universität innsbruck

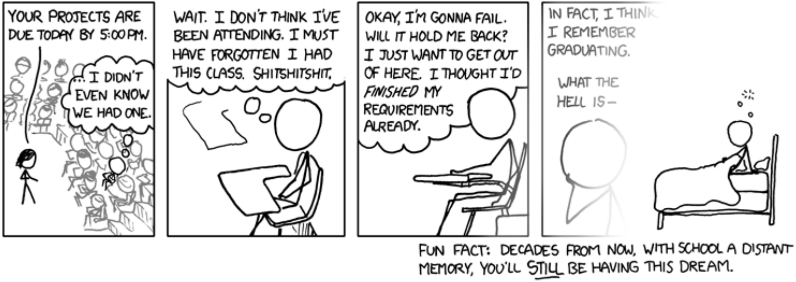
Information Security II – Proseminar

Topic Assignment and Side Channels

Dr. Pascal Schöttle

Tentative Schedule – Summer Term 2018

08.03.18	1.	Introduction, topic presentation
15.03.18	2.	Topic assignment
22.03.18	3.	Presentation of expected outcome (Room SR 1/2, ICT building)
12.04.18	4.	Exercise sheet distribution
19.04.18	5.	Presentation of related work
26.04.18	6.	Exercise sheet discussion
03.05.18	7.	Introduction to game theory
17.05.18	8.	Homework assignment
24.05.18	9.	Homework discussion
07.06.18	10.	Lecture
14.06.18	11.	**Final presentations** (+ 60 min.)
21.06.18		No seminar
28.06.18	12.	Reserved


YOUR PROJECTS ARE DUE TODAY BY 5:00 PM.
...I DIDN'T EVEN KNOW WE HAD ONE.
WAIT. I DON'T THINK I'VE BEEN ATTENDING. I MUST HAVE FORGOTTEN I HAD THIS CLASS. SHITSHITSHIT.
OKAY, I'M GONNA FAIL. WILL IT HOLD ME BACK? I JUST WANT TO GET OUT OF HERE. I THOUGHT I'D *FINISHED* MY REQUIREMENTS ALREADY.
IN FACT, I THINK I REMEMBER GRADUATING.
WHAT THE HELL IS—
FUN FACT: DECADES FROM NOW, WITH SCHOOL A DISTANT MEMORY, YOU'LL STILL BE HAVING THIS DREAM.

Important Dates

	Deadline
Submission 1: Topic preferences	14.03.2018
Submission 2: Expected outcome presentation	22.03.2018
Submission 3: Related work presentation	19.04.2018
Submission 4: Related work write-up	20.04.2018
Submission 5: Homework due	24.05.2018
Submission 6: Final presentation	14.06.2018
Submission 7: Final write-up	08.07.2018

Topics Assigned

This is also the order of the talks on March 22nd!

Topic	Group
Key Reinstallation Attack against WPA2	Leitner/Summerer
Vulnerabilities of Out-of-order Execution	Treichl/Vettori
IoT Light Bulb Covert Channel	Wanker/Piater
Security of the Signal Messaging Protocol	Nicolussi/Salzmann
Robustness of Deep Learning Approaches	Mayerl/Meusburger
Shedding Light into an Obscure Cryptocurrency	Floriani/Hasler

Agenda for next Week (March 22nd)

THURSDAY 22

8.30	Meeting point for UNITN students @ Povo2 entrance
9 -12	UNITN travel
12 - 13.15	UNITN lunch at Bierstindl

	@Technik campus (ICT building, Seminarräume 1-2)
13.40 - 14	**Opening** (Prof. Böhme)
14 - 15-30	**Team presentation**s: Shining, PraiseTheSun, bearthebear, zabatago, Watermunchkin, wmnotfound, Watermarkgroup
15.30 - 15.50	**Coffee break**
15.50 - 16.40	**UIBK student presentations**
16.40 - 17.30	**Team presentations:** Crazy, Tenacious _Deep, teamname, Sailor Moon

20	**Dinner** at Löwenhaus

FRIDAY 23

	@Technik campus (ICT building, Seminarräume 1-2)
9 - 10.20	**Team presentations:** groupname, Gherini, notice_me_senpai, 4-Gerry-Localization, hideinlena, batcable
10.20 - 11.40	**Keynote talk:** Thomas Gloe (dence GmbH)
11.40 -12.10	**Image Forensics Challenge:** behind the scenes and awards
12.10	**Final lunch**

13.30 - 16	Free time in Innsbruck
16 - 19	UNITN travel back to Trento

Expected Outcome Presentation (Recap)

Purpose: Present why your topic is practically relevant and what you expect to demonstrate at the end of the semester. This presentation helps us to see if your expectations might be overly ambitious.

Target Audience: Students from UNITN

Present your topic in a structured way, accessible for students with a general CS background, but not the content of Information Security I & II.

- Support your talk with two or three slides, preferably including a visualization.
- Duration: 5 minutes

Not-So-Random Number Generators (Recap)

NIST National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC: GO

CONTACT SITE MAP

Computer Security Division CSD
Computer Security Resource Center CSRC

CSRC Home | About CSD | Projects / Research | Publications | News & Events

CSRC HOME > GROUPS > ST > CRYPTOGRAPHIC TOOLKIT

NIST SP 800-90A, REVISION 1

April 21, 2014: NIST Invites Comments on Draft SP 800-90A, Revision 1

NIST requests comments on a draft revision of SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Based on public concerns and an evaluation of the algorithm, NIST is proposing the removal of the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG). The revised document is available for a 30-day public comment period.

Background: Public concern has been expressed that one of the random bit generators in SP 800-90A, the Dual_EC_DRBG, could contain a backdoor when used with the parameters specified in the publication. This could allow attackers to successfully predict the secret cryptographic keys that form the foundation for the assurances provided by security products. Cryptographers identified this potential weakness during the development of this guideline, and the issue was initially mitigated by providing mechanisms to generate alternative parameters that would not be susceptible to this weakness. However, news reports on leaked classified information have heightened concern over the possibility of a backdoor in this algorithm.

The Specification

Available at:
`http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf`

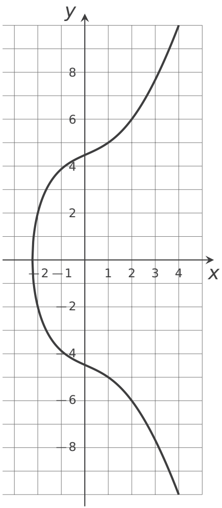
What is an Elliptic Curve ? (Recap)

Definition (Weierstrass Equation)

An elliptic curve E (over $\mathbb{R}$) is defined as the set of points (x, y) satisfying a (simplified) Weierstrass equation:

$$E: \quad y^2 = x^3 + ax + b,$$

with $a, b \in \mathbb{R}$.



E. g.: $E: y^2 = x^3 + 4x + 20$

What is an Elliptic Curve? (Re

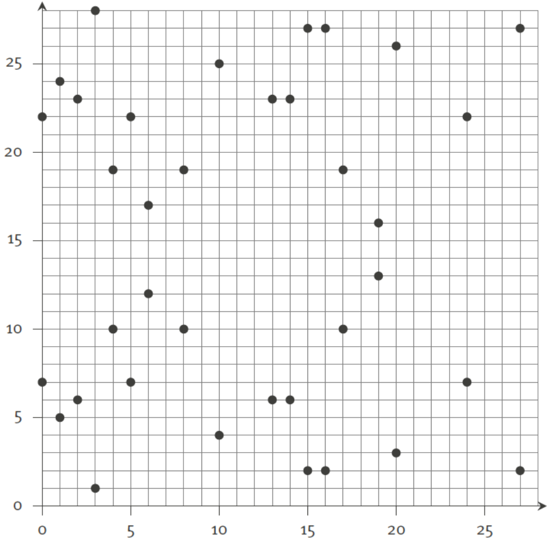
Definition (Weierstrass Equation)

An elliptic curve E (over $\mathbb{R}$) is defined as the set points (x, y) satisfying a (simplified) Weierstrass equation:

$$E: \quad y^2 = x^3 + ax + b,$$

with $a, b \in K$.

E. g.: $E : y^2 = x^3 + 4x + 20/\mathbb{F}_{29}$

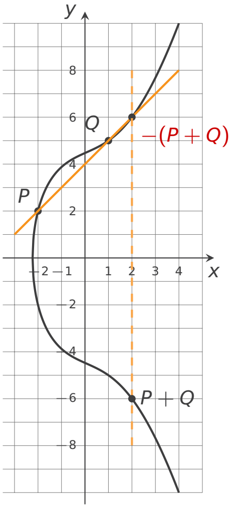


The Group Law – Addition ($P \neq Q$)

- Problem: Naïve approach
  $P + Q = ((x_P + x_Q), (y_P + y_Q)) \notin E$.
- Idea: Draw line through P and Q, as every line has exactly 3 points of intersection with E.
- Draw vertical line through this point and define $P + Q$ as intersection with E.

  Calculate slope as: $s = \frac{y_Q - y_P}{x_Q - x_P}$, and

  $x_{P+Q} = s^2 - x_Q - x_P$; $y_{P+Q} = s(x_P - x_{P+Q}) - y_P$

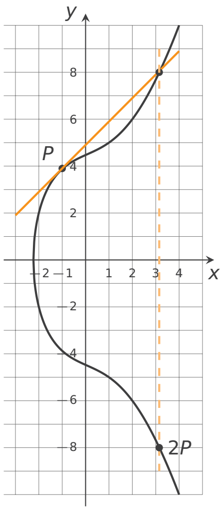


The Group Law – Doubling ($P = Q$)

- Problem: For $P = Q$, slope $s = \frac{0}{0}$ is not defined
- Idea: Draw tangent on E through P;
- Draw vertical line through this point and define $2P$ as intersection with E.

  Use first derivation of E to calculate $s = \left(\frac{3x_P^2+a}{2y_P}\right)$, and

  $x_{2P} = s^2 - 2x_P$; $y_{2P} = s(x_P - x_{2P}) - y_P$



The Group Law – Scalar Multiplication

Intuitive extension of addition: $dP = \underbrace{P + P + \cdots + P}_{d \text{ times}}$

Efficient calculation: *Double & Add* algorithm:

Input: $d = (d_{n-1}d_{n-2}\ldots d_0)_2, P \in E$

Output: dP

1. $Q \leftarrow \mathcal{O}$
2. $\texttt{For } i \texttt{ from } n-1 \texttt{ down to } 0 \texttt{ do}$

   $Q \leftarrow 2Q$

   $\texttt{If } d_i = 1 \texttt{ then } \quad Q \leftarrow Q + P$
3. $\texttt{Return } Q$

Elliptic Curve Discrete Logarithm Problem

The *Elliptic Curve Discrete Logarithm Problem* (ECDLP) is defined as:

Definition (ECDLP)

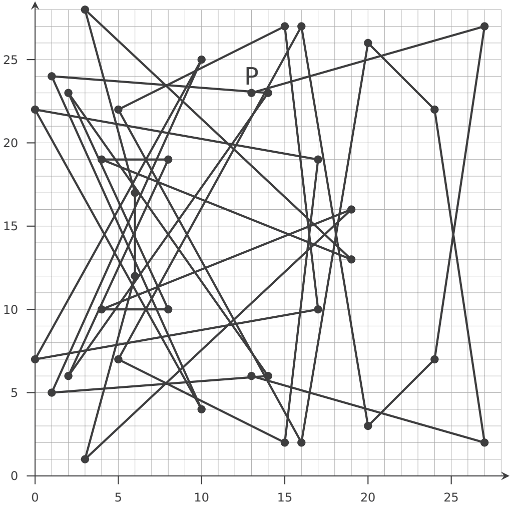
Given an elliptic curve $E(K)$ over a field K, a generator of the elliptic curve P with order $\#P = n$ and another point $Q \in E(K)$:

$$\text{Find } d \in K \text{ such that } Q = dP.$$

(NB: The order of a point P, $\#P = n$, is the number $n \in K$ for which it holds that $nP = \mathcal{O}$. This is also the security parameter of an elliptic curve cryptosystem.)

Group Generation of an Elliptic Curve

$$E : y^2 = x^3 + 4x + 20 \text{ over } \mathbb{F}_{29}$$



Some Iterations of Dual EC-DRBG

Official parameters of Curve P-256:

$$
\begin{aligned}
p &= 115792089210356248762697446949407573530086143415290314195533631308867097853951 \\
n &= 115792089210356248762697446949407573529996955224135760342422259061068512044369 \\
b &= 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b \\
G_x &= 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 \\
G_y &= 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
\end{aligned}
$$

So, let’s use $E : y^2 = x^3 + 4x + 20/\mathbb{F}_{29}$
with $P = (13, 23)$, $n = 37$.
What else do we need?

Countermeasures

- use „better“ curves (e.g. NIST P-384, P-512 ?)
- „cut off“ more than 16 bits
- use a random point Q every time
- use another PRNG . . .