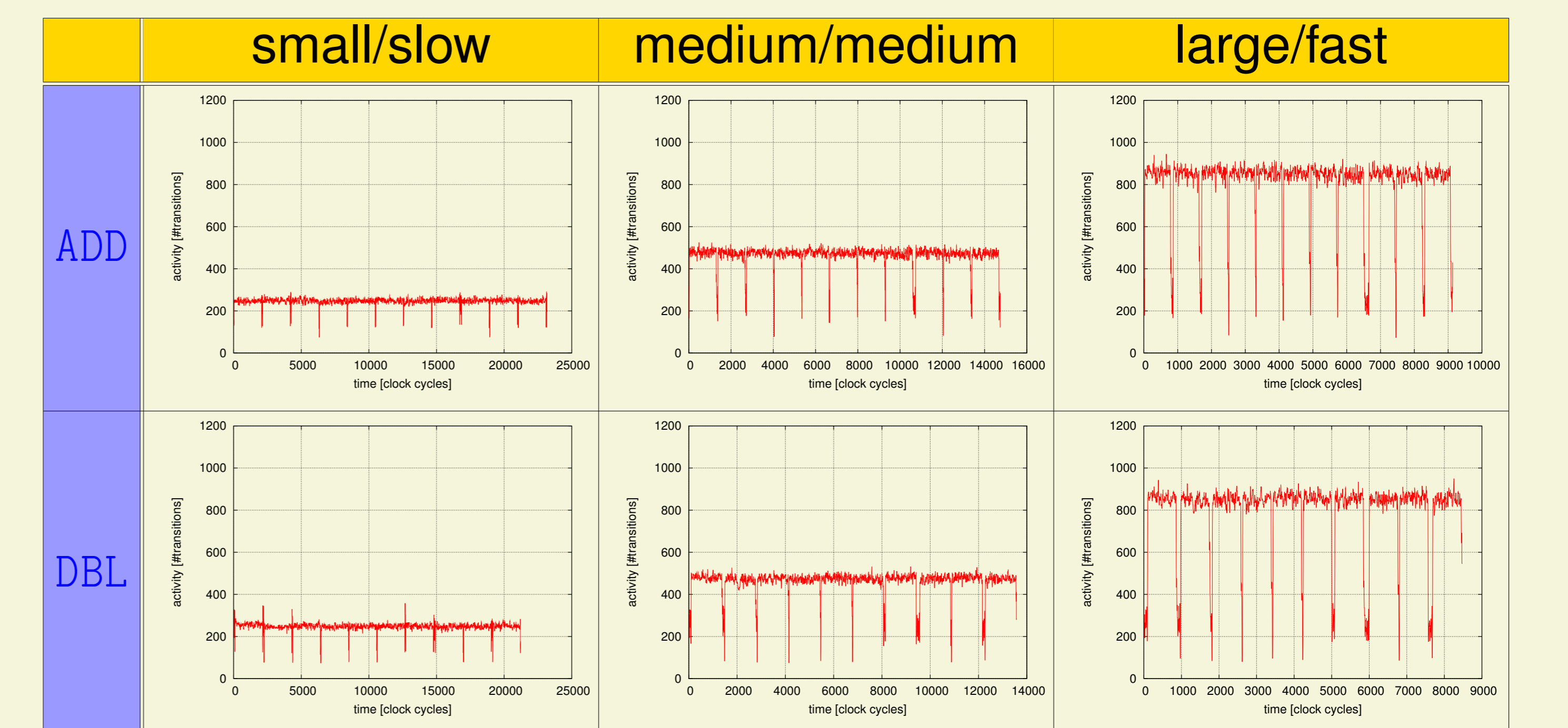
Recoding	BIN	NAF-2	NAF-3	NAF-4
area slices (FF/LUT)	565 (1321/1461)	570 (1340/1479)	571 (1344/1495)	503 (1348/1489)
freq. (MHz)	225	228	237	217

Area/speed trade-offs for ECC and HECC configurations:

	#mult.	BRAM	mult. 1 col.		mult. 2 col.		mult. 4 col.	
ECC	1	2	503 (1348/1489)	217	626 (1450/1643)	230	694 (1649/1891)	211
	2	2	689 (1744/1894)	219	754 (1948/2208)	234	931 (2345/2712)	220
	3	2	809 (2146/2245)	205	942 (2449/2704)	222	1105 (3046/3436)	222
HECC	1	2	522 (1344/1405)	228	520 (1434/1535)	217		
	2	2	634 (1746/1786)	226	689 (1926/2055)	220	area	freq.
	4	2	852 (2552/2531)	201	917 (2912/3045)	195	slices (FF/LUT)	MHz
	8	2	1347 (4145/3882)	204	1601 (4865/4928)	209		

9. Algorithms and Architecture Impacts on SCAs

Activity traces from CABA¹ simulations (after filtering) for several configurations of the field multiplier (area/speed)



¹ Cycle Accurate Bit Accurate (i.e. simulations close to real power measurements)