BINARY EDWARDS CURVES FOR INTRINSICALLY SECURE ECC IMPLEMENTATION FOR THE IOT

Séminaire SoSySec | Antoine Loiseau | 07/09/2018

TABLE OF CONTENTS

OUR APPROACH

- **Goal : build a elliptic curves based system for a 32-bits RISC V architecture**

- **RISC V :**
  - Open source instruction set architecture (University of California)
    - 32 bits architecture
  - Modular architecture with extended instructions
    - Specific instructions available for future optimizations
  - No carry flag

- **ECC for IoT :**
  - FIPS 186-4 (NIST)
    - Old : upgrades available on the arithmetic and security
  - Edwards curve : Ed25519
    - Prime field : carry propagation

ELLIPTIC CURVES IN CRYPTOGRAPHY

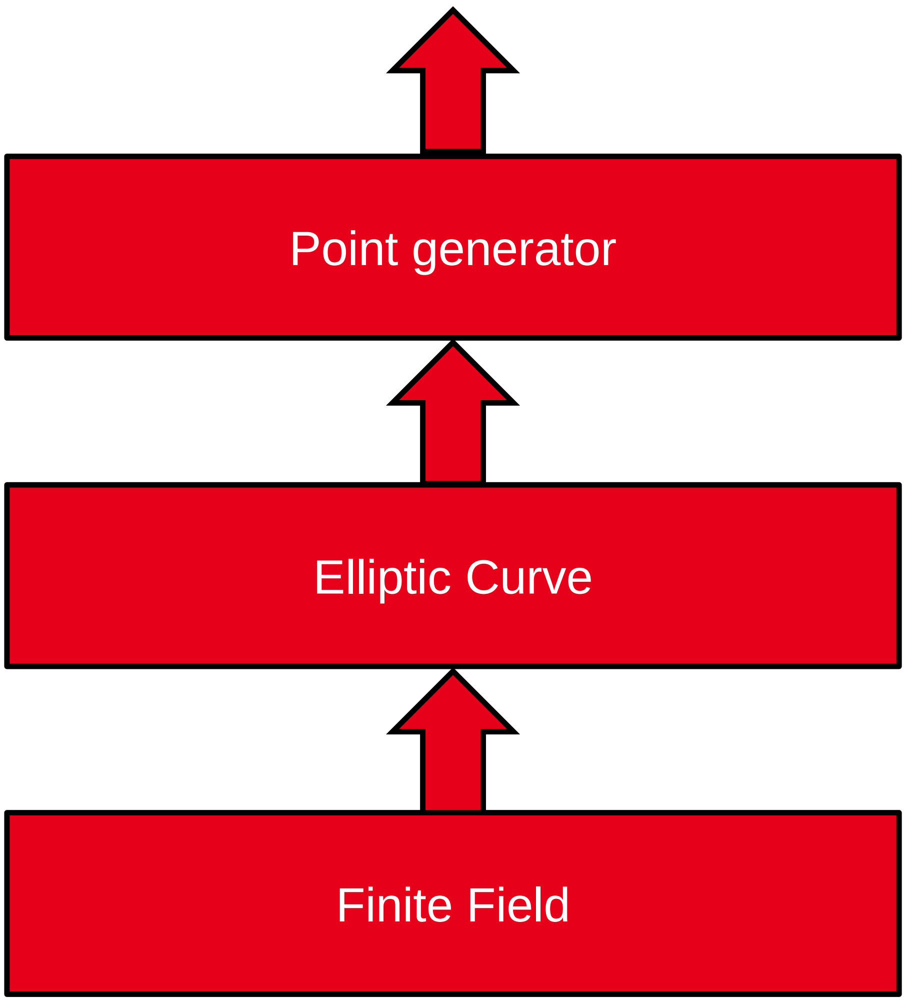
- **NIST standards**
  - Define a set of elliptic curves over prime and binary fields
  - Define a digital signature based on ECC : ECDSA
  - Define a key exchange method on ECC : ECDH

- **Other standardizations :**
  - Brainpool curves
  - Edwards curves (Ed25519)

- **ECC systems are based on the difficulty of the Discrete Logarithm Problem on the group of a elliptic curve.**
  - Let G and P points of the group of the elliptic curve such as $P = kG$. It is hard to find k from G and P.
  - Usually P is called public key, k is called private key and G is called the generator of the group.

HOW TO GENERATE NEW ELLIPTIC CURVES ?

Cryptographic Protocols : ECDSA, ECDH…



- Random point
- Optimized point

- Elliptic curve model
- Parameters
- Point representation

- Prime or binary fields
- Representation
- Modulus

HOW TO GENERATE NEW ELLIPTIC CURVES ?

Cryptographic Protocols : ECDSA, ECDH…

↑

Optimized point

- Random point
- Optimized point

↑

Binary Edwards Curves

- Elliptic curve model
- Parameters
- Point representation

↑

Binary Fields

- Prime or binary field
- Representation
- Modulus

MODULUS FOR BINARY FIELDS

- **NIST recommendations :**
  - Trinomials : $p(x) = x^m + x^a + 1,\ m > a > 0$
  - Pentanomials : $p(x) = x^m + x^a + x^b + x^c + 1,\ m > a > b > c > 0$
  - With small a, b and c

- **Scott's polynomials**
  - Lucky trinomials : $m - a \ \equiv 0\ [w]$
  - Lucky pentanomials : $m - a \ \equiv 0[w], m - b \equiv 0[w]$ and $m - c \equiv 0[w]$
  - w is the width of the targeted architecture (32 bits, 64 bits…)

- **Selection of Scott's polynomials of degree from 256 to 512 to address security level from 128 to 256 bits**

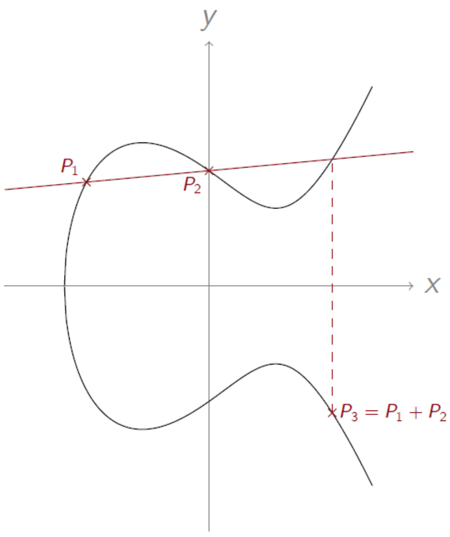
- **Security requirements : m shall be prime to avoid GHS attack**

NEW ELLIPTIC CURVES

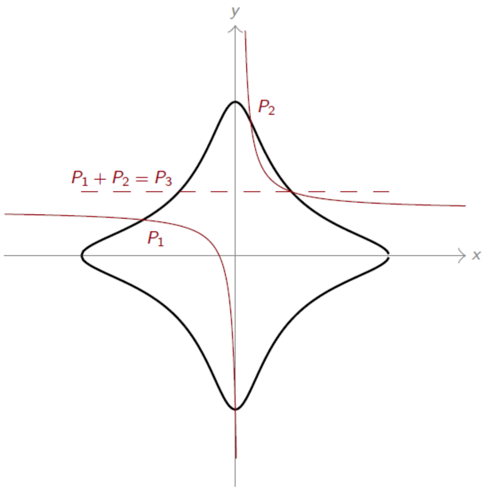
Secu.	Name	Modulus	Parameter d	Generator
112	BEC223	$x^{223} + x^{159} + 1$		
128	BEC257	$x^{257} + x^{65} + 1$		
156	BEC313	$x^{313} + x^{121} + 1$		
215	BEC431	$x^{431} + x^{303} + x^{239} + x^{111} + 1$		
239	BEC479	$x^{479} + x^{255} + 1$		
243	BEC487	$x^{487} + x^{295} + x^{167} + x^{39} + 1$		
260	BEC521	$x^{521} + x^{489} + 1$		
284	BEC569	$x^{569} + x^{441} + x^{313} + x^{121} + 1$		

ELLIPTIC CURVES

- **Weierstrass curves**
  - Prime fields : $y^2 = x^3 + ax + b$
  - Binary fields : $y^2 + xy = x^3 + ax^2 + b$
  - Neutral element : Infinite point



- **Edwards curves**
  - Prime fields : $x^2 + y^2 = 1 + dx^2y^2$
  - Neutral element : $(1, 0)$
  - Complete group law



BINARY EDWARDS CURVES (BEC)

- **Definition :**
  - Let d a element of $GF(2^m)$ with a trace different from 0, the BEC of parameter d is given by :

$$d(x+y+x^2+y^2) = xy + xy(x+y)x^2y^2$$

- **Properties :**
  - Neutral element : $(0,0)$
  - $\forall P \in E\big(GF(2^m)\big), P = (x,y) \rightarrow -P = (y,x)$
  - $P + (1,1) = (x,\ y) + (1,1) = (x+1, y+1)$
  - $d(X+Y)Z^3 + d(X^2+Y^2)Z^2 = XYZ^2 + XY(X+Y) + X^2Y^2$
  - Complete group law
  - Birational equivalent to a Weierstrass curve :

$$v^2 + uv = u^3 + (d^2+d)u^2 + d^8$$

ARITHMETIC ON BEC

- ***w*-differential coordinate :**
  - Let $P = (x, y) \rightarrow w(P) = x + y$
  - We can compute $w(2P)$ and $w(P+Q)$ with $w(P), w(Q)$ and $w(P-Q)$
  - Useful with the Montgomery Ladder algorithm to compute kP
  - We represent $w(P)$ as $\frac{W_P}{Z}$ and $w(Q)$ as $\frac{W_Q}{Z}$
  - 5 multiplications, 4 squares, 1 multiplication by d

Algorithm 2 w-coordinates Adding and Doubling re-visited with the Co-Z trick.

Require: $W_2, W_3, Z, \frac{1}{w_1}$

$C \leftarrow (W_2 + W_3)^2$
$D \leftarrow Z^2$
$E \leftarrow \frac{1}{w_1} C$
$U \leftarrow E + C$
$V \leftarrow E + D$
$S \leftarrow (W_2(Z + W_2))^2$
$T \leftarrow S + dD^2$
$W_4 \leftarrow UT$
$W_5 \leftarrow VS$
$Z' \leftarrow VT$
return W_4, W_5, Z'

Algorithm 3 Montgomery Ladder

Require: $w(P), k = (k_{t-1}, \ldots, k_0)_2$

$R_0 \leftarrow O$
$R_1 \leftarrow P$
for $j = t-1$ **to** 0 **do**
  if $k_j = 0$ **then**
    $R_1 \leftarrow R_0 + R_1$
    $R_0 \leftarrow 2R_0$
  else
    $R_0 \leftarrow R_0 + R_1$
    $R_1 \leftarrow 2R_1$
  end if
end for
return $R_0 = w(kP), R_1 = w(kP + P)$

SECURITY REQUIREMENTS

- **Main requirements :**
  - Number of points : $|E| = 2^c p$, with c small and p a large prime
  - Number of points on the Twist : we have the same requirement
- **Secondary requirements :**
  - j-invariant : $^1/_{d^8}$ shall generate $GF(2^m)$
  - Avoiding small discriminant : $\Delta_E = Tr(E)^2 - 4q$ where $q = 2^m$ shall be divisible by a large prime
  - Avoiding pairing attack : the embedding degree of the curve shall be large, greater than $\frac{p-1}{100}$

NEW ELLIPTIC CURVES

Secu.	Name	Modulus	Parameter d	Generator
112	BEC223	$x^{223} + x^{159} + 1$	$t^{64} + t^{36} + t^{5} + 1$	
128	BEC257	$x^{257} + x^{65} + 1$	$t^{65} + t^{31} + t^{14} + 1$	
156	BEC313	$x^{313} + x^{121} + 1$	$t^{38} + t^{33} + t^{28} + 1$	
215	BEC431	$x^{431} + x^{303} + x^{239} + x^{111} + 1$	$t^{83} + t^{66} + t^{17} + 1$	
239	BEC479	$x^{479} + x^{255} + 1$	$t^{73} + t^{29} + t^{3} + 1$	
243	BEC487	$x^{487} + x^{295} + x^{167} + x^{39} + 1$	$t^{69} + t^{33} + t^{15} + 1$	
260	BEC521	$x^{521} + x^{489} + 1$	$t^{66} + t^{29} + t^{28} + 1$	
284	BEC569	$x^{569} + x^{441} + x^{313} + x^{121} + 1$	$t^{56} + t^{45} + t^{41} + 1$	

- **49 new curves**
- **3 months of computing over a cluster of 80 cores**
- **Selection rate : 0,001%**

OPTIMIZED GENERATOR

- **Each step of the Montgomery Ladder, we have a multiplication by $^{1}/_{w_1}$ where $w_1 = w(G)$, G the point generator**

- **We can choose a generator with a small inverse w representation**

- **Re-write the BEC equation with w :**
  - $d(w + w^2) = x^4 + (1 + w + w^2)x^2 + (w + w^2)x$

- **We save 20% of the computation time of the Montgomery Ladder**

NEW ELLIPTIC CURVES

Secu.	Name	Modulus	Parameter d	Generator
112	BEC223	$x^{223} + x^{159} + 1$	$t^{64} + t^{36} + t^{5} + 1$	$t^{32} + 1$
128	BEC257	$x^{257} + x^{65} + 1$	$t^{65} + t^{31} + t^{14} + 1$	t^{192}
156	BEC313	$x^{313} + x^{121} + 1$	$t^{38} + t^{33} + t^{28} + 1$	$t^{64} + 1$
215	BEC431	$x^{431} + x^{303} + x^{239} + x^{111} + 1$	$t^{83} + t^{66} + t^{17} + 1$	$t^{64} + 1$
239	BEC479	$x^{479} + x^{255} + 1$	$t^{73} + t^{29} + t^{3} + 1$	$t^{64} + 1$
243	BEC487	$x^{487} + x^{295} + x^{167} + x^{39} + 1$	$t^{69} + t^{33} + t^{15} + 1$	$t^{64} + 1$
260	BEC521	$x^{521} + x^{489} + 1$	$t^{66} + t^{29} + t^{28} + 1$	$t^{32} + 1$
284	BEC569	$x^{569} + x^{441} + x^{313} + x^{121} + 1$	$t^{56} + t^{45} + t^{41} + 1$	$t^{64} + 1$

BEC AND PHYSICAL ATTACKS

Physical Attacks	Intrinsic Resitance		Remaining Vulnerability
	Due to choice of parameters of BEC	Due to implementation done	Additional countermeasure
Timming Attacks	Unified arithmetics	Montgomery Ladder/Constant time programming	-
SPA			
CPA/DPA	-	-	Randomization of coordinates
Template Attack			
Relative doubling Attack	-	-	Blinded scalar
RPA/ZPA	W-coordinates arithmetics	Direct implementation of the generator	-
Carry-based Attack	Binary curves chosen	-	-
Horizontal Attack	-	-	Attack model to be tested
Safe error	-	Montgomery Ladder	-
Invalid point analysis	-	-	Verify that point is on the curve
Invalide curve analysis	Curves' parameters on Twist for eg	Direct implementation of curve parameter	-
Twist Attack	Curves' parameter for Twist	-	-
DFA	-	-	Blinded scalar

PERFORMANCES

- **RISC V at 100MHz**
- **Cortex M3 at 96MHz**

- **Bec Library**
  - W-coordinate
  - Montgomery Ladder

- **MbedTLS**
  - Jacobian coordinates
  - Sliding window (w=7)

Security Level	Curves	RISV V	Cortex M3
86	**P192**	-	**66 ms**
112	BEC223	32 ms	-
	P224	-	**85 ms**
128	BEC257	46 ms	-
	Ed25519	-	**94 ms**
	P256	-	**122 ms**
151	BEC313	79 ms	-
192	**P384**	-	**202 ms**
215	BEC431	188 ms	-
240	BEC479	242 ms	-
	BEC487	264 ms	-
256	**P512**	-	**351 ms**
	BEC521	316 ms	-
284	BEC569	396 ms	-

CONCLUSION

- **New set of Binary Edwards Curves**
  - Check all security requirements
  - Optimized for 32 bits architectures
  - Secure against a set of physical attacks

- **With great performances**

- **Works in progress :**
  - Check the physical security
  - Complete integration in ECC protocols (ECDH, ECDSA, EdDSA)

Thanks for your attention

Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 rue des Martyrs | 38054 Grenoble Cedex | France
www.leti.fr