Theses

accompanying the dissertation

Constructive and Computational Aspects of Cryptographic Pairings

by

Michael Naehrig

1. Conjecture: There exist infinitely many pairs of prime numbers (p, n) of the form

$$\begin{aligned} p &= 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\ n &= 36u^4 + 36u^3 + 18u^2 + 6u + 1 \end{aligned}$$

for an integer $u \in \mathbb{Z}$.

All such prime pairs with $|u| < 8$ are given in the following table:

u	(p, n)	u	(p, n)
-1	$(19, 13)$	5	$(27631, 27481)$
1	$(103, 97)$	6	$(55333, 55117)$
-2	$(373, 349)$	-7	$(75223, 74929)$
-3	$(2143, 2089)$	7	$(100003, 99709)$

2. Let q be a prime power, and let

$$f(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + qa_2x^2 + q^2a_1x + q^3 \in \mathbb{Z}[x].$$

Let $\zeta_3 \in \mathbb{C}$ be a primitive 3rd root of unity and let $A = -\frac{1}{3}a_1^2 + a_2 - 3q$ and $B = \frac{2}{27}a_1^3 - \frac{1}{3}a_1a_2 + a_3 - a_1q$.

Then the six roots of f are the complex numbers

$$\frac{s_j}{2} \pm \sqrt{\frac{s_j^2}{4} - q}, \; j = 0, 1, 2,$$

where

$$s_j = -\frac{a_1}{3} + \zeta_3^j \sqrt[3]{-\frac{B}{2} + \sqrt{\frac{B^2}{4} + \frac{A^3}{27}}} + \zeta_3^{2j} \sqrt[3]{-\frac{B}{2} - \sqrt{\frac{B^2}{4} + \frac{A^3}{27}}}.$$

3. To realize pairing-based cryptography, an elliptic curve over a prime field of size 256 bits with embedding degree 12 and a prime number of rational points over the ground field is currently the best choice to provide a comfortable security level.

4. Let T be a random variable which describes the (primary) delay time of a periodically operating train at a fixed point on a railroad line. The probability distribution of T can be described by the following probability distribution function

   $$F(t) = \begin{cases} 1 - p_V e^{-\lambda t} & \text{if } t \geq 0, \\ 0 & \text{if } t < 0, \end{cases}$$

   where p_V is the probability that the train is delayed, and λ is the reciprocal of the expected delay time. This distribution function has been empirically confirmed by means of a sample measured in the German railway network [1].

   A systematic use of analytic tools in the construction of train schedules and for the reduction of delays can significantly increase the quality of service in a railway network.

   [1] Ekkehard Wendler, Michael Naehrig: *Statistische Auswertung von Verspätungsdaten* - In: Eisenbahn-Ingenieur-Kalender (2004), Tetzlaff - Verlag Hamburg, pp. 321–331, 2003

5. The application of mathematical methods in engineering can lead to progress of technology. Whether such methods are helpful or obstructive strongly depends on how good engineers understand them.

6. A deadline is a point in time by which something must be done. There is no rule saying that the task needs to be accomplished as close to this point as possible. Completing it earlier has several advantages.

7. Every human being has the right to be in a bad mood. In particular, not every morning needs to be considered beautiful by everyone. Furthermore, the diversity of human characters implies that excessive optimism does not necessarily lead to better performance and personal growth, but sometimes defensive pessimism does (see [2]).

   [2] Julie K. Norem, Edward C. Chang: *The positive psychology of negative thinking*, Journal of Clinical Psychology, Vol. 58, No. 9, pp. 993–1001, 2002.

8. The distance between Aachen (Reutershagweg) and Eindhoven (Den Dolech) according to the website http://maps.google.nl is exactly 107 km. According to more than 100 measurements with a VW Touran between April 2008 and April 2009, it is 108 km. The minimal driving time of all measurements was 69 minutes. This is exactly 3 minutes longer than the average playing time of a Metallica studio album.

9. The piece with number 2 in part I of Johann Sebastian Bach's mass in b minor (BWV 232) is a perfect realization of a musical pairing.

10. To make proper tea, the current teapot in the coffee corner (north side) on the 9th floor of the Hoofdgebouw needs at least two tea bags when filled completely, no matter what the instructions on the tea package say.

11. Benne de Weger not only looks like a wise man, he actually is one.

12. In principle, everything is easy.