BINARY EDWARDS CURVES FOR INTRINSICALLY SECURE ECC IMPLEMENTATION FOR THE IOT
TABLE OF CONTENTS

Our approach

How to generate new elliptic curves?

Scott’s polynomials

Binary Edwards Curves

Optimized Generator

Performances
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
• **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...

- Point generator
  - Random point
  - Optimized point

- Elliptic Curve
  - Elliptic curve model
  - Parameters
  - Point representation

- Finite Field
  - Prime or binary fields
  - Representation
  - Modulus
HOW TO GENERATE NEW ELLIPTIC CURVES?

Cryptographic Protocols: ECDSA, ECDH...

- Random point
- Optimized point

- Elliptic curve model
- Parameters
- Point representation

- Prime or binary field
- Representation
- Modulus

Binary Fields

Binary Edwards Curves

Optimized point
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: \( m - a \equiv 0 \mod w \)
  - Lucky pentanomials: \( m - a \equiv 0 \mod w, m - b \equiv 0 \mod w \) and \( m - c \equiv 0 \mod w \)
  - \( w \) 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

<table>
<thead>
<tr>
<th>Secu.</th>
<th>Name</th>
<th>Modulus</th>
<th>Parameter d</th>
<th>Generator</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>BEC223</td>
<td>$x^{223} + x^{159} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>BEC257</td>
<td>$x^{257} + x^{65} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>156</td>
<td>BEC313</td>
<td>$x^{313} + x^{121} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>215</td>
<td>BEC431</td>
<td>$x^{431} + x^{303} + x^{239} + x^{111} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>239</td>
<td>BEC479</td>
<td>$x^{479} + x^{255} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>243</td>
<td>BEC487</td>
<td>$x^{487} + x^{295} + x^{167} + x^{39} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>260</td>
<td>BEC521</td>
<td>$x^{521} + x^{489} + 1$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>284</td>
<td>BEC569</td>
<td>$x^{569} + x^{441} + x^{313} + x^{121} + 1$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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 : $(0, 0)$
  - $\forall P \in E\left(GF(2^m)\right), P = (x, y) \rightarrow -P = (y, x)$
  - $P + (1, 1) = (x, y) + (1, 1) = (x + 1, y + 1)$
  - $d(X + Y)Z^3 + d(X^2 + Y^2)Z^2 = XYZ^2 + XY(X + Y) + X^2Y^2$
  - Complete group law
  - Birational equivalent to a Weierstrass curve:
    \[ v^2 + uv = u^3 + (d^2 + d)u^2 + d^8 \]
$w$-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 revisited with the Co-Z trick.

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

1. $C \leftarrow (W_2 + W_3)^2$
2. $D \leftarrow Z^2$
3. $E \leftarrow \frac{1}{w_1} C$
4. $U \leftarrow E + C$
5. $V \leftarrow E + D$
6. $S \leftarrow \left( W_2(Z + W_2) \right)^2$
7. $T \leftarrow S + dD^2$
8. $W_4 \leftarrow UT$
9. $W_5 \leftarrow VS$
10. $Z' \leftarrow VT$
11. return $W_4, W_5, Z'$

---

**Algorithm 3** Montgomery Ladder

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

1. $R_0 \leftarrow 0$
2. $R_1 \leftarrow P$
3. for $j = t - 1 \text{ to } 0$ do
4.  if $k_j = 0$ then
5.  $R_1 \leftarrow R_0 + R_1$
6.  $R_0 \leftarrow 2R_0$
7.  else
8.  $R_0 \leftarrow R_0 + R_1$
9.  $R_1 \leftarrow 2R_1$
10. end if
11. end for
12. 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

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

- 49 new curves
- 3 months of computing over a cluster of 80 cores
- Selection rate: 0.001%
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

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

<table>
<thead>
<tr>
<th>Physical Attacks</th>
<th>Intrinsic Resistance</th>
<th>Remaining Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Due to choice of parameters of BEC</td>
<td>Due to implementation done</td>
</tr>
<tr>
<td>Timming Attacks</td>
<td>Unified arithmetics</td>
<td>Montgomery Ladder/Constant time programming</td>
</tr>
<tr>
<td>SPA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPA/DPA</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Template Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relative doubling Attack</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>RPA/ZPA</td>
<td>W-coordinates arithmetics</td>
<td>Direct implementation of the generator</td>
</tr>
<tr>
<td>Carry-based Attack</td>
<td>Binary curves chosen</td>
<td>-</td>
</tr>
<tr>
<td>Horizontal Attack</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Safe error</td>
<td>-</td>
<td>Montgomery Ladder</td>
</tr>
<tr>
<td>Invalid point analysis</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Invalide curve analysis</td>
<td>Curves’ parameters on Twist for eg</td>
<td>Direct implementation of curve parameter</td>
</tr>
<tr>
<td>Twist Attack</td>
<td>Curves’ parameter for Twist</td>
<td>-</td>
</tr>
<tr>
<td>DFA</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
PERFORMANCES

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

- Bec Library
  - W-coordinate
  - Montgomery Ladder

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

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Curves</th>
<th>RISV V</th>
<th>Cortex M3</th>
</tr>
</thead>
<tbody>
<tr>
<td>86</td>
<td>P192</td>
<td>-</td>
<td>66 ms</td>
</tr>
<tr>
<td>112</td>
<td>BEC223</td>
<td>32 ms</td>
<td>-</td>
</tr>
<tr>
<td>128</td>
<td>BEC257</td>
<td>46 ms</td>
<td>-</td>
</tr>
<tr>
<td>128</td>
<td>Ed25519</td>
<td>-</td>
<td>94 ms</td>
</tr>
<tr>
<td>151</td>
<td>BEC313</td>
<td>79 ms</td>
<td>-</td>
</tr>
<tr>
<td>192</td>
<td>P384</td>
<td>-</td>
<td>202 ms</td>
</tr>
<tr>
<td>215</td>
<td>BEC431</td>
<td>188 ms</td>
<td>-</td>
</tr>
<tr>
<td>240</td>
<td>BEC479</td>
<td>242 ms</td>
<td>-</td>
</tr>
<tr>
<td>256</td>
<td>P512</td>
<td>-</td>
<td>351 ms</td>
</tr>
<tr>
<td>284</td>
<td>BEC521</td>
<td>316 ms</td>
<td>-</td>
</tr>
<tr>
<td>284</td>
<td>BEC569</td>
<td>396 ms</td>
<td>-</td>
</tr>
</tbody>
</table>
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