Current Topics in Cryptography
CTiC Seminar

Prof. Dr. Blömer

AG Codes und Kryptographie

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Preliminaries

You should have basic knowledge in at least two of the following areas

- IT security
- cryptography
- network theory
- algorithms and data structures
- complexity theory
- probability theory and stochastics

Overview

- **All meetings are mandatory**
- **General kick-off meeting (today)**
- **Topic choice**
  - Send us your top 3 topics and your preferred time slot for your talk: feidens@mail.upb.de
  - We distribute the topics
  - You can also swap your topic once with another willing person

- **Introductory Talk**
  - We will give a talk on the style of a scientific paper and how to work with literature.

Overview

- **Topic kick-off Meeting**
  - Meeting with your supervisor.
  - You should have read your assigned topic paper and understood main ideas
  - We discuss your tasks and questions you have

- **Q&A day**
  - We answer all of your questions in a personal meeting

- **Essay Draft**
  - You hand in a "feature complete“ draft of your essay
  - "feature complete", i.e. everything you plan to have in the final essay should be included in this version.
  - This is your chance to get comprehensive feedback on your work.

Overview

- **Talk Slides**
  - We ask you to turn in the slides of your talk (presentation). We will give feedback for this.
  - Any slot: All students have to hand in their slides one week before their talk.

- **Talk**
  - You will present your topic for all seminar participants and the supervisors in one of the available time slots (you have to be present for both time slots).
  - Your talk should last 1h including discussion (plan to talk 45-50 minutes).

- **Essay Final Version**
  - The final version of the essay should incorporate the feedback given for the draft version and your talk.

Topics

Topics

- **BBA+: Improving the Security and Applicability of Privacy-Preserving Point Collection**
  - Refines security properties of a privacy-preserving point-collection system
  - Generic instantiation of the system
- **Breaking and Fixing Anonymous Credentials for the Cloud**
  - Moves the computational taxing tasks from IoT devices to a proxy (in the cloud).
  - Shows flaws in previous works
  - Shows how to fix them in a new model
- **Handoff All Your Privacy – A Review of Apple’s Bluetooth Low Energy Continuity Protocol**
  - Analyses what user data is leaked
  - Shows attacks on user's privacy
  - Reverse-engineered the continuity protocol

Topics

- **Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping**
  - Detection and analysation of IoT specific network traffic
  - Adversaries track user movement, device usage, and more
  - Shows an algorithm to mix the regular IoT traffic better with non-IoT traffic
- **Fiat Shamir with Aborts**
  - A technique to turn identification protocols into signatures.
  - It is used to create efficient lattice-based signatures, which are post-quantum secure.
- **LWE Encryption**
  - An encryption scheme based on the LWE assumption, which is assumed to be post-quantum secure.

Topics

- **Foundations of Differential Privacy**
  - Privacy-preserving data analysis.
  - Need a meaningful and rigorous definition of privacy.
  - Goal: Introduce fundamental techniques of differential privacy.
- **Optimal Differentially Private Mechanisms for Randomised Response**
  - Randomised Response eliminates bias in surveying.
  - Participants flip a coin to determine how to answer (truthfully or random).
  - Goal: Examine Randomised Response in the context of differential privacy.

Topics

- **Matchmaking Encryption**
  - Special encryption: Users have policies and attributes. User A and User B can communicate if A's policy fits B's attributes and vice versa.
- **Efficient Verifiable Delay Functions**
  - A VDF is a function f such that f(x) takes lots of time to compute, but given x and y, it is easy to check if f(x) = y. Useful for Proofs of Work.
- **A systematic literature review of blockchain-based applications: Current status, classification and open issues**
  - Blockchains are append-only ledgers for which huge ecosystems have recently been developed. This includes cryptocurrencies, but also other applications.
- **Algorand: Scaling Byzantine Agreements for Cryptocurrencies**
  - Algorand is a cryptocurrency that uses proofs of stake as a consensus mechanism (instead of costly proofs of work).

Topics

- **On Privacy Notions in Anonymous Communication**
  - Communication over the internet is not anonymous (e.g., IP addresses leak location). Anonymous communication aims at preserving sender privacy. The paper is about privacy definitions.
- **Darknet Security: A Categorization of Attacks to the Tor Network**
  - Tor is a tool for anonymous communication. Their design emphasizes performance, leading to many (interesting) attack surfaces.
- **Robust Synchronous P2P Primitives Using SGX Enclaves**
  - Intel SGX is a secure enclave within modern processors. Using its guarantees, one can cheaply implement secure efficient peer-to-peer networks.

Topics

- **Software protection and simulation on oblivious RAM**
  - Oblivious RAM enables access to remote storage without the remote storage server learning the accessed data, the data's address or even the type of access performed.
  - It has applications in cloud computing and multi-party computation.
  - This paper addresses the foundations of oblivious RAM and a simple, yet inefficient, ORAM scheme.
- **Path ORAM: An extremely simple oblivious RAM protocol**
  - The paper presents a more recent and much more efficient ORAM scheme whose performance is close to the optimal performance.

Dates

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Time table

PADERBORN UNIVERSITY

	What	
Until Monday 14th	send us top 3 topics and your preferred time slot	deadline is at 23:59
Wednesday 16th	assignment of topics	
Until Friday 18th	exchange topic with willing students and inform us	deadline is at 23:59
Individual meetings with supervisor	topic kick-off meeting	
23.10.19, 16:15	introductory talk	
08.11.19	Q&A day	
10.12.19, 16:15	first slot for talk	send us your slides one week before your talk
29.01.20 & 30.01.20	second slot for talk	send us your slides one week before your talk
21.02.20	essay draft	
16.03.20	deadline: essay final version	

Questions…