



POLITECNICO
DI TORINO

DISMA

Dipartimento di
Scienze Matematiche
G. L. Lagrange

ECCELLENZA 2018 · 2022

A study on the use of Pell hyperbolas in DLP-based cryptosystems

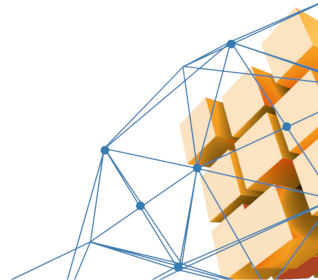
Based on a joint work with S. Dutto and N. Murru

Gessica Alecci

Politecnico di Torino, Disma

May 17, 2022

Seminario DeCifris



Summary

Part I

- Generalization of the group structure of Pell hyperbolas
- Parameterization of Pell hyperbolas
- ElGamal scheme

Summary

Part I

- Generalization of the group structure of Pell hyperbolas
- Parameterization of Pell hyperbolas
- ElGamal scheme

Part II

- ElGamal PKE schemes based on Pell hyperbolas
- Numerical results
- Conclusions

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

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

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

$$C_d(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid x^2 - dy^2 = 1\}. \tag{2}$$

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 $d = 92$ [3].

He discovered that given two solutions of (1), namely $(x_1, y_1), (x_2, y_2)$, 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 $d = 92$ [3].

He discovered that given two solutions of (1), namely $(x_1, y_1), (x_2, y_2)$, 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 or power of an 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 or power of an 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 with same value of $\chi_q(d)$ are isomorphic. In particular, if $\chi_q(d) = \chi_q(d')$, then $d' = ds^2$ for some $s \in \mathbb{F}_q$ and the group isomorphism is

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

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

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

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

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

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

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

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

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

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

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

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

Generalized Pell hyperbolas

Theorem

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:

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

The inverse group homomorphism is

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

Generalized Pell hyperbolas

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

$$\begin{aligned} (\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}) &\xrightarrow{\sim} (\mathcal{C}_{c',d}(\mathbb{F}_q), \otimes_{a',b',c',d}), \\ (x, y) &\longmapsto (a', b') \otimes_{a,b,c,d} (x, y). \end{aligned} \tag{5}$$

Generalized Pell hyperbolas

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

$$\begin{aligned} (\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d}) &\xrightarrow{\sim} (\mathcal{C}_{c',d}(\mathbb{F}_q), \otimes_{a',b',c',d}), \\ (x, y) &\longmapsto (a', b') \otimes_{a,b,c,d} (x, y). \end{aligned} \quad (5)$$

Whereas, if $(\mathcal{C}_{c,d}(\mathbb{F}_q), \otimes_{a,b,c,d})$ and $(\mathcal{C}_{c',d'}, \otimes_{a',b',c',d'})$ with $\chi_q(d) = \chi_q(d')$ and $d' = ds^2$, then composing $(\tau_{c,d}^{a,b})^{-1}$, $\delta_{d,d'}$ and $\tau_{c',d'}^{a',b'}$ results in a group isomorphism between the two generalized Pell hyperbolas given explicitly by

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

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

Let us consider the quotient ring

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

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 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

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

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

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

$$\begin{aligned} \mathbb{P}_{d,q} &= \begin{cases} \{[m+t] \mid m \in \mathbb{F}_q\} \cup \{[1]\}, & \text{if } d \text{ is a non-square,} \\ \{[m+t] \mid m \in \mathbb{F}_q \setminus \{\pm s\}\} \cup \{[1]\}, & \text{otherwise} \end{cases} \\ &\sim \begin{cases} \mathbb{F}_q \cup \{\alpha\}, & \text{if } d \text{ is a non-square,} \\ \mathbb{F}_q \setminus \{\pm s\} \cup \{\alpha\}, & \text{otherwise.} \end{cases} \end{aligned} \quad (6)$$

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

$$\begin{aligned} \mathbb{P}_{d,q} &= \begin{cases} \{[m+t] \mid m \in \mathbb{F}_q\} \cup \{[1]\}, & \text{if } d \text{ is a non-square,} \\ \{[m+t] \mid m \in \mathbb{F}_q \setminus \{\pm s\}\} \cup \{[1]\}, & \text{otherwise} \end{cases} \\ &\sim \begin{cases} \mathbb{F}_q \cup \{\alpha\}, & \text{if } d \text{ is a non-square,} \\ \mathbb{F}_q \setminus \{\pm s\} \cup \{\alpha\}, & \text{otherwise.} \end{cases} \end{aligned} \quad (6)$$

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

$$m_1 \otimes_d m_2 = \begin{cases} m_1, & \text{if } m_2 = \alpha, \\ m_2, & \text{if } m_1 = \alpha, \\ \frac{m_1 m_2 + d}{m_1 + m_2}, & \text{if } m_1 + m_2 \neq 0, \\ \alpha, & \text{otherwise.} \end{cases} \quad (7)$$

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

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

$$\begin{aligned}\phi_d : (\mathbb{P}_{d,q}, \otimes_d) &\xrightarrow{\sim} (\mathcal{C}_d(\mathbb{F}_q), \otimes_d), \\ m &\longmapsto \begin{cases} \left(\frac{m^2+d}{m^2-d}, \frac{2m}{m^2-d} \right), & \text{if } m \neq \alpha, \\ (1, 0), & \text{otherwise,} \end{cases} \\ \phi_d^{-1} : (\mathcal{C}_d(\mathbb{F}_q), \otimes_d) &\xrightarrow{\sim} (\mathbb{P}_{d,q}, \otimes_d), \\ (x, y) &\longmapsto \begin{cases} (x+1)/y, & \text{if } y \neq 0, \\ 0, & \text{if } (x, y) = (-1, 0), \\ \alpha, & \text{if } (x, y) = (1, 0). \end{cases}\end{aligned}$$

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

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

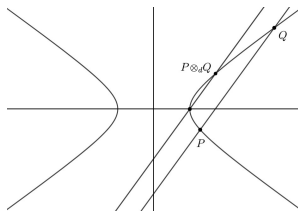
$$\begin{aligned}\phi_d : (\mathbb{P}_{d,q}, \otimes_d) &\xrightarrow{\sim} (\mathcal{C}_d(\mathbb{F}_q), \otimes_d), \\ m &\longmapsto \begin{cases} \left(\frac{m^2+d}{m^2-d}, \frac{2m}{m^2-d} \right), & \text{if } m \neq \alpha, \\ (1, 0), & \text{otherwise,} \end{cases} \\ \phi_d^{-1} : (\mathcal{C}_d(\mathbb{F}_q), \otimes_d) &\xrightarrow{\sim} (\mathbb{P}_{d,q}, \otimes_d), \\ (x, y) &\longmapsto \begin{cases} (x+1)/y, & \text{if } y \neq 0, \\ 0, & \text{if } (x, y) = (-1, 0), \\ \alpha, & \text{if } (x, y) = (1, 0). \end{cases}\end{aligned}$$

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 $m = \alpha$.

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

A geometric interpretation

From a geometrical point of view, the parameter m of a point (x, y) is the slope of the line through (x, y) and $(-1, 0)$ written considering x variable with y . Given two points P and Q of the Pell Hyperbola, their product $P \otimes_d Q$ is obtained 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.

Exponentiation with Rédei rational functions

The product on the parameters can be evaluated efficiently with the Rédei rational functions, in particular

$$m^{\otimes_d e} = Q_e(m, d),$$

with

$$Q_n(m, d) = \frac{A_n(m, d)}{B_n(m, d)},$$

where A_n, B_n are two sequences of polynomials obtained by the powers

$$(m + \sqrt{d})^n = A_n(m, d) + B_n(m, d)\sqrt{d}.$$

$A_n(m, d)$ and $B_n(m, d)$ can be evaluated by the modified More algorithm.

Public-key encryption with the Pell hyperbola

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.

Public-key encryption with the Pell hyperbola

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

KeyGen(n):

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

Encrypt(m, pk):

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

Decrypt(c_1, c_2, pk, sk):

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

ElGamal with the cyclic group $(\mathcal{C}_d(\mathbb{Z}_q), \otimes_d)$

KeyGen(n):

- 1: $q \leftarrow_{\$} \{0, 1\}^n$ power of a prime
- 2: $d \leftarrow_{\$} \mathbb{F}_q$ with $\chi_q(d) = -1$
- 3: $G \leftarrow_{\$} \mathcal{C}_d(\mathbb{F}_q)$ of order $q + 1$
- 4: $sk \leftarrow_{\$} \{2, \dots, q\}$
- 5: $H = G^{\otimes_d sk} \in \mathcal{C}_d(\mathbb{F}_q)$
- 6: $pk = (q, d, G, H)$
- 7: **return** pk, sk

Let q be a power of a prime n bits long and after choosing $d \in \mathbb{F}_q$, a random generator G of $\mathcal{C}_d(\mathbb{F}_q)$ is taken. Then the algorithm proceeds by taking a random exponent sk (step 4) and obtaining a public point $H \in \mathcal{C}_d(\mathbb{F}_q)$.

ElGamal with the cyclic group $(\mathcal{C}_d(\mathbb{Z}_q), \otimes_d)$

Encrypt(msg, pk):

Require: $msg < q$

- 1: $y \leftarrow msg$
- 2: $x = \sqrt{1 + d y^2} \in \mathbb{F}_q$
- 3: $r \leftarrow_{\$} \{2, \dots, q\}$
- 4: $C_1 = G^{\otimes_d r} \in \mathcal{C}_d(\mathbb{F}_q)$
- 5: $C_2 = H^{\otimes_d r} \otimes_d (x, y) \in \mathcal{C}_d(\mathbb{F}_q)$
- 6: **return** C_1, C_2

Decrypt(C_1, C_2, pk, sk):

- 1: $(x, y) = (C_1^{\otimes_d sk})^{-1} \otimes_d C_2 \in \mathcal{C}_d(\mathbb{F}_q)$
- 2: $msg \leftarrow y$
- 3: **return** msg

The message determines the y coordinate of a point, and the corresponding x is chosen under the condition $(x, y) \in \mathcal{C}_d(\mathbb{F}_q)$. After taking a random exponent r , C_1 and C_2 are obtained through exponentiations with the Brahmagupta product.

ElGamal with the cyclic group $(\mathcal{C}_d(\mathbb{Z}_q), \otimes_d)$

Encrypt(msg, pk):

Require: $msg < q$

- 1: $y \leftarrow msg$
- 2: $x = \sqrt{1 + d y^2} \in \mathbb{F}_q$
- 3: $r \leftarrow_{\$} \{2, \dots, q\}$
- 4: $C_1 = G^{\otimes_d r} \in \mathcal{C}_d(\mathbb{F}_q)$
- 5: $C_2 = H^{\otimes_d r} \otimes_d (x, y) \in \mathcal{C}_d(\mathbb{F}_q)$
- 6: **return** C_1, C_2

Decrypt(C_1, C_2, pk, sk):

- 1: $(x, y) = (C_1^{\otimes_d sk})^{-1} \otimes_d C_2 \in \mathcal{C}_d(\mathbb{F}_q)$
- 2: $msg \leftarrow y$
- 3: **return** msg

The message determines the y coordinate of a point, and the corresponding x is chosen under the condition $(x, y) \in \mathcal{C}_d(\mathbb{F}_q)$. After taking a random exponent r , C_1 and C_2 are obtained through exponentiations with the Brahmagupta product.

During the decryption, the point (x, y) is retrieved as the Brahmagupta product of the inverse of $C_1^{\otimes_d sk}$ with C_2 .

EIGamal with the parameterization $(\mathbb{P}_{d,q}, \otimes_d)$

KeyGen(n):

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

A random non-square $d \in \mathbb{F}_q$ is taken. After choosing a generator $g \in \mathbb{P}_{d,q}$ and a random exponent sk , a parameter $h = g^{\otimes_d sk}$ is evaluated in step 5 with the modified More algorithm.

ElGamal with the parameterization $(\mathbb{P}_{d,q}, \otimes_d)$

Encrypt(msg, pk):

Require: $msg < q$

- 1: $r \leftarrow_{\$} \{2, \dots, q\}$
- 2: $c_1 = g^{\otimes_d r} \in \mathbb{P}_{d,q}$
- 3: $c_2 = h^{\otimes_d r} \otimes_d msg \in \mathbb{P}_{d,q}$
- 4: **return** c_1, c_2

Decrypt(c_1, c_2, pk, sk):

- 1: $msg = -c_1^{\otimes_d sk} \otimes_d c_2 \in \mathbb{P}_{d,q}$
- 2: **return** msg

The encryption considers the message as a parameter $msg \in \mathbb{P}_{d,q}$. Step 1 takes a random exponent r , which is used in steps 2-3 to obtain the parameters c_1 and c_2 . The ciphertext requires half of the space than in the previous algorithm.

ElGamal with the parameterization $(\mathbb{P}_{d,q}, \otimes_d)$

Encrypt(msg, pk):

Require: $msg < q$

- 1: $r \leftarrow_{\$} \{2, \dots, q\}$
- 2: $c_1 = g^{\otimes_d r} \in \mathbb{P}_{d,q}$
- 3: $c_2 = h^{\otimes_d r} \otimes_d msg \in \mathbb{P}_{d,q}$
- 4: **return** c_1, c_2

Decrypt(c_1, c_2, pk, sk):

- 1: $msg = -c_1^{\otimes_d sk} \otimes_d c_2 \in \mathbb{P}_{d,q}$
- 2: **return** msg

The encryption considers the message as a parameter $msg \in \mathbb{P}_{d,q}$. Step 1 takes a random exponent r , which is used in steps 2-3 to obtain the parameters c_1 and c_2 . The ciphertext requires half of the space than in the previous algorithm.

The decryption retrieves the message as the parameter product between the inverse of $c_1^{\otimes_d sk}$ (which is simply its opposite) and c_2 .

EIGamal 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: $sk \leftarrow_{\$} \{2, \dots, q\}$
- 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 analogous to the previous one, except for the smallest non-square d taken in step 3, which is used for the exponentiation in step 6 and then included in the public key.

EIGamal 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: $r \leftarrow_{\$} \{2, \dots, q\}$
- 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.

EIGamal 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: $r \leftarrow_{\$} \{2, \dots, q\}$
- 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, analogous to the previous case, the message must be retrieved from the point related to the obtained parameter (step 2).

Numerical results

Security

Since in all the introduced schemes the parameter $d \in \mathbb{F}_q$ is a non-square, there is an explicit group isomorphism between $(\mathcal{C}_d(\mathbb{F}_q), \otimes_d)$ and the multiplicative subgroup $G \subset \mathbb{F}_{q^2}^\times$ of order $q + 1$ [2], this is true also for $(\mathbb{P}_{d,q}, \otimes_d)$ through ϕ_d . Thus, the DLP related to the Pell hyperbola can be reduced to that in a finite field that, with respect to the standard security strengths from [1] for ElGamal in Finite Field Cryptography (FFC), has halved size of q .

Numerical results

Security

Sec.	FFC	$\mathcal{C}_d(\mathbb{F}_q)$	$\mathbb{P}_{d,q}$	$\phi_{d'}, \delta_{d,d'}$
80	1024	512	512	512
112	2048	1024	1024	1024
128	3072	1536	1536	1536
192	7680	3840	3840	3840
256	15360	7680	7680	7680

Field size in bits for different DLP-based cryptosystems depending on the cyclic group and the classic security strength in bits.

Numerical results

Data-size

Data-size in bits for ElGamal with FFC, $\mathcal{C}_d(\mathbb{F}_q)$, $\mathbb{P}_{d,q}$ and the alternative formulation, 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

Numerical results

Data-size

Data-size in bits for ElGamal with FFC, $\mathcal{C}_d(\mathbb{F}_q)$, $\mathbb{P}_{d,q}$ and the alternative formulation, 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
$\mathcal{C}_d(\mathbb{F}_q)$	$4n$	$2n$	n	n	$4n$
	2048	1024	512	512	2048

Numerical results

Data-size

Data-size in bits for ElGamal with FFC, $\mathcal{C}_d(\mathbb{F}_q)$, $\mathbb{P}_{d,q}$ and the alternative formulation, 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
$\mathcal{C}_d(\mathbb{F}_q)$	$4n$	$2n$	n	n	$4n$
	2048	1024	512	512	2048
$\mathbb{P}_{d,q}$	$3n$	n	n	n	$2n$
	1536	512	512	512	1024

Numerical results

Data-size

Data-size in bits for ElGamal with FFC, $\mathcal{C}_d(\mathbb{F}_q)$, $\mathbb{P}_{d,q}$ and the alternative formulation, depending on the size n of q and for 80 bits of security.

Formulation	par	pk	sk	msg	c_1, c_2
FFC	$2n$ 2048	n 1024	n 1024	n 1024	$2n$ 2048
$\mathcal{C}_d(\mathbb{F}_q)$	$4n$ 2048	$2n$ 1024	n 512	n 512	$4n$ 2048
$\mathbb{P}_{d,q}$	$3n$ 1536	n 512	n 512	n 512	$2n$ 1024
$\phi_d, \delta_{d,d'}$	$2n$ 1024	n 512	n 512	$2n$ 1024	$3n$ 1536

Numerical results

Performance

Sec.	Alg.	FFC	$C_d(\mathbb{F}_q) \times 2$	$\mathbb{P}_{d,q} \times 2$	$\phi_d, \delta_{d,d'}$
80	Gen	0.011079	0.011713	0.009781	0.007524
	Enc	0.022311	0.059983	0.040459	0.028152
	Dec	0.012183	0.023631	0.020472	0.010203
112	Gen	0.074718	0.073778	0.056865	0.038527
	Enc	0.149400	0.364686	0.229299	0.164122
	Dec	0.077622	0.148194	0.115962	0.057106
128	Gen	0.233983	0.227347	0.171958	0.112873
	Enc	0.467730	1.103675	0.689103	0.496599
	Dec	0.239429	0.454805	0.347872	0.171190
192	Gen	3.188959	2.811594	2.127992	1.372381
	Enc	6.372422	13.791595	8.525471	6.291258
	Dec	3.218019	5.630895	4.273549	2.103753
256	Gen	22.874051	18.155630	13.841428	9.519104
	Enc	45.766954	87.457496	55.563741	42.658508
	Dec	22.981310	36.287580	27.792128	14.464945

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

Numerical results

Performance





Sec.	Alg.	FFC	$\phi_d, \delta_{d,d'}$
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 for fixed msg length, depending on the security strength.

Conclusion

The first two new cryptosystems remain interesting from the theoretical point of view, but are not competitive in practice. On the other hand, the new ElGamal formulation that exploits the new group isomorphisms $\phi_d, \delta_{d,d'}$ seems to be a very powerful alternative for DLP-based cryptosystems because of the big advantage in key and ciphertext size and the comparable times with the classical ElGamal in FFC.

Bibliography

-  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.