


Unified Formulas for Some Deterministic Almost-Injective Encodings into Hyperelliptic Curves

Michel SECK
michel.seck@ucad.edu.sn
Joint work with Nafissatou Diarra

Cheikh Anta Diop University
Department of Mathematics and Computer Science

Africacrypt-2018
May 7-9, 2018- Marrakesh, Morocco

Outline

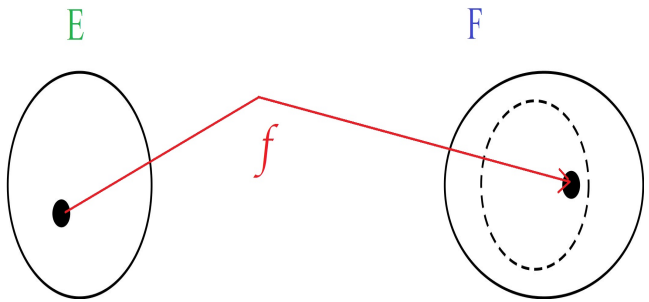
Introduction

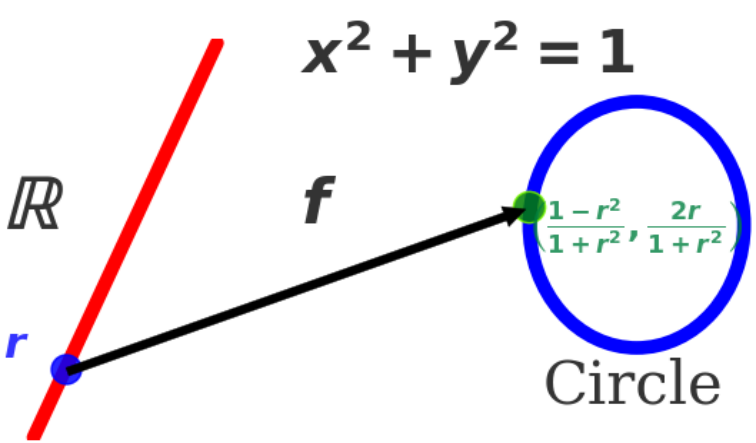
Introduction : Encoding function ?

Input:

- A set E, A set (group) F
- An element of E;

Output: An element of F;





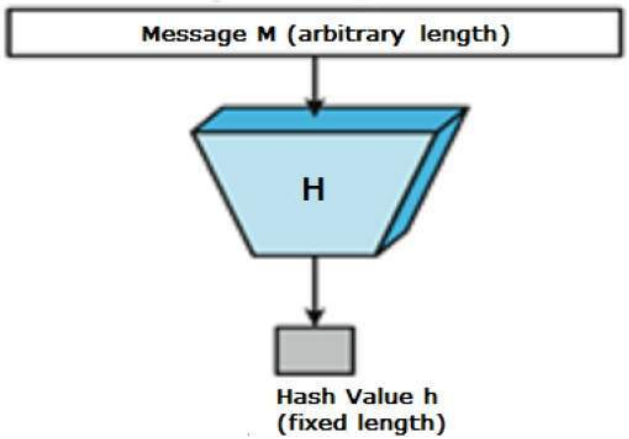
In ECC and HECC:

- ☛ $E = \mathbb{F}_q$
- ☛ F is an (hyper)elliptic curve.

Applications of encoding functions in HECC : Construction of hash functions

Cryptographic Hash Functions

A one-way function without trapdoor.



$h : \{0,1\}^* \rightarrow \{0,1\}^l$

1. *preimage resistant*;
2. *collision resistant*;
3. *second-preimage resistant*.

Applications of encoding functions in HECC : Construction of hash functions

- ☛ Classical method : **Probabilistic**
- ☛ Second method: **Deterministic** :

$$H(m) = f(h(m))$$

where f is deterministic encoding in constant time and h a classical hash function modelled as random oracle

Applications of encoding functions in HECC : Construction of hash functions

Let $h_1, h_2, ..., h_s : \{0,1\}^* \to \mathbb{F}_q$ be s classical hash functions modelled as random oracles. Then the construction $\phi^{\otimes s} : m \mapsto \phi_g(h_1(m)) + \phi_g(h_2(m)) + \ldots + \phi_g(h_s(m))$ is indifferentiable from a random oracle **if :**

- ϕ_g is a deterministic encoding well-distributed
- $s >$ genus of the curve

R. R. Farashahi, P.-A. Fouque, I. E. Shparlinski, M. Tibouchi and J. F. Voloch. Indifferentiable Deterministic Hashing To Elliptic And Hyperelliptic Curves. In Mathematics of Computation vol. 82,number 281, pp. 491-512. January 2013.

Elliptic and Hyperelliptic curves

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ its algebraic closure.

Definition

An **Hyperelliptic curve** $\mathcal{C}$ of genus $g \geq 1$ over $\mathbb{K}$ is given by an equation of the form $\mathcal{C}: \ y^2 + h(x)y = f(x)$, where:

- $h \in \mathbb{K}[x]$ is a polynomial of degree at most g,
- $f \in \mathbb{K}[x]$ is a monic polynomial of degree $2g + 1$,
- there are no point in $\mathcal{C}$ satisfying simultaneously $2y + h = 0$ and $yh' - f' = 0$.

Elliptic curve (Weierstrass form): when $g = 1$.

Different forms of an Hyperelliptic curve of genus 2 over Real field

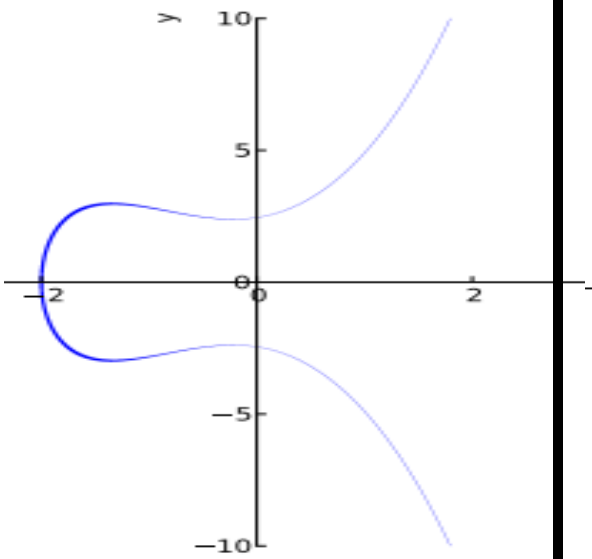


Figure 1:
$\mathbb{H}_1 : y^2 = x^5 - 5x^3 + 4x$

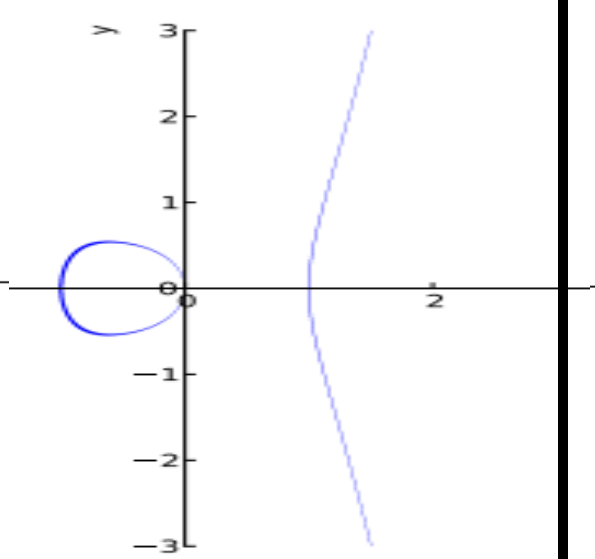


Figure 2: $\mathbb{H}_2 : y^2 = x^5 + x^4 - x^2 - x$

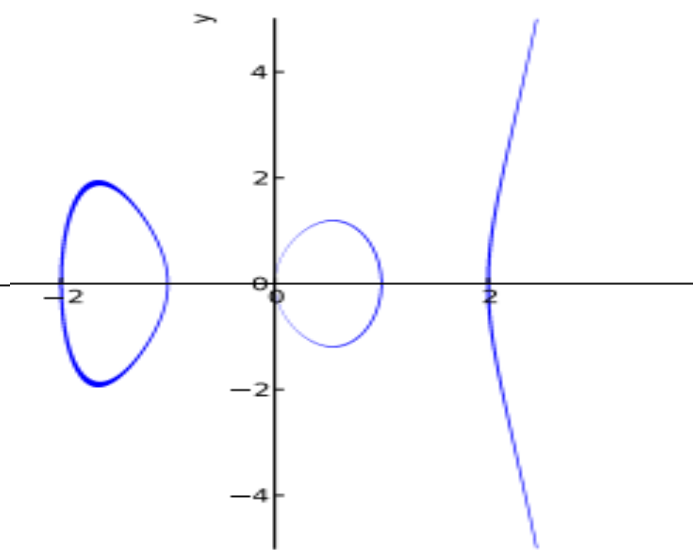


Figure 3:
$\mathbb{H}_3 : y^2 = x^5 + 2x^4 + 4x^3 + 8x^2 + 3x + 6$

Quadratic character

Fix $q \in \mathbb{Z}$, an odd prime power. We say that a in the finite field $\mathbb{F}_q$ is a quadratic residue , if a is a square in $\mathbb{F}_q$ i.e. if there is $m \in \mathbb{F}_q$ such that $a = m^2$. One then defines the quadratic character as follows:

$$\chi(a) = \left(\frac{a}{q}\right) = \begin{cases} 0, & \text{if } a = 0 \text{ in } \mathbb{F}_q \\ 1, & \text{if } a \text{ is a nonzero square} \\ -1, & \text{if } a \text{ is not a square.} \end{cases}$$

Overview on Encodings into Elliptic and Hyperelliptic Curves

Overview on Encodings into Elliptic and Hyperelliptic Curves

For genus $g = 1$:

Boneh and Franklin (**2001**):
$y^2 = x^3 + b$;

Shallue and Woestjine (**2006**):
$y^2 = x^3 + ax + b$;

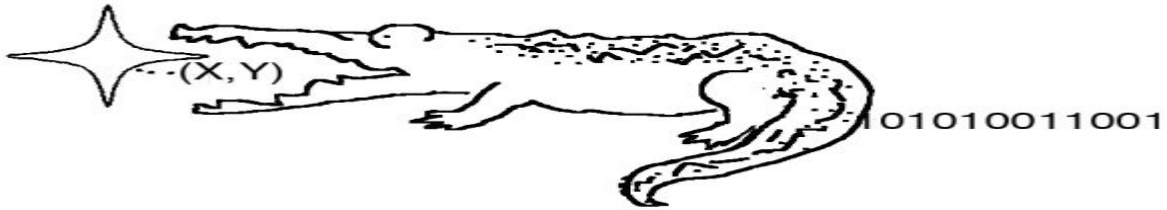
Icart (**2009**):
$y^2 = x^3 + ax + b$;

Farashahi (**2011**):
$x^3 + y^3 = 1 + 3dxy$;

Overview on Encodings into Elliptic and Hyperelliptic Curves

For genus $g = 1$:

- **Elligator 1-2** from Bernstein *et al.*(**2013**):
  $x^2 + y^2 = 1 + dx^2y^2$ Edwards form;
  $y^2 = x^3 + Ax^2 + Bx$ Weierstrass form;



Daniel. J. Bernstein, Mike. Hamburg, Anna. Krasnova, and Tanja Lange. *Elligator: Elliptic-curve points indistinguishable from uniform random strings*. In V. Gligor and M. Yung, editors, ACM CCS, 2013.

Overview on Encodings into Elliptic and HyperElliptic Curves

For genus $g \geq 2$:

Ulas (**2007**):
$y^2 = x^n + ax + b$
$y^2 = x^n + ax^2 + bx,\ n \geq 5$

Kammerer *et al.* (**2010**):
$y^2 = (x^3 + 3ax + 2)^2 + 8bx^3$;

Brier *et al.* (**2010**):
simplified version of Ulas's encoding;

Fouque, Joux and Tibouchi (**2013**):
$H_d^\lambda : y^2 = \lambda a x^5 + (c^2 + 1/c^2)x^3 + x$

Overview on Encodings into Elliptic and HyperElliptic Curves : Seck et al. (AFRICACRYPT2017)

- $\mathbb{H}^1 : \ y^2 = x^5 + ax^4 + cx^2 + dx$
- $\mathbb{H}^2 : \ y^2 = x^5 + bx^3 + dx + e$
- $\mathbb{H}^3 : \ y^2 = x^5 + ax^4 + e$

Michel Seck, Hortense Boudjou, Nafissatou Diarra and Ahmed Youssef Ould Cheikh. *On Indifferentiable Hashing into the Jacobian of Hyperelliptic Curves of Genus 2*. In: Joye M., Nitaj A. (eds) Progress in Cryptology - AFRICACRYPT 2017. AFRICACRYPT 2017. Lecture Notes in Computer Science, vol 10239. Springer, Cham, pages 205-222.

Generalization of our encoding functions in genus $g = 2$

After successfully enconding in genus two, we have asked the following questions

Question 1

☛ Can we apply the same technique to encode into an hyperelliptic curve of genus $g > 2$?

Question 2

If yes,
☛ Can we generalize the same technique by encoding into an hyperelliptic curve of any genus g?

Deterministic almost-injective encodings into hyperelliptic curves of genus $g \leq 5$

New deterministic almost-injective encoding functions $\psi_i : \mathcal{R}_i \subset \mathbb{F}_q \to \mathbb{H}_i$ for $i = 1, 3, 4, 5$

$$\mathbb{H}_1 : y^2 = f_1(x) = x^3 + a_1 x + a_0$$

$$\mathbb{H}_2 : y^2 = f_2(x) = x^5 + a_3 x^3 + a_1 x + a_0 \text{ ➥ Africacrypt-2017}$$

$$\mathbb{H}_3 : y^2 = f_3(x) = x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0;$$

$$\mathbb{H}_4 : y^2 = f_4(x) = x^9 + a_7 x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0;$$

$$\mathbb{H}_5 : y^2 = f_5(x) = x^{11} + a_9 x^9 + a_7 x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0.$$

Our encoding function in genus $g = 3$

- Assume that $\mathrm{char}(\mathbb{F}_q) = p \neq 2, 3, 7$.
- Let $s \in \mathbb{F}_q^*$ such that $31s^2 + 42s - 441 = 0$.
- Let $w \in \mathbb{F}_q^\star$ is an arbitrary parameter.
- Let $\mathbb{H}_3 : y^2 = f_3(x) = x^7 + a_5x^5 + a_3x^3 + a_1x + a_0$, with $a_5 = sw^2$, $a_1 = \frac{sw^6}{3}$, $a_3 = \frac{5sw^4}{3}$ and $a_0 = \frac{s-21}{21}w^7$, be an hyperelliptic curve of genus 3 over $\mathbb{F}_q$ with $q \equiv 7 \mod 8$.
- Let u be a parameter such that $\chi(u) = -1$ and define $\mathcal{R}_3 = \left\{ r \in \mathbb{F}_q^*, f_3(w[ur^2(-651s - 441) - 1]) \neq 0 \right\}$

Our encoding function in genus $g = 3$

Algorithm 1

Input: The hyperelliptic curve $\mathbb{H}_3$, an element $r \in \mathcal{R}_3$
Output: A point (x, y) on $\mathbb{H}_3$

$$v := w[ur^2(-651s - 441) - 1];$$
$$\varepsilon := \chi(v^7 + a_5 v^5 + a_3 v^3 + a_1 v + a_0);$$
$$x := \frac{1+\varepsilon}{2} v + \frac{1-\varepsilon}{2}\left(\frac{w(-v+w)}{v+w}\right);$$
$$y := -\varepsilon\sqrt{x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0};$$

return (x, y).

Encoding function: $\psi_3 : \mathcal{R}_3 \to \mathbb{H}_3 : r \mapsto \psi_3(r) = (x, y)$ is well-defined.

The inverse of our encoding function in genus $g = 3$

Theorem 1

1. Let (x, y) be a point of the hyperelliptic curve $\mathbb{H}_3$, then $(x, y) \in \mathrm{Im}(\psi_3)$ if and only if $uw(x + w)(-441 - 651s)$ is a nonzero square in $\mathbb{F}_q$.
2. Let $(x, y) \in \mathrm{Im}(\psi_3)$ and define $\bar{r}$ as follows:
   - $\bar{r} = \sqrt{\frac{x+w}{uw(-441-651s)}}$, if $y \notin \sqrt{\mathbb{F}_q^2}$
   - $\bar{r} = \sqrt{\frac{2w}{u(x+w)(-441-651s)}}$, if $y \in \sqrt{\mathbb{F}_q^2}$

   Then $\bar{r} \in \mathcal{R}_3$ and $\psi_3(\bar{r}) = (x, y)$.

Our encoding functions in genus $g = 1, 4, 5$

We have similar algorithms and theorems in genus

- $g = 1$
- $g = 2$
- $g = 4$
- $g = 5$

Unified formulas for all our encodings

Encoding in the curve

$\mathbb{H} : \mathbf{y^2 = f_g(x) = x^{(2g+1)} + a_{(2g-1)}x^{(2g-1)} + a_{(2g-3)}x^{(2g-3)} + \ldots + a_1x + a_0}$
of genus $g \leq 5$

Unified formulas

$$\mathbb{H}_1 : y^2 = f_1(x) = x^3 + a_1 x + a_0$$

$$\mathbb{H}_2 : y^2 = f_2(x) = x^5 + a_3 x^3 + a_1 x + a_0 \text{ ➥ Africacrypt-2017}$$

$$\mathbb{H}_3 : y^2 = f_3(x) = x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0;$$

$$\mathbb{H}_4 : y^2 = f_4(x) = x^9 + a_7 x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0;$$

$$\mathbb{H}_5 : y^2 = f_5(x) = x^{11} + a_9 x^9 + a_7 x^7 + a_5 x^5 + a_3 x^3 + a_1 x + a_0.$$

Encoding into the hyperelliptic curve of genus $g \leq 5$

$$\mathbb{H} : \mathbf{y^2 = f_g(x) = x^{(2g+1)} + a_{(2g-1)} x^{(2g-1)} + a_{(2g-3)} x^{(2g-3)} + \ldots + a_1 x + a_0}$$

The fundamental second degree equation

Genus g	Curve	Second degree equation in s
1	$\mathbb{H}_1 = E : y^2 = f_1(x)$	$s^2 + 6s - 9 = 0$
2	$\mathbb{H}_2 : y^2 = f_2(x)$	$7s^2 + 20s - 100 = 0$
3	$\mathbb{H}_3 : y^2 = f_3(x)$	$31s^2 + 42s - 441 = 0$
4	$\mathbb{H}_4 : y^2 = f_4(x)$	$127s^2 + 72s - 1296 = 0$
5	$\mathbb{H}_5 : y^2 = f_5(x)$	$511s^2 + 110s - 3025 = 0$

Goal: to give an equation which generalize the five equations.

Note that 7, 31 and 127 are prime numbers.

Remark

1. The parameter $s \in \mathbb{F}_q^*$ satisfy the equation $\alpha_g s^2 + \beta_g s - \gamma_g = 0$ where
   - $\alpha_g = 2^{2g-1} - 1$
   - $\beta_g = 4g^2 + 2g$
   - $\gamma_g = (2g^2 + g)^2$

   $\Longrightarrow$ g is the genus of the curve.
2. Note that $\alpha_g = 2^{2g-1} - 1$ is a Mersenne number and $7, 31$ and 127 are the 2nd, 3th and 4th prime Mersenne numbers.

The different values of v

Genus g	Curve	Value of v
1	$\mathbb{H}_1 : y^2 = f_1(x)$	$v = w[ur^2(-3s - 9) - 1]$
2	$\mathbb{H}_2 : y^2 = f_2(x)$	$v = w[ur^2(-35s - 50) - 1]$
3	$\mathbb{H}_3 : y^2 = f_3(x)$	$v = w[ur^2(-651s - 441) - 1]$
4	$\mathbb{H}_4 : y^2 = f_4(x)$	$v = w[ur^2(-2286s - 648) - 1]$
5	$\mathbb{H}_5 : y^2 = f_5(x)$	$v = w[ur^2(-28105s - 3025) - 1]$

Remark

$v = v(g) = w[ur^2(-m_g s - n_g) - 1]$ where

- $m_g = \frac{1}{2} \times \alpha_g \times \beta_g$ and $n_g = (2g^2 + g)^2$ if the genus g is odd
- $m_g = \frac{1}{4} \times \alpha_g \times \beta_g$ and $n_g = \frac{1}{2} \times (2g^2 + g)^2$ if g is even

Our encoding function in genus $g \leq 5$

- Let $g \in \{1, 2, 3, 4, 5\}$.
- Let $\mathbb{F}_q$ be a finite field with $\mathrm{char}(\mathbb{F}_q) = p$, $p \neq 2$ and $p \nmid (2g^2 + g)$ and $q = p^n$ is an odd prime power such that $q \equiv 7 \mod 8$.
- Let $s \in \mathbb{F}_q^*$ such that $(2^{2g-1} - 1)s^2 + (4g^2 + 2g)s - ((2g^2 + g)^2) = 0$:
- Let $w \in \mathbb{F}_q^\star$ be an arbitrary parameter.

Our encoding function in genus $g \leq 5$

- Let $\mathbb{H}_g : y^2 = h_g(x) = x^{(2g+1)} + a_{(2g-1)}x^{(2g-1)} + a_{(2g-3)}x^{(2g-3)} + \ldots + a_1 x + a_0$ be an hyperelliptic curve of genus g over $\mathbb{F}_q$ with the previous conditions on q where $a_0 = \frac{\left(s-(2g^2+g)\right)}{(2g^2+g)} w^{(2g+1)}$, $a_{(2g-1)} = sw^2$, $a_1 = \frac{sw^{2g}}{g}$ for $g \geq 1$, $a_3 = \frac{2g-1}{3} sw^{2g-2}$ for $g \geq 3$, $a_5 = \frac{7sw^4}{2}$ if $g = 4$ and $a_7 = 6sw^4$, $a_5 = \frac{42sw^6}{5}$ if $g = 5$
- Let u be a parameter such that $\chi(u) = -1$ and define $\mathcal{R}_g = \left\{ r \in \mathbb{F}_q^\star, h_g(w[ur^2(-m_g s - n_g) - 1]) \neq 0 \right\}$

Our encoding function in genus $g \leq 5$

Algorithm 2

Input: The hyperellitic curve $\mathbb{H}_g$, an element $r \in \mathcal{R}_g$
Output: A point (x, y) on $\mathbb{H}_g$

$v := v(g) = w[ur^2(-m_g s - n_g) - 1];$

$\varepsilon := \chi(v^{(2g+1)} + a_{(2g-1)}v^{(2g-1)} + a_{(2g-3)}v^{(2g-3)} + \ldots + a_1 v + a_0);$

$$x := \frac{1+\varepsilon}{2}v + \frac{1-\varepsilon}{2}\left(\frac{w(-v+w)}{v+w}\right);$$

$$y := -\varepsilon\sqrt{x^{(2g+1)} + a_{(2g-1)}x^{(2g-1)} + a_{(2g-3)}x^{(2g-3)} + \ldots + a_1 x + a_0};$$

return (x, y).

Encoding function: $\psi_g : \mathcal{R}_g \to \mathbb{H}_g : r \mapsto \psi_g(r) = (x, y)$ is well-defined.

The inverse of our encoding function in genus $g \leq 5$

Theorem 2

1. Let (x, y) be a point of the hyperelliptic curve $\mathbb{H}_g$, then $(x, y) \in \mathrm{Im}(\psi_g)$ if and only if $uw(x + w)(-n_g - m_g s)$ is a nonzero square in $\mathbb{F}_q$.
2. Let $(x, y) \in \mathrm{Im}(\psi_g)$ and define $\bar{r}$ as follows:
   - $\bar{r} = \sqrt{\frac{x+w}{uw(-n_g - m_g s)}}$, if $y \notin \sqrt{\mathbb{F}_q^2}$
   - $\bar{r} = \sqrt{\frac{2w}{u(x+w)(-n_g - m_g s)}}$, if $y \in \sqrt{\mathbb{F}_q^2}$

   then $\bar{r} \in \mathcal{R}_g$ and $\psi_g(\bar{r}) = (x, y)$.

Implementation using the Sage Computer algebra

Implementation: Genus 1

```
q = 1009
fe = EncodingAndInvertGenusg(q=q,u=11,w=5,g=1); print(fe)
pt = fe.encode(121); print("\n (x,y) = "+str(pt)+"\n")
dc = fe.decode(pt); print("\n"+str(dc)+"\n")

Hyperelliptic curve defined by y^2=x^3 + 297*x + 370 over
finite field F_1009/< a + 1008 >

(x,y) = (282, 101)

The preimages of (282 , 101) by the encoding function
are equal to (219 , 790) or (121 , 888)
```

Implementation: Genus 2

```
q = 1009 #
fe = EncodingAndInvertGenusg(q=q,u=11,w=5,g=2); print(fe)
pt = fe.encode(121); print("\n (x,y) = "+str(pt)+"\n")
dc = fe.decode(pt); print("\n"+str(dc)+"\n")

Hyperelliptic curve defined by
y^2=x^5 + 619*x^3 + 170*x + 72 over
 finite field F_1009/< a + 1008 >

(x,y) = (888, 600)

The preimages of (888 , 600) by the encoding function
 are equal to (121 , 888) or (172 , 837)
```

Implementation: Genus 3

```
q = 1009 #
fe = EncodingAndInvertGenusg(q=q,u=11,w=5,g=3); print(fe)
pt = fe.encode(121); print("\n (x,y) = "+str(pt)+"\n")
dc = fe.decode(pt); print("\n"+str(dc)+"\n")

Hyperelliptic curve defined by
 y^2=x^7 + 949*x^5 + 527*x^3 + 617*x + 297
over finite field F_1009/< a + 1008 >

(x,y) = (462, 317)

The preimages of (462 , 317) by the encoding function
are equal to (171 , 838) or (121 , 888)
```

Implementation: Genus 4

```
q = 1009 #
fe = EncodingAndInvertGenusg(q=q,u=11,w=5,g=4); print(fe)
pt = fe.encode(121); print("\n (x,y) = "+str(pt)+"\n")
dc = fe.decode(pt); print("\n"+str(dc)+"\n")

Hyperelliptic curve defined by
y^2=x^9 + 290*x^7 + 150*x^5 + 482*x^3 + 210*x + 752
over finite field F_1009/< a + 1008 >

(x,y) = (754, 163)

The preimages of (754 , 163) by the encoding function
 are equal to (131 , 878) or (121 , 888)
```

Implementation: Genus 5

```
q = 1009 #
fe = EncodingAndInvertGenusg(q=q,u=11,w=5,g=5); print(fe)
pt = fe.encode(121); print("\n (x,y) = "+str(pt)+"\n")
dc = fe.decode(pt); print("\n"+str(dc)+"\n")
Hyperelliptic curve defined by
y^2=x^11 + 665*x^9 + 868*x^7 + 110*x^5 + 838*x^3
+ 724*x + 99 over finite field F_1009/< a + 1008 >

(x,y) = (135, 150)

The preimages of (135 , 150) by the encoding function
are equal to (33 , 976) or (121 , 888)
```

Conclusion

- We have successfully constructed a deterministic encoding into an hyperelliptic curve of genus $g \leq 5$ that generalize some results of Seck *et al.*.
- We have also showed in what conditions one can invert the encoding function.

Open problem

It should be nice if one can extend our encoding to any genus.

Thank you for your attention!