NTNU | Norwegian University of Science and Technology

COURSE INTRODUCTION

TTM4205 – Lecture 1

Tjerand Silde

20.08.2024

Overview

Course Staff

Motivation

Real-World Example

Course Description

Fall 2023

Fall 2024

Contents

Tjerand Silde

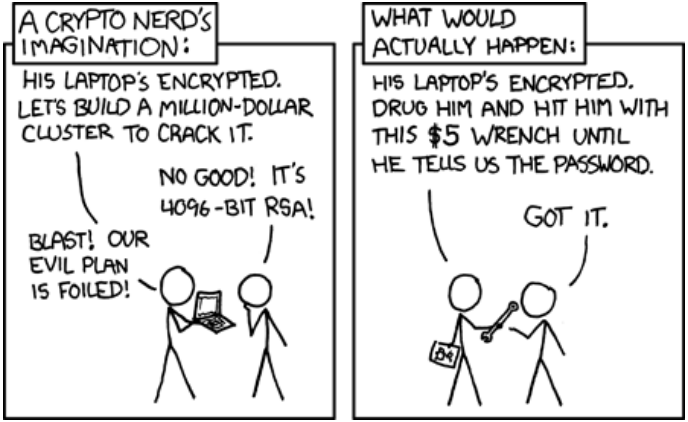
- Associate Professor in Cryptology at IIK
- Research Group Leader at the NTNU Applied Cryptology Lab (NaCl)
- PhD in privacy and crypto from IMF
- Work as Security and Cryptography Expert at startup Pone Biometrics
- Have earlier taught Linear Algebra (M3) and Discrete Mathematics at NTNU

Caroline Sandsbråten

- Lab/Teaching Assistant in TTM4205
- PhD Candidate in Cryptology at IIK
- Researching lattice-based crypto
- Master thesis on breaking ECDSA
- TA/guest lecturer in TTM4137
- Volunteer at Samfundet (ITK)

Contents

Mathematical Security vs. Real-World Security



Mathematical Security vs. Real-World Security

It is somewhere in between the above, and we need to protect against:

- correctness errors and lack of parameter checks
- side-channel and fault injection attacks
- weak or faulty randomness generation
- mismatch when composing protocols
- lack of integrity checks and bad padding

Context

- IIK is creating a new MTKOM profile: Cryptographic Engineering
- We wanted a new practical engineering course in cryptography
- There is a high demand from academia, industry, and government
- Very few people know cryptographic engineering in Norway...

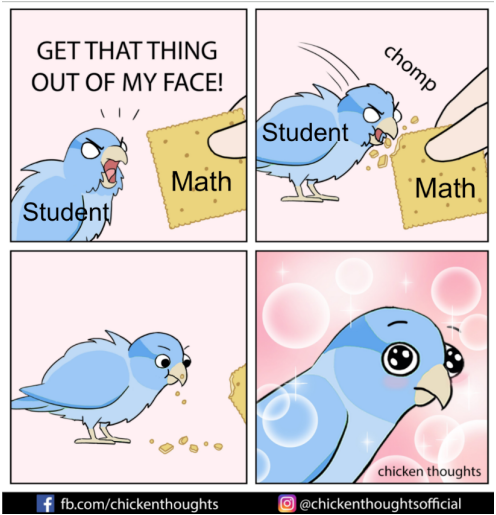
Context

Personal Reasons

I wanted to create a fun and exciting course that I wish I could have taken as a student, and acquire new knowledge that I can use for my own research.

I have included topics I hope you will find interesting and the industry will appreciate that you are familiar with. I want the course to be practical, project- and group-based, with oral presentation and reports instead of a final exam.

Goal


GET THAT THING OUT OF MY FACE!
Student
Math
chomp
Student
Math
chicken thoughts
fb.com/chickenthoughts
@chickenthoughtsofficial

Contents

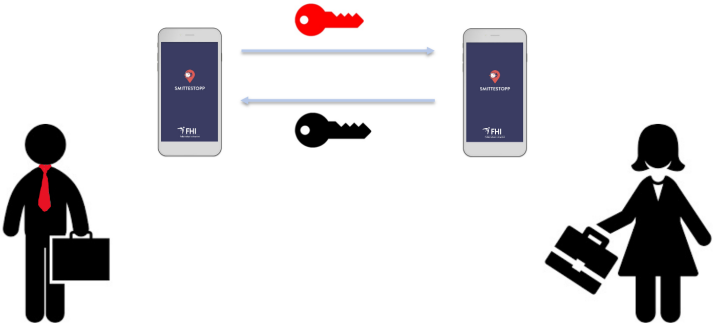
Private Contact Tracing

We created a new application for contact tracing in Norway that preserved the anonymity of users that reported infections, building upon the GAEN API.

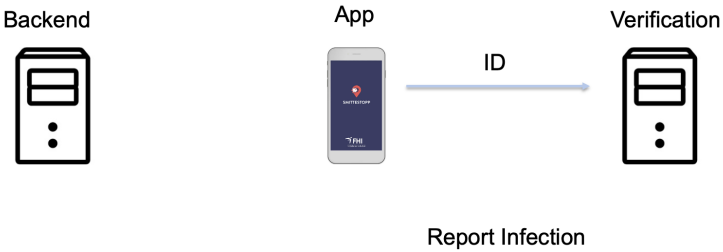
Our application used randomizable anonymous tokens based on specialized elliptic curve cryptography and zero-knowledge proofs.

This was joint work with Martin Strand (FFI), Henrik Walker Moe (Bekk), Johannes Brodwall (Sopra Steria) and Sindre Møgster Braaten (FHI).

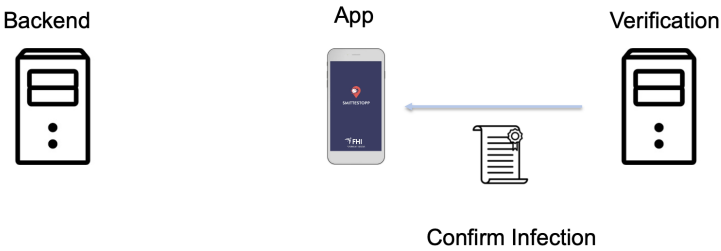
Smittestopp



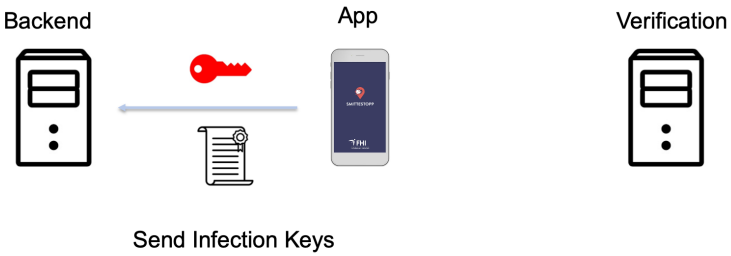
Smittestopp



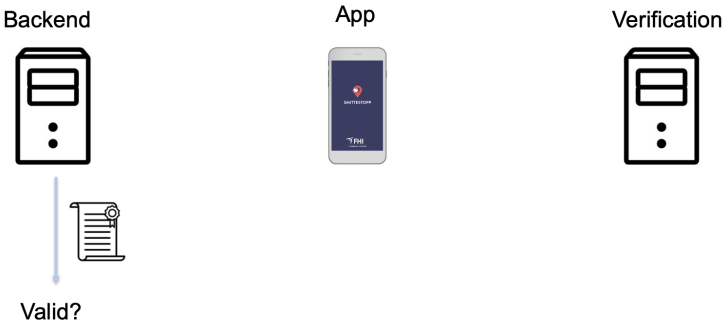
Smittestopp



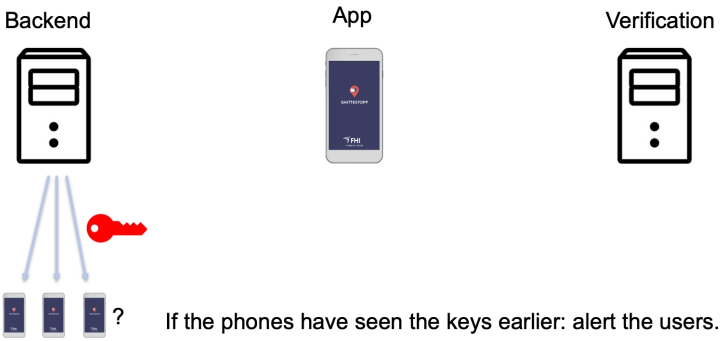
Smittestopp



Smittestopp

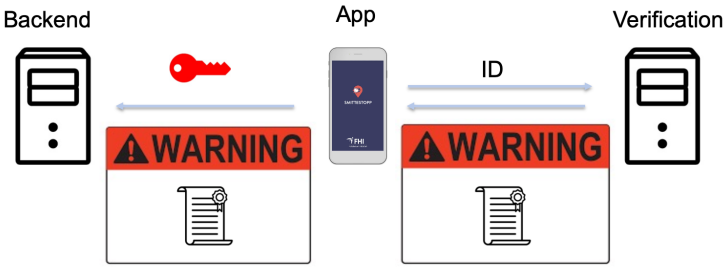


Smittestopp



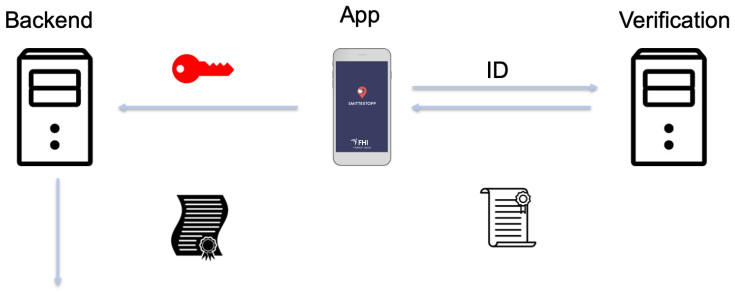
If the phones have seen the keys earlier: alert the users.

Smittestopp



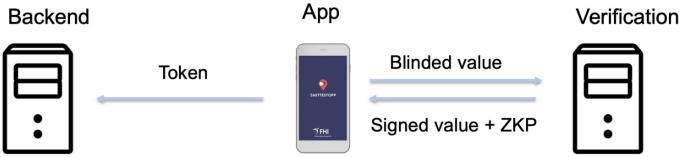
ID can be tied to infection keys when uploading!

Smittestopp



Solution: The app randomises the token before forwarding.

Protocol

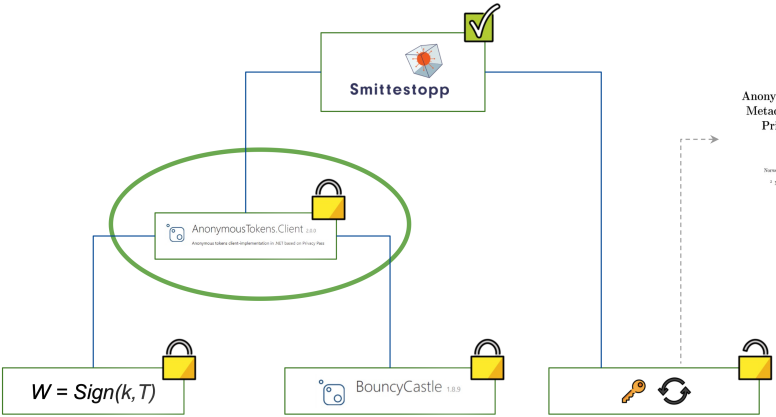


4. Verify token

1. Choose a random and blinded value to be signed

3. Verify proof and unblind

2. Sign the value, and prove that it was correctly signed



Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing

Tjerand Silde[1] and Martin Strand[2]

[1] Department of Mathematical Sciences, Norwegian University of Science and Technology – NTNU, t.jerand.silde@ntnu.no
[2] Norwegian Defence Research Establishment – FFI, martin.strand@ffi.no

Private Contact Tracing

Our open-source library had to make sure that:

- correct and standardized parameters were used
- the elliptic curve library was trustworthy
- the zero-knowledge proof was securely implemented
- no fake tokens or proofs would be accepted

Contents

Course Content

The course covers how to implement, analyse, attack, protect and securely compose cryptographic algorithms in practice. It goes in depth on how to

- implement computer arithmetic
- attack implementations using side-channel attacks and fault injection
- exploit padding oracles and low-entropy randomness
- utilise techniques to defend against these attacks
- securely design misuse-resistant APIs

Learning Outcome

Knowledge

Advanced knowledge about the mathematical building blocks underlying modern cryptography, properties of and applications of cryptographic primitives, challenges and common mistakes when implementing cryptography, side-channel attacks and countermeasures, and high level design principles for secure use of cryptography in practice.

Learning Outcome

Skills

Able to implement the underlying mathematics and high-level protocols used in symmetric key and public key cryptosystems, perform simple side-channel attacks and implement countermeasures, analyse side-channel countermeasures and design misuse resistant APIs for cryptography.

Learning Outcome

General competence

Experience on how to organise projects in small groups, conduct experiments, and write academic reports.

Learning Methods and Activities

Lectures, invited lectures, group projects and laboratory exercises.

Further on Evaluation

Portfolio assessment is the basis for the grade in this course. The portfolio consists of one or more projects covering implementation, analysis, attacks and protection of cryptographic primitives, including a final practical assignment given at the end of the semester. This will be announced at the beginning of the term. The work on all tasks composes 100 % of the final grade. The results for the projects are given in points and in %-scores. The entire portfolio is assigned a letter grade. All assignments will be given in English only and reports must be submitted in English. If a student has the final grade F/failed, the student must repeat the entire course. Also in the case a student wants to improve their grade, they must repeat the entire course.

Recommended Previous Knowledge

The following or equivalent courses are recommended:

- TMA4140 Discrete Mathematics
- TDT4100 Object-Oriented Programming
- TDT4120 Algorithms and Data Structures
- TTM4135 Applied Cryptography and Network Security

It is also recommended to take TMA4160 Cryptography prior to or at the same time as this course.

Course Materials

To be announced at the beginning of the term.

The main course material will be given in the form of slides, notes, manuals, research papers, books and recordings.

Useful course material:

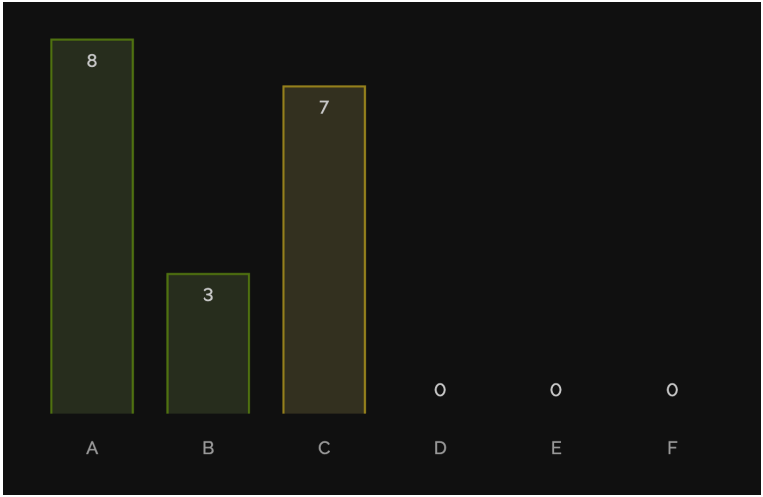
- ChipWhisperer: `https://www.newae.com/chipwhisperer`
- *Serious Cryptography* by Jean-Philippe Aumasson
- *Real World Cryptography* by David Wong
- *The Hardware Hacking Handbook* by van Woudenberg and O'Flynn

Contents

Course Information

The course material, grade distribution and student evaluation from fall 2023 is available on the current course website. The content is similar this year, but we have made some improvements based on the student feedback and experience from the lectures and grading.

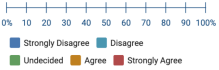
Grade Distribution



Learning Activities

Learning Activities

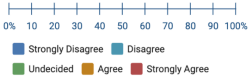
Svar	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Diagram
There were many good learning activities that required me to work actively (rather than just listen).				1	8	
The learning activities have been well prepared and clearly structured .				3	6	
The learning activities have been engaging and motivating .			1	4	4	
The course required that I prepared for the classes .		2	4	1	2	
There has been a good correspondence between the learning goals and what was asked for in the exam and/or assignments .			1	5	3	



Course Information

Teachers and Learning Assistants

Svar	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Diagram
Teachers have made an effort to make the subject interesting.					9	
Teachers have been very good at explaining things.				3	6	
Teachers have also tried to understand the challenges one may have with the course and listened to feedback.				2	7	
The learning assistants have given me the type and amount of help I can expect.			1	3	5	



Contents

Course Information

This is the second time this course has ever been organized. We have planned well, but some things might go differently, and your feedback is essential.

We will make adjustments during the semester and provide help to everyone.

Lecture Plan

This course will consist of lectures and lab/exercise sessions, but note that the formal varies based on the topic of the week. Watch the lecture plan carefully at the course website. Also: some sessions are already cancelled.

Sessions fall 2024: Tuesdays at 08:15-10:00 (lecture OR lab) and Fridays at 10:15-12:00 (lecture) and 12:15-14:00 (lab OR exercise) in lecture hall B2.

Lecture Plan

Week	Date	Format	Responsible	Topic
34	20/8	Lecture	Tjerand	Course Introduction
34	23/8	Lecture	Tjerand	Randomness 1: Entropy
34	23/8	Exercises	Caroline	Exercise Class
35	27/8	Lecture	Tjerand	Randomness 2: Randomization
35	30/8	Lecture	Caroline	Randomness 3: Breaking ECDSA
35	30/8	Exercises	Caroline	Exercise Class
36	3/9	No Class		
36	6/9	No Class		
36	6/9	No Class		
37	10/9	Lecture	Tjerand	Legacy Crypto 1: Crypto Wars
37	13/9	Lecture	Tjerand	Legacy Crypto 2: Attacks on TLS
37	13/9	Exercises	Caroline	Exercise Class
38	17/9	Lab	Caroline	SCA Lab 1 (Setup)
38	20/9	Lecture	Tjerand	Side-Channel Attacks (SCA): Intro
38	20/9	Lab	Caroline	SCA Lab 2

Ed Forum

We have created an Ed Forum for you to ask questions and discuss course content at `https://edstem.org/eu/courses/1290/discussion`.

We encourage all of you to both ask and answer questions related to the course. The staff will pay attention and follow up when appropriate.

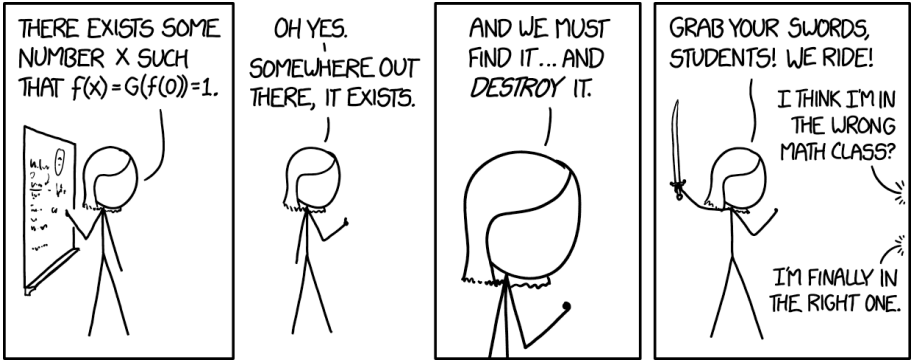
Portfolio Assignments

The course evaluation will consist of three assignments of 100 points total.

You must pass all assignments to pass the course; at least 40% on each.

We will use the official NTNU grading scale to assign combined grades: https://i.ntnu.no/wiki/-/wiki/English/Grading+scale+using+percentage+points.

Weekly Problems



Weekly Problems

This assignment is worth 40 points total. You can make up for mistakes by solving bonus problems. It contains the following kind of problems:

- Mathematics problems
- Coding problems
- CryptoHack problems

Solutions written in LaTeX. The submission deadline is December 6th at 23:59.

ChipWhisperer Lab

ChipWhisperer Lab

This assignment is worth 20 points total. It contains the following activities:

- Side-channel attacks (measure time and voltage during computation)
- Fault injections (make things go wrong or skip instructions)
- Analyse captured data (mean, average, difference, graphs)

Lab will be published soon. The submission deadline is December 6th at 23:59.

ChipWhisperer Lab

Figure: ChipWhisperer Husky

Technical Essay

Technical Essay

This assignment is worth 40 points total. You will write a technical essay and present about either a topic not covered by the lectures, or to cover a topic from the lectures more in-depth. You can choose the topic yourself.

Technical Essay

Most important guidelines:

- Groups of 2 or 3 students each
- Essays of roughly 8 to 10 pages
- Essays written in LaTeX
- Short oral presentations

Technical Essay

Deadlines:

- Topic/scope/group approval: **November 1st**
- Short oral presentations: **November 19th** or **22nd**
- Draft submission for feedback: **November 22nd**
- Receive feedback on draft: **December 6st**
- Final submission: December 20th at 23:59

We provide LaTeX-templates for the essay and the presentation.

Course Material

- We will make all the slides available on the course website
- You do not need to buy any books but we give recommendations
- You can make an account for free at `https://cryptohack.org`
- We provide ChipWhisperer equipment for the lab assignments

Reference Group

We highly value constructive feedback and encourage you to join the reference group. This is especially important since it is a new course, and you will have more impact than in any other reference group.

Send me an email to join. We plan three meetings during the semester.

Questions?