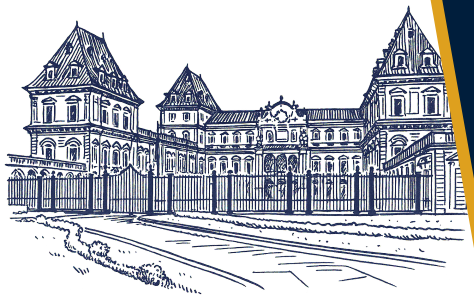
Politecnico di Torino

CrypTO
Crittografia e Teoria dei Numeri
DISMA - Politecnico di Torino



What the Pell

Cryptanalysis of degree-two Pell curves

Leonardo Errati - ITASEC 2026

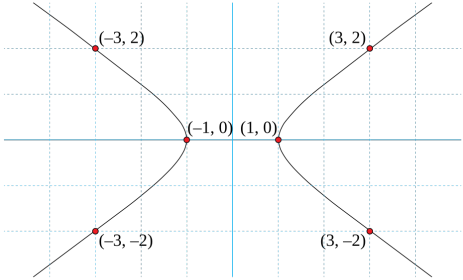
Table of Contents

Pell curves of degree two

Definition

For a fixed non-zero d in $\mathbb{F}$, the *degree-two Pell curve over* $\mathbb{F}$ *of parameter* d is the $\mathbb{F}$-variety

$$\mathcal{P}_d(\mathbb{F}) = \left\{(x, y) \in \mathbb{F} \times \mathbb{F} : x^2 - dy^2 = 1\right\}$$



$x^2 - 2y^2 = 1$

The sum of $\mathcal{A} = (x_\mathcal{A}, y_\mathcal{A})$ and $\mathcal{B} = (x_\mathcal{B}, y_\mathcal{B})$ is given by the "Brahmagupta product",

$$(x_\mathcal{A}, y_\mathcal{A}) \otimes_d (x_\mathcal{B}, y_\mathcal{B}) = (x_\mathcal{A}x_\mathcal{B} + dy_\mathcal{A}y_\mathcal{B}, x_\mathcal{A}y_\mathcal{B} + x_\mathcal{B}y_\mathcal{A})$$

Pell curves of degree two
Over $\mathbb{F}_q$

We have an alternative construction.
Consider the ring $\mathcal{R}_d = \mathbb{F}_q[W]/\langle W^2 - d \rangle$ with norm

$$N_d(x + yW) = (x + yW)(x - yW) = x^2 - dy^2$$

Lemma

1. The set $\mathcal{U}(\mathcal{R}_d) = \{f \in \mathcal{R}_d \mid N_d(f) = +1\}$ is a group.
   It inherits the operation of $\mathcal{R}_d$, polynomial multiplication modulo $W^2 - d$.
2. There is a correspondence between $\mathcal{P}_d(\mathbb{F}_q)$ and $\mathcal{U}(\mathcal{R}_d)$.

Structure Lemma [MV92]

The group $(\mathcal{P}_d(\mathbb{F}_q), \otimes_d)$ is isomorphic to a cyclic group of order $q - \chi(d)$, or more explicitly

$$(\mathcal{P}_d(\mathbb{F}_q), \otimes_d) \simeq \begin{cases} (\mathbb{F}_q^*, \cdot) & \text{if } \chi(d) = +1 \\ (U_{q+1}, \cdot) & \text{if } \chi(d) = -1 \end{cases}$$

Efficient isomorphisms

non-splitting curve: $\chi(d) = -1$

Remark that $\mathcal{P}_d(\mathbb{F}_q) \simeq \mathcal{U}(\mathcal{R}_d)$, for $\mathcal{R}_d = \mathbb{F}_q[W]/\langle W^2 - d\rangle$. The behaviour of $W^2 - d$ allows to build explicit forwards and backwards isomorphisms.

Case 1: no split.

The polynomial is irreducible, thus $\mathcal{R}_d = \mathbb{F}_q[W]/\langle W^2 - d\rangle$ is a field isomorphic to $\mathbb{F}_{q^2}$ via

$$(x, y) \mapsto x + yW$$
$$x + Wy \mapsto (x, y)$$

Here $\mathcal{U}(\mathcal{R}_d)$ is isomorphic to U_{q+1}, the unique subgroup of order $q + 1$ of $\mathbb{F}_{q^2}^*$.

Case 2: split.

The polynomial is reducible, thus $\mathcal{R}_d = \mathbb{F}_q[W]/\langle W^2 - d\rangle$ contains a quadratic residual a such that $W^2 - d = (W - a)(W + a)$, and it is isomorphic to $\mathbb{F}_q$ via

$$(x, y) \mapsto x - ay$$

Here $\mathcal{U}(\mathcal{R}_d)$ is isomorphic to $\mathbb{F}_q^*$, of order $q - 1$. The inverse isomorphism is harder to achieve.

Lemma

If $\chi(d) = +1$, the curve point corresponding to $t \in \mathbb{F}_q^*$ is

$$x = \frac{1+t^2}{2t} \quad \text{and} \quad y = \frac{1-t^2}{2at}$$

where a is one of the square roots of d.

There are two different choices for the square root of d.

$$\varphi_{a_+}^{-1} : t \mapsto \left(\frac{1+t^2}{2t}, \frac{1-t^2}{2at}\right) = (x, y)$$

$$\varphi_{a_-}^{-1} : t \mapsto \left(\frac{1+t^2}{2t}, \frac{1-t^2}{2(-a)t}\right) = \left(\frac{1+t^2}{2t}, -\frac{1-t^2}{2at}\right) = (x, -y)$$

Efficient isomorphisms

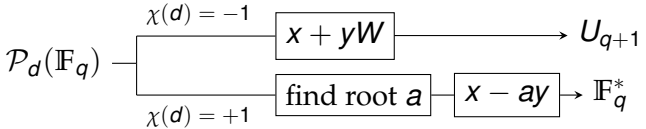


Table of Contents

CrypTO

DLOG

Consider a finite cyclic group $\mathbb{G} = \langle g \rangle$ of order n.

- Parameters: a description $(\mathbb{G}, g)$ of $\mathbb{G}$.
- Instance: an element $h \in \mathbb{G}$.
- Task: find the unique $x \in \mathbb{Z}_n$ such that $g^x = h$.

DLOG equivalence

DLOG-$\mathcal{P}$ is PPT-equivalent to DLOG-$\mathbb{F}$.

Security assumptions

. . . and more

This also holds for other assumptions. For instance,

RSA Inversion

Consider a finite cyclic group $\mathbb{G} = \langle g \rangle$ of order N.

- *Parameters:* a description $(\mathbb{G}, g)$ of $\mathbb{G}$, an e in $\mathbb{Z}_N$ such that $\gcd(e, N) = 1$.
- *Instance:* an element $x \in \mathbb{G}$.
- *Task:* find the unique $y \in \mathbb{G}$ such that $y^e = x$.

RSAI equivalence

RSAI-$\mathcal{P}$ is PPT-equivalent to RSAI-$\mathbb{F}$.

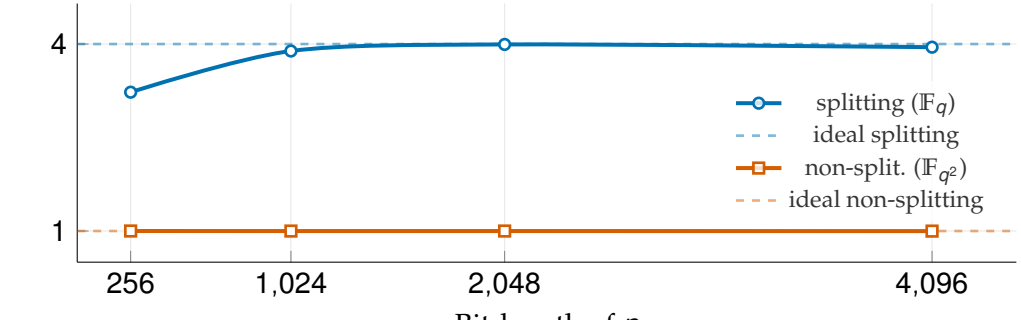
Operations in $\mathcal{P}_d(\mathbb{F}_q)$

Brahmagupta

Apply the isomorphism.

— If the curve splits, the improvement factor of isomorphic multiplication is $T_{\otimes_d}(\mathcal{P})/T_{\times}(\mathbb{F}_q) \approx 4$.

— If the curve does not split, the improvement factor of isomorphic multiplication is $T_{\otimes_d}(\mathcal{P})/T_{\times}(\mathbb{F}_{q^2}) \approx 1$.



Operations in $\mathcal{P}_d(\mathbb{F}_q)$
square-and-multiply

We can also consider Pell square-and-multiply [ADM22] and the ratio between $T_{\text{SquareMultiply}}(\mathcal{P})$ and $T_{\text{SquareMultiply}}(\mathbb{F}_q)$.

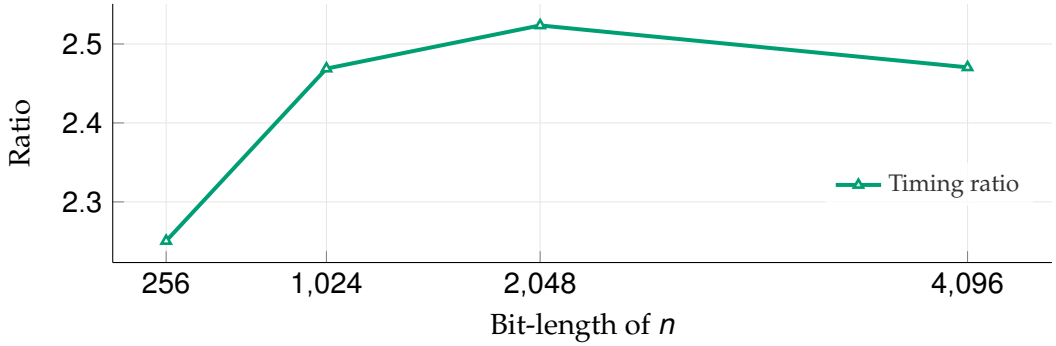


Table of Contents

Take-aways

Work-in-progress:

— Isomorphisms of curves of degree three.

— Isomorphisms of curves of degree n..?

— Adapting existing algorithms to remove Pell curves.

Destructive:

— Pell curves offer no computational or security advantages over finite fields.

— Unsuitable for DLOG, RSAI, etc (e.g., [ADM22; Pad06; MB19]).

Constructive:

— Explicit isomorphisms allow algorithms to be rewritten without them (e.g., [DM25; Bar+25], etc.)

References

[ADM22] Gessica Alecci, Simone Dutto, and Nadir Murru. *Pell hyperbolas in DLP–based cryptosystems*. 2022.

[Bar+25] Fadi Barbara et al. *BTLE: Atomic swaps with time-lock puzzles*. 2025.

[DM25] Luca Di Domenico and Nadir Murru. *Novel Performant Primality Test on a Pell's Cubic*. 2025.

[MB19] Nadir Murru and Emanuele Bellini. *A multi-factor RSA-like scheme with fast decryption*. 2019.

[MV92] Alfred J Menezes and Scott A Vanstone. *A note on cyclic groups, finite fields, and the discrete logarithm problem*. 1992.

[Pad06] Sahadeo Padhye. *A Public Key Cryptosystem Based on Pell Equation*. 2006.

Thank you!