NTNU | Norwegian University of Science and Technology

COURSE INTRODUCTION

TTM4205 – Lecture 1

Tjerand Silde

22.08.2023

Overview

Course Staff

Motivation

Real-World Example

Course Description

Course Content

ChipWhisperer Setup

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

Jonathan Komada Eriksen

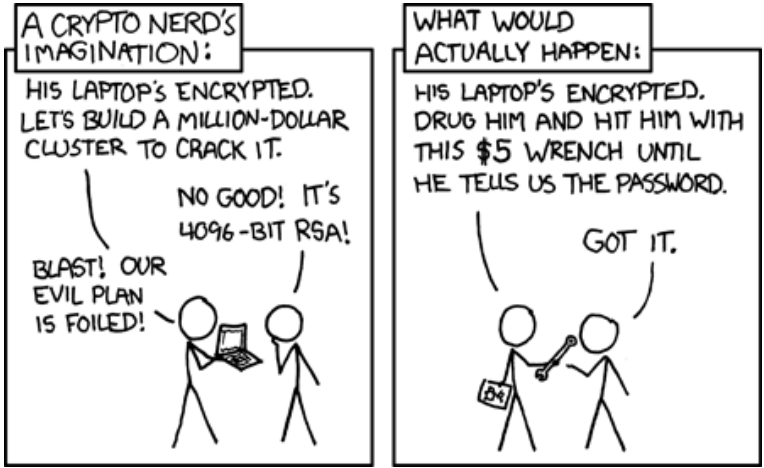
- Lab/Teaching Assistant in TTM4205
- PhD Candidate in Cryptology at IIK
- Researching isogeny-based crypto
- #9 all-time ranking at CryptoHack

Caroline Sandsbråten

- Substitute Lecturer in TTM4205
- PhD Candidate in Cryptology at IIK
- Researching lattice-based crypto
- Master thesis on breaking ECDSA

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...

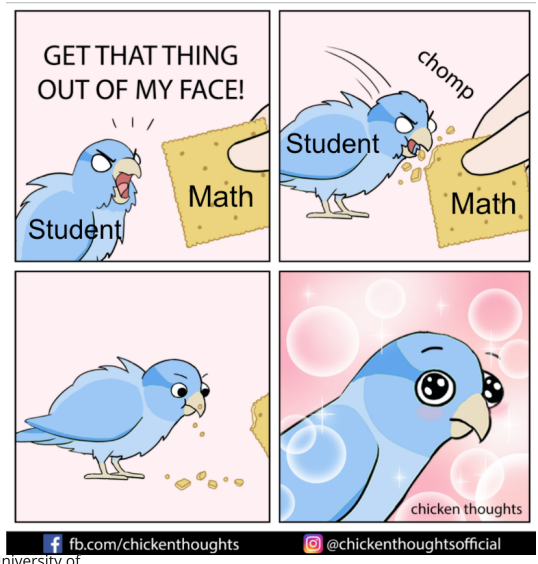
Context

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 work and research.

I have included topics you will find interesting and that the industry will appreciate that you are familiar with. I want the course to be practical, project- and group-based, with oral presentation and report 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

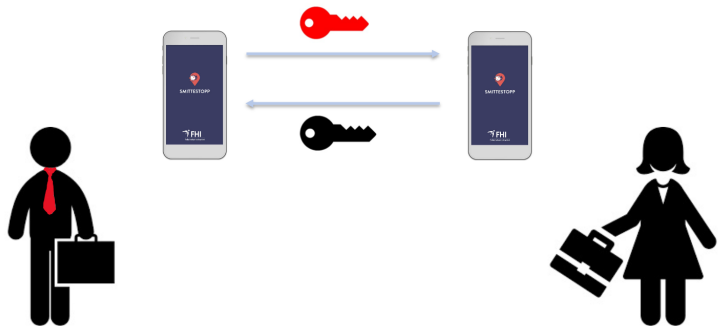
Private Contact Tracing

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.

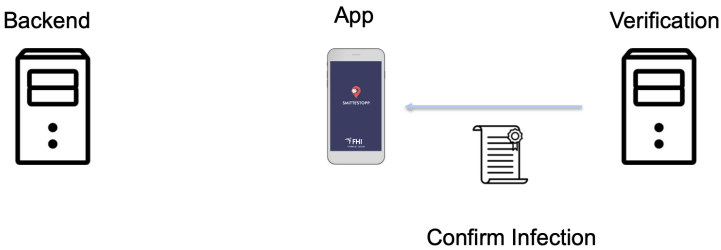
This was joint work with Martin Strand (FFI), Henrik Walker Moe (Bekk), Johannes Brodwall (Sopra Steria) and Sindre Møgster Braaten (FHI).

Smittestopp

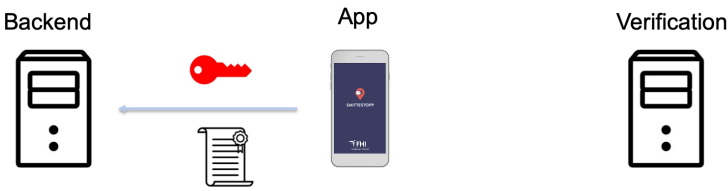


Smittestopp

Smittestopp



Smittestopp



Smittestopp

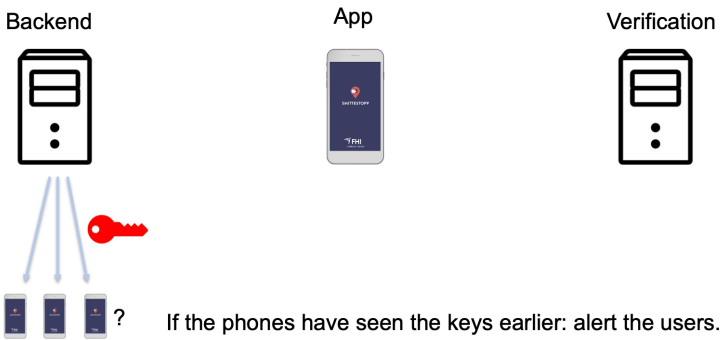
Backend

App

Verification

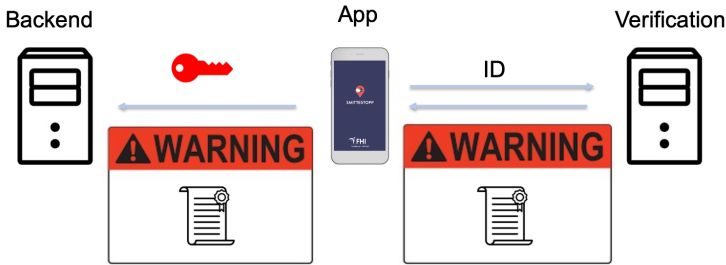
Valid?

Smittestopp



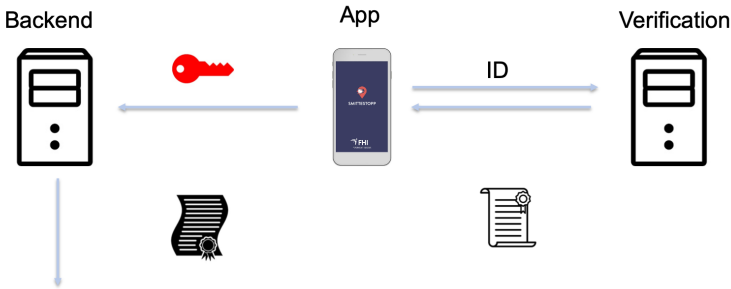
If the phones have seen the keys earlier: alert the users.

Smittestopp



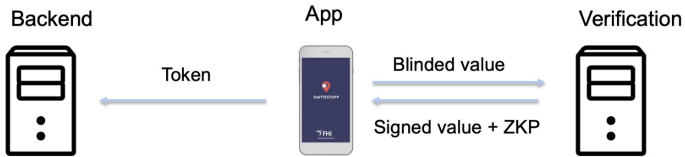
ID can be tied to infection keys when uploading!

Smittestopp



Solution: The app randomises the token before forwarding.

Protocol

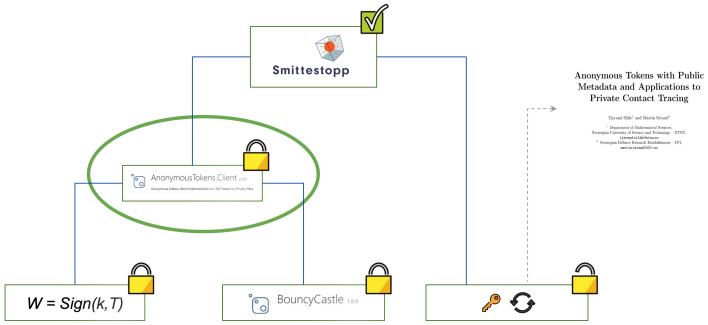


4. Verify token

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


Smittestopp
AnonymousTokens.Client
W = Sign(k, T)
BouncyCastle 1.8.9
Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing

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

Disclaimer

This is the first 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.

Course Information

The official course website of TMA4205 Secure Cryptographic Implementations is at https://tjerandsilde.no/TTM4205.

Lecture Plan

This course will consist of lectures and lab/exercise sessions. There will be a lecture and a lab/exercise session every Tuesday. The format on Thursdays will change between the two depending on the topic of the week: watch the lecture plan carefully at https://tjerandsilde.no/TTM4205/#lecture-plan.

Sessions fall 2023: Tuesdays at 12:15-14:00 (lecture) and 14:15-16:00 (lab/exercise) in R92 and Thursdays at 10:15-12:00 (lecture OR lab/exercise) in B3.

Lecture Plan

Week	Date	Format	Responsible	Topic	Resources
34	22/8	Lecture	Tjerand	Course Introduction	
34	22/8	Lab/Ex	Tjerand	Assignments & Setup	
34	24/8	Lecture	Tjerand	Randomness 1	
35	29/8	Lecture	Caroline	Randomness 2	
35	29/8	Lab/Ex	Caroline	Randomness Exercises	
35	31/8	Lecture	Tjerand	Randomness 3	
36	5/9	Lecture	Tjerand	Legacy Crypto 1	
36	5/9	Lab/Ex	Jonathan	Legacy Crypto Exercises	
36	7/9	Lecture	Tjerand	Legacy Crypto 2	
37	12/9	Lecture	Tjerand	Side-Channel Attacks 1	
37	12/9	Lab/Ex	Jonathan	SCA Lab 1	
37	14/9	Lab/Ex	Jonathan	SCA Lab 2	

Forum

We have a Piazza forum for you to ask questions and discuss course content at https://piazza.com/ntnu.no/fall2023/ttm4205. The sign-up code is:

3dnp6nmmz59

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.

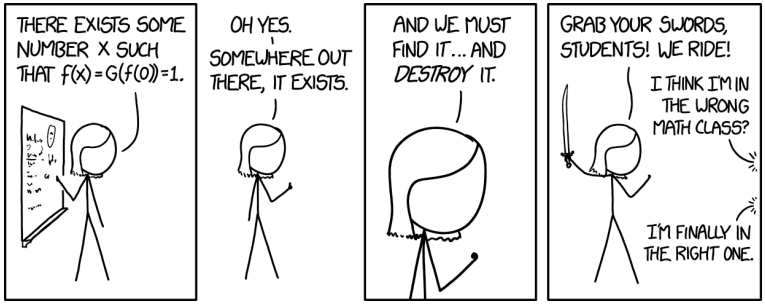
Portfolio Assignments

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

You must pass both 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 at most 40 points total. Bonus problems can give an additional 2 points each. It will contain the following kind of problems:

- Pen & paper problems
- Coding problems
- CryptoHack problems
- ChipWhisperer labs

The submission deadline is December 1st at 23:59. The problems are available at `https://tjerandsilde.no/files/TTM4205_Weekly_Problems.pdf`.

Special Topic Project

Special Topic Project

This assignment is to write a paper about either a topic not covered by the lectures, or to cover a topic from the lectures more in-depth.

Most important guidelines:

- Groups of 1-3 members
- Papers of 10-20 pages
- Papers written in LaTeX
- Short oral presentations

Special Topic Project

Deadlines:

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

We provide LaTeX-templates. The project description is available at `https://tjerandsilde.no/files/TTM4205_Special_Topic_Project.pdf`.

Course Material

- We will make all slides decks 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

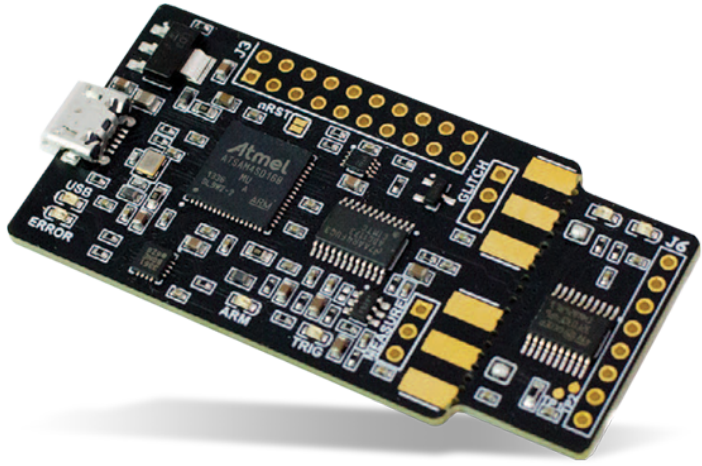
We highly value constructive feedback and encourage you to join the reference group. This is especially important this year since it is a new course, and you will have more impact than in any other reference group.

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

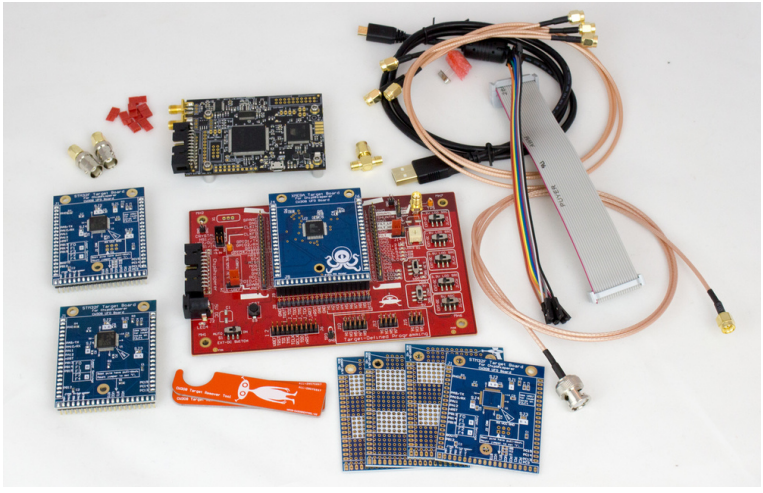
We also encourage you to provide (anonymous) feedback via the Piazza forum.

Contents

ChipWhisperer Nano



ChipWhisperer Level 1 Kit



Installation Guide

The ChipWhisperer installation guide is available at
https://github.com/tjesi/TTM4205/blob/main/CW-Setup.ipynb.

Questions?