Exploring the use of Pell hyperbolas in DLP-based cryptosystems

Based on a joint work with S. Dutto and N. Murru

Gessica Alecci

Politecnico di Torino

Young Researchers Algebra Conference
July 28th, 2023

Outline

Table of Contents

Pell hyperbolas

The general quadratic Diophantine equation in the two unknown integers x and y is given by

$$ax^2 + by^2 = k,$$

with a, b and k positive or negative integers.

Pell hyperbolas

The general quadratic Diophantine equation in the two unknown integers x and y is given by

$$ax^2 + by^2 = k,$$

with a, b and k positive or negative integers.

The Pell equation is a special case of it and, for a fixed non-zero element $d \in \mathbb{K}$, it is

$$x^2 - dy^2 = 1. \quad (1)$$

Pell hyperbolas

The general quadratic Diophantine equation in the two unknown integers x and y is given by

$$ax^2 + by^2 = k,$$

with a, b and k positive or negative integers.

The Pell equation is a special case of it and, for a fixed non-zero element $d \in \mathbb{K}$, it is

$$x^2 - dy^2 = 1. \tag{1}$$

The Pell hyperbola over a field $\mathbb{K}$ is a curve defined as

$$\mathcal{C}_d(\mathbb{K}) = \left\{(x, y) \in \mathbb{K} \times \mathbb{K} \,|\, x^2 - dy^2 = 1\right\}. \tag{2}$$

Pell hyperbolas

Brahmagupta was one of the first mathematicians to study the solutions of (1); in particular, he studied the case with $d = 83$ and $d = 92$.
He discovered that given two solutions of (1), namely (x_1, y_1) and (x_2, y_2), also $(x_1x_2 + dy_1y_2, x_1y_2 + y_1x_2)$ will be a solution.

Pell hyperbolas

Brahmagupta was one of the first mathematicians to study the solutions of (1); in particular, he studied the case with $d = 83$ and $d = 92$.
He discovered that given two solutions of (1), namely (x_1, y_1) and (x_2, y_2), also $(x_1x_2 + dy_1y_2, x_1y_2 + y_1x_2)$ will be a solution.

From the definition of the Brahmagupta product

$$(x_1, y_1) \otimes_d (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + y_1x_2),$$

it follows that $(\mathcal{C}_d(\mathbb{K}), \otimes_d)$ is a group where the identity element is the vertex of the hyperbola with coordinates $(1, 0)$ and the inverse of a point (x, y) is $(x, -y)$.

Pell hyperbolas

If $\mathbb{K} = \mathbb{F}_q$ that is a finite field of order q, with q odd prime, then the group over the Pell hyperbola is cyclic of order $q - \chi_q(d)$ where $\chi_q(d)$ is the quadratic character of $d \in \mathbb{F}_q$, i.e.

$$\chi_q(d) = \begin{cases} 0 & \text{if } d = 0, \\ 1 & \text{if } d \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{if } d \text{ is a non–square in } \mathbb{F}_q. \end{cases}$$

Pell hyperbolas

If $\mathbb{K} = \mathbb{F}_q$ that is a finite field of order q, with q odd prime, then the group over the Pell hyperbola is cyclic of order $q - \chi_q(d)$ where $\chi_q(d)$ is the quadratic character of $d \in \mathbb{F}_q$, i.e.

$$\chi_q(d) = \begin{cases} 0 & \text{if } d = 0, \\ 1 & \text{if } d \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{if } d \text{ is a non–square in } \mathbb{F}_q. \end{cases}$$

All Pell hyperbolas such that $\chi_q(d) = \chi_q(d')$ are isomorphic, in particular, if $d' = ds^2$ for some $s \in \mathbb{F}_q$, the group isomorphism is

$$\begin{aligned} \delta_{d,d'} : \left(\mathcal{C}_d(\mathbb{F}_q), \otimes_d\right) &\xrightarrow{\sim} \left(\mathcal{C}_{d'}(\mathbb{F}_q), \otimes_{d'}\right), \\ (x, y) &\longmapsto (x, y/s). \end{aligned} \tag{3}$$

Table of Contents

Generalized Pell hyperbolas

The equation of the Pell hyperbola is a particular case of the canonical form of hyperbolas and ellipses that, over a finite field, is given by

$$\mathcal{C}_{c,d}(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid x^2 - dy^2 = c\}.$$

Generalized Pell hyperbolas

The equation of the Pell hyperbola is a particular case of the canonical form of hyperbolas and ellipses that, over a finite field, is given by

$$\mathcal{C}_{c,d}(\mathbb{F}_q) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \,|\, x^2 - dy^2 = c\right\}.$$

Considering as identity any point $(a, b) \in \mathcal{C}_{c,d}(\mathbb{F}_q)$, the Brahmagupta product can be generalized obtaining $\otimes_{a,b,c,d}$.

$$(x_1, y_1) \otimes_{a,b,c,d} (x_2, y_2) = \frac{1}{c}(a, -b) \otimes_d (x_1, y_1) \otimes_d (x_2, y_2). \qquad (4)$$

Generalized Pell hyperbolas

The equation of the Pell hyperbola is a particular case of the canonical form of hyperbolas and ellipses that, over a finite field, is given by

$$\mathcal{C}_{c,d}(\mathbb{F}_q) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \,|\, x^2 - dy^2 = c\right\}.$$

Considering as identity any point $(a, b) \in \mathcal{C}_{c,d}(\mathbb{F}_q)$, the Brahmagupta product can be generalized obtaining $\otimes_{a,b,c,d}$.

$$(x_1, y_1) \otimes_{a,b,c,d} (x_2, y_2) = \frac{1}{c}(a, -b) \otimes_d (x_1, y_1) \otimes_d (x_2, y_2). \quad (4)$$

The inverse of a point (x, y) becomes the point

$$\frac{1}{c}(a, b) \otimes_d (a, b) \otimes_d (x, -y) \quad (5)$$

Generalized Pell hyperbolas

The equation of the Pell hyperbola is a particular case of the canonical form of hyperbolas and ellipses that, over a finite field, is given by

$$\mathcal{C}_{c,d}(\mathbb{F}_q) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \,|\, x^2 - dy^2 = c\right\}.$$

Considering as identity any point $(a, b) \in \mathcal{C}_{c,d}(\mathbb{F}_q)$, the Brahmagupta product can be generalized obtaining $\otimes_{a,b,c,d}$.

$$(x_1, y_1) \otimes_{a,b,c,d} (x_2, y_2) = \frac{1}{c}(a, -b) \otimes_d (x_1, y_1) \otimes_d (x_2, y_2). \quad (4)$$

The inverse of a point (x, y) becomes the point

$$\frac{1}{c}(a, b) \otimes_d (a, b) \otimes_d (x, -y) \quad (5)$$

$\left(\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}\right)$ is a group.

Generalized Pell hyperbolas

Theorem (A., Dutto, Murru)

Given $c, d \in \mathbb{F}_q^\times$ and a point $(a, b) \in \mathcal{C}_{c,d}(\mathbb{F}_q)$, the following map is a group isomorphism

$$\begin{aligned} \tau_{c,d}^{a,b} : \left(\mathcal{C}_d(\mathbb{F}_q), \otimes_d\right) &\xrightarrow{\sim} \left(\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}\right), \\ (x, y) &\longmapsto (a, b) \otimes_d (x, y). \end{aligned}$$

Its inverse is

$$\begin{aligned} (\tau_{c,d}^{a,b})^{-1} : \left(\mathcal{C}_{c,d}, \otimes_{a,b,c,d}\right) &\xrightarrow{\sim} \left(\mathcal{C}_d, \otimes_d\right), \\ (x, y) &\longmapsto (1, 0) \otimes_{a,b,c,d} (x, y). \end{aligned}$$

Generalized Pell hyperbolas

The explicit isomorphism between two generalized Pell hyperbolas with same parameter d is

$$\begin{aligned} (\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}) &\xrightarrow{\sim} (\mathcal{C}_{c',d}(\mathbb{F}_q), \otimes_{a',b',c',d}), \\ (x, y) &\longmapsto (a', b') \otimes_{a,b,c,d} (x, y). \end{aligned} \tag{6}$$

Generalized Pell hyperbolas

The explicit isomorphism between two generalized Pell hyperbolas with same parameter d is

$$\begin{aligned}\left(\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}\right) &\xrightarrow{\sim} \left(\mathcal{C}_{c',d}(\mathbb{F}_q), \otimes_{a',b',c',d}\right),\\ (x,y) &\longmapsto (a',b') \otimes_{a,b,c,d} (x,y).\end{aligned} \tag{6}$$

Whereas, if $\left(\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}\right)$ and $\left(\mathcal{C}_{c',d'}, \otimes_{a',b',c'd'}\right)$ with $\chi_q(d) = \chi_q(d')$ and $d' = ds^2$, then the group isomorphism between the two generalized Pell hyperbolas given explicitly by

$$\tau_{c',d'}^{a',b'} \circ \delta_{d,d'} \circ (\tau_{c,d}^{a,b})^{-1}(x,y) = \frac{1}{c}\big(a'(ax - dby) + d'b'(ay - bx)/s, \\ a'(ay - bx)/s + b'(ax - dby)\big).$$

Table of Contents

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

Let us consider the quotient

$$\mathcal{R}_{d,q} = \mathbb{F}_q[t]/(t^2 - d) = \left\{x + ty \,|\, x, y \in \mathbb{F}_q,\ t^2 = d\right\}.$$

For any two elements $x_1 + ty_1, x_2 + ty_2 \in \mathcal{R}_{d,q}$, the product naturally induced from the quotient is

$$(x_1 + ty_1)(x_2 + ty_2) = (x_1x_2 + dy_1y_2) + t(x_1y_2 + y_1x_2),$$

which is essentially the classic Brahmagupta product, so that in the following we will use the notation $\otimes_d$ adopted with the Pell hyperbola.

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

The invertible elements of $\mathcal{R}_{d,q}$ with respect to $\otimes_d$ indicated as $\mathcal{R}_{d,q}^{\otimes_d}$, may be:

1. if $d \in \mathbb{F}_q^{\times}$ is a non–square, then

$$\mathcal{R}_{d,q}^{\otimes_d} = \mathcal{R}_{d,q} \setminus \{0\};$$

2. if $d \in \mathbb{F}_q^{\times}$ is a square and $s \in \mathbb{F}^{\times}$ is a square root of d, then

$$\mathcal{R}_{d,q}^{\otimes_d} = \mathcal{R}_{d,q} \setminus \{0, \pm sy + yt \,|\, y \in \mathbb{F}_q\}.$$

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

The invertible elements of $\mathcal{R}_{d,q}$ with respect to $\otimes_d$ indicated as $\mathcal{R}_{d,q}^{\otimes_d}$, may be:

1. if $d \in \mathbb{F}_q^\times$ is a non–square, then

$$\mathcal{R}_{d,q}^{\otimes_d} = \mathcal{R}_{d,q} \setminus \{0\};$$

2. if $d \in \mathbb{F}_q^\times$ is a square and $s \in \mathbb{F}^\times$ is a square root of d, then

$$\mathcal{R}_{d,q}^{\otimes_d} = \mathcal{R}_{d,q} \setminus \{0, \pm sy + yt \,|\, y \in \mathbb{F}_q\}.$$

Thus, we define $\mathbb{P}_{d,q} = \mathcal{R}_{d,q}^{\otimes_d} / \mathbb{F}_q^\times$.

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

$$\mathbb{P}_{d,q} = \begin{cases} \{[m+t] \mid m \in \mathbb{F}_q\} \cup \{[1]\}, & \text{if } d \text{ is a non–square,} \\ \{[m+t] \mid m \in \mathbb{F}_q \setminus \{\pm s\}\} \cup \{[1]\}, & \text{otherwise} \end{cases}$$
$$\sim \begin{cases} \mathbb{F}_q \cup \{\alpha\}, & \text{if } d \text{ is a non–square,} \\ \mathbb{F}_q \setminus \{\pm s\} \cup \{\alpha\}, & \text{otherwise.} \end{cases} \tag{7}$$

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

$$\mathbb{P}_{d,q} = \begin{cases} \{[m+t] \mid m \in \mathbb{F}_q\} \cup \{[1]\}, & \text{if } d \text{ is a non–square,} \\ \{[m+t] \mid m \in \mathbb{F}_q \setminus \{\pm s\}\} \cup \{[1]\}, & \text{otherwise} \end{cases}$$
$$\sim \begin{cases} \mathbb{F}_q \cup \{\alpha\}, & \text{if } d \text{ is a non–square,} \\ \mathbb{F}_q \setminus \{\pm s\} \cup \{\alpha\}, & \text{otherwise.} \end{cases} \tag{7}$$

The operation $\otimes_d$ between canonical representatives in $\mathbb{P}_{d,q}$ is

$$m_1 \otimes_d m_2 = \begin{cases} m_1, & \text{if } m_2 = \alpha, \\ m_2, & \text{if } m_1 = \alpha, \\ \frac{m_1 m_2 + d}{m_1 + m_2}, & \text{if } m_1 + m_2 \neq 0, \\ \alpha, & \text{otherwise.} \end{cases} \tag{8}$$

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

Considering the canonical representatives in $\mathbb{P}_{d,q}$, the group isomorphism is

$$\phi_d : (\mathbb{P}_{d,q}, \otimes_d) \xrightarrow{\sim} (\mathcal{C}_d(\mathbb{F}_q), \otimes_d),$$

$$m \longmapsto \begin{cases} \left(\frac{m^2+d}{m^2-d}, \frac{2m}{m^2-d}\right), & \text{if } m \neq \alpha, \\ (1,0), & \text{otherwise,} \end{cases}$$

$$\phi_d^{-1} : (\mathcal{C}_d(\mathbb{F}_q), \otimes_d) \xrightarrow{\sim} (\mathbb{P}_{d,q}, \otimes_d),$$

$$(x,y) \longmapsto \begin{cases} (x+1)/y, & \text{if } y \neq 0, \\ 0, & \text{if } (x,y) = (-1,0), \\ \alpha, & \text{if } (x,y) = (1,0). \end{cases}$$

Parameterization for $\mathcal{C}_d(\mathbb{F}_q)$

Considering the canonical representatives in $\mathbb{P}_{d,q}$, the group isomorphism is

$$\phi_d : (\mathbb{P}_{d,q}, \otimes_d) \xrightarrow{\sim} (\mathcal{C}_d(\mathbb{F}_q), \otimes_d),$$

$$m \longmapsto \begin{cases} \left(\frac{m^2+d}{m^2-d}, \frac{2m}{m^2-d}\right), & \text{if } m \neq \alpha, \\ (1,0), & \text{otherwise,} \end{cases}$$

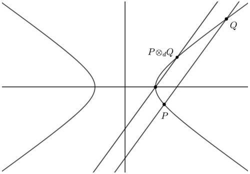
$$\phi_d^{-1} : (\mathcal{C}_d(\mathbb{F}_q), \otimes_d) \xrightarrow{\sim} (\mathbb{P}_{d,q}, \otimes_d),$$

$$(x,y) \longmapsto \begin{cases} (x+1)/y, & \text{if } y \neq 0, \\ 0, & \text{if } (x,y) = (-1,0), \\ \alpha, & \text{if } (x,y) = (1,0). \end{cases}$$

Thus, the parameters in $\mathbb{P}_{d,q}$ of the Pell hyperbola can be obtained considering the lines $y = \frac{1}{m}(x+1)$ for m varying in $\mathbb{F}_q$ or $m = \alpha$.

A geometric interpretation

Given two points P and Q of the Pell Hyperbola, their product $P \otimes_d Q$ is obtaining by considering the intersection between the hyperbola and the line through the identity point $(1, 0)$ and parallel to the line through P and Q.



Geometric interpretation of the Brahmagupta product.

Table of Contents

Three different ElGamal like schemes

Since the group of the Pell hyperbola is cyclic, it can be applied in Public-Key Encryption (PKE) schemes where the security is based on the Discrete Logarithm Problem (DLP), such as the ElGamal PKE scheme.

Three different ElGamal like schemes

Since the group of the Pell hyperbola is cyclic, it can be applied in Public-Key Encryption (PKE) schemes where the security is based on the Discrete Logarithm Problem (DLP), such as the ElGamal PKE scheme.

In particular, three schemes have been studied

- ElGamal with Pell hyperbola,
- ElGamal with the parameterization,
- ElGamal with the obtained isomorphisms.

Classic ElGamal cryptosystem

$\texttt{KeyGen}(n)$:

1: $q \leftarrow_{\$} \{0,1\}^n$ order of $(G, \cdot)$
2: g generator of $(G, \cdot)$
3: $sk \leftarrow_{\$} \{2, \ldots, q-1\}$
4: $h = g^{sk} \in G$
5: $pk = (G, g, h)$
6: **return** pk, sk

$\texttt{Encrypt}(msg, pk)$:

1: $r \leftarrow_{\$} \{1, \ldots, q-1\}$
2: $e = h^r \in G$
3: $c_1 = g^r \in G$
4: $c_2 = msg \cdot e \in G$
5: **return** c_1, c_2

$\texttt{Decrypt}(c_1, c_2, pk, sk)$:

1: $d = c_1^{sk} \in G$
2: $msg = c_2 \cdot d^{-1} \in G$
3: **return** msg

Classic ElGamal cryptosystem

$\texttt{KeyGen}(n)$:

1: $q \leftarrow_{\$} \{0,1\}^n$ order of $(G, \cdot)$
2: g generator of $(G, \cdot)$
3: $sk \leftarrow_{\$} \{2, \dots, q-1\}$
4: $h = g^{sk} \in G$
5: $pk = (G, g, h)$
6: **return** pk, sk

$\texttt{Encrypt}(msg, pk)$:

1: $r \leftarrow_{\$} \{1, \dots, q-1\}$
2: $e = h^r \in G$
3: $c_1 = g^r \in G$
4: $c_2 = msg \cdot e \in G$
5: **return** c_1, c_2

$\texttt{Decrypt}(c_1, c_2, pk, sk)$:

1: $d = c_1^{sk} \in G$
2: $msg = c_2 \cdot d^{-1} \in G$
3: **return** msg

The verification of decryption phase:

$$c_2 \cdot d^{-1} = msg \cdot e \cdot d^{-1} = msg \cdot h^r \cdot c_1^{-sk} =$$
$$= msg \cdot h^r \cdot g^{-r \cdot sk} = msg \cdot h^r \cdot h^{-r} = msg$$

ElGamal with two Pell hyperbolas

`KeyGen`(n):

1: $q \leftarrow_{\$} \{0,1\}^n$ power of a prime
2: $d \in \mathbb{F}_q$ minimum with $\chi_q(d) = -1$
3: $g \leftarrow_{\$} \mathbb{P}_{d,q}$ of order $q+1$
4: $sk \leftarrow_{\$} \{2, \ldots, q\}$
5: $h = g^{\otimes_d sk} \in \mathbb{P}_{d,q}$
6: $pk = (q, d, g, h)$
7: **return** pk, sk

The key generation is standard, except for the smallest non-square d taken in step 2, which is used for the exponentiation in step 5 and then included in the public key.

ElGamal with two Pell hyperbolas

Encrypt(msg, pk):
Require: $msg \leq (q-1)^2$
1: $(x, y) \leftarrow msg$
2: $d' = \frac{x^2-1}{y^2} \in \mathbb{F}_q$ with $\chi_q(d') = -1$
3: $m = \frac{x+1}{y} \in \mathbb{P}_{d',q}$
4: $r \leftarrow_\$ \{2, \ldots, q\}$
5: $s = \sqrt{d'/d} \in \mathbb{F}_q$
6: $c_1 = (gs)^{\otimes_{d'} r} \in \mathbb{P}_{d',q}$
7: $c_2 = (hs)^{\otimes_{d'} r} \otimes_{d'} m \in \mathbb{P}_{d',q}$
8: **return** c_1, c_2, d'

Decrypt(c_1, c_2, d', pk, sk):
1: $m = (-c_1^{\otimes_{d'} sk}) \otimes_{d'} c_2$
2: $msg \leftarrow \left(\frac{m^2+d'}{m^2-d'}, \frac{2m}{m^2-d'}\right)$
3: **return** msg

Step 2 searches for a quadratic non-residue $d' \in \mathbb{F}_q$ such that $(x, y) \in \mathcal{C}_{d'}(\mathbb{F}_q)$. Then, in step 3, the parameter m related to the point is obtained through the parameterization. Now, since the public key contains parameters of points of $\mathcal{C}_d(\mathbb{F}_q)$, the isomorphism between Pell hyperbolas $\delta_{d,d'}$ is exploited.

ElGamal with two Pell hyperbolas

Encrypt(msg, pk):

Require: $msg \leq (q-1)^2$

1: $(x, y) \leftarrow msg$
2: $d' = \frac{x^2-1}{y^2} \in \mathbb{F}_q$ with $\chi_q(d') = -1$
3: $m = \frac{x+1}{y} \in \mathbb{P}_{d',q}$
4: $r \leftarrow_{\$} \{2, \ldots, q\}$
5: $s = \sqrt{d'/d} \in \mathbb{F}_q$
6: $c_1 = (gs)^{\otimes_{d'} r} \in \mathbb{P}_{d',q}$
7: $c_2 = (hs)^{\otimes_{d'} r} \otimes_{d'} m \in \mathbb{P}_{d',q}$
8: **return** c_1, c_2, d'

Decrypt(c_1, c_2, d', pk, sk):

1: $m = (-c_1^{\otimes_{d'} sk}) \otimes_{d'} c_2$
2: $msg \leftarrow \left(\frac{m^2+d'}{m^2-d'}, \frac{2m}{m^2-d'}\right)$
3: **return** msg

Step 2 searches for a quadratic non-residue $d' \in \mathbb{F}_q$ such that $(x, y) \in \mathcal{C}_{d'}(\mathbb{F}_q)$. Then, in step 3, the parameter m related to the point is obtained through the parameterization. Now, since the public key contains parameters of points of $\mathcal{C}_d(\mathbb{F}_q)$, the isomorphism between Pell hyperbolas $\delta_{d,d'}$ is exploited.

In the decryption the message is retrieved from the point related to the obtained parameter (step 2).

Table of Contents

Security

The security strength for the DLP–based cryptosystems relies on the adopted cyclic group. Since in the introduced scheme the parameter $d \in \mathbb{F}_q$ is a non-square, there is an explicit group isomorphism between $\left(\mathcal{C}_d(\mathbb{F}_q), \otimes_d\right)$ and the multiplicative subgroup $G \subset \mathbb{F}_{q^2}^{\times}$ of order $q+1$. This is true also for $\left(\mathbb{P}_{d,q}, \otimes_d\right)$.

The DLP related to the Pell hyperbola can be reduced to that in a finite field that, with respect to the standard security strengths for ElGamal in Finite Field Cryptography (FFC), has halved size of q.

Sec.	FFC	PCI
80	1024	512
112	2048	1024
128	3072	1536
192	7680	3840
256	15360	7680

Field size in bits for FFC and PCI depending on the cyclic group and the classical security strength in bits.

Data–size

Data–size in bits for ElGamal with FFC and PCI depending on the size n of q and for 80 bits of security.

Formulation	par	pk	sk	msg	c_1, c_2
FFC	$2n$	n	n	n	$2n$
	2048	1024	1024	1024	2048
PCI	$2n$	n	n	$2n$	n
	1024	512	512	1024	1536

Performance

Sec.	Alg.	FFC	PCI
80	Gen	0.011079	0.007524
	Enc	0.022311	0.028152
	Dec	0.012183	0.010203
112	Gen	0.074718	0.038527
	Enc	0.149400	0.164122
	Dec	0.077622	0.057106
128	Gen	0.233983	0.112873
	Enc	0.467730	0.496599
	Dec	0.239429	0.171190
192	Gen	3.188959	1.372381
	Enc	6.372422	6.291258
	Dec	3.218019	2.103753
256	Gen	22.874051	9.519104
	Enc	45.766954	42.658508
	Dec	22.981310	14.464945

Average times in seconds for 10 random instances of fixed msg length, depending on the security strength.

References

- E. Barker, SP 800-57 Part 1: Recommendation for Key Management, NIST, 2020.
- A. J. Menezes, S. A. Vanstone, *A Note on Cyclic Groups, Finite Fields, and the Discrete Logarithm Problem*, Applicable Algebra in Engineering, Communication and Computing, Vol. 3, 67–74, 1992.
- A. Weil, *Number theory: an approach through history.* Boston: Birkhauser, 1984.
- G. Alecci, S. Dutto, N. Murru, *Pell Hyperbolas in DLP-based cryptosystem*, Finite Fields and Their Applications 84, 102112.

Thank you for your attention!

gessica.alecci@polito.it