STELLINGEN

accompanying the thesis

CRYPTOGRAPHY ON ISOGENY GRAPHS

by Lorenz Panny

---

1. In practice, the halting problem is trivial: it halts.

2. Contrary to popular opinion, nihilism is the *least* depressing philosophy of life.

3. It is extremely remarkable that cryptography running on a cheap microcontroller can (seemingly) withstand multi-billion dollar cryptanalysis. *Cryptography rearranges power: it configures who can do what, from what.* [1]

4. Heaps of unnecessary complexity are what makes computer security difficult.

5. The teaching of mathematics should focus less on the *how* and more on the *why.*

6. Using standard definitions[2]: $\forall n \in \mathbb{N},\ \bigcup\bigcup(n \times n) = n$.

7. Consider the smooth projective curves $C\colon y^2 = x^7 + x$ and $E_a\colon y^2 = x^3 + ax$ over a field k containing a nontrivial cube root of unity $\zeta \in k$. The morphism

$$\begin{aligned} C &\longrightarrow E_1 \times E_{-3} \times E_{-3} \\ (x, y) &\longmapsto (x^3, yx;\ x + 1/x, y/x^2;\ x/\zeta + \zeta/x, y/x^2) \end{aligned}$$

   induces an isogeny $\mathrm{Jac}(C) \longrightarrow E_1 \times E_{-3} \times E_{-3}$ with kernel isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$.

8. *"Trivial" is but another word for "we understood it".* [3]

9. The *concept* of "fake news" can be as dangerous as the disinformation it refers to.

10. A date on a research paper is much more useful than a research paper on a date.

---

[1] Phillip Rogaway. *The Moral Character of Cryptographic Work*. 2015.

[2] Karel Hrbacek and Thomas Jech. *Introduction to Set Theory*. 3rd ed. Pure and Applied Mathematics. Marcel Dekker, Inc., 1978.

[3] Chloe Martindale and Lorenz Panny. "How to not break SIDH". In: *CFAIL 2019*. 2019.