



LIT Secure and Correct
Systems Lab

Secure Systems Group @ LIT Secure and Correct Systems Lab



Univ.Prof. Priv.-Doz. DDI Dr. Stefan Rass
www.jku.at/secsys

**JOHANNES KEPLER
UNIVERSITY LINZ**
Altenberger Straße 69
4040 Linz, Austria
jku.at/secsys

About me (Prof. Stefan Rass)

The **Secure Systems Group** is part of the **LIT Secure and Correct Systems Lab**, a cross-institute, interdisciplinary research platform.

Research areas:

Supply Chain Security

Security Management

- Model-Based (quantitative) Security
- IT Risk Management
- Decision theory and game theory with applications in cybersecurity
- Security of Artificial Intelligence
- Security Economics

Applied Cryptography

- Key Management for Public-Key and Symmetric Cryptography
- Quantum Key Distribution and -Networks
- Information Theoretical Security
- Complexity Theory

Bachelor Theses (some topics, but suggestions are very welcome)

Implementation of Multipath Authentication in an Overlay Network

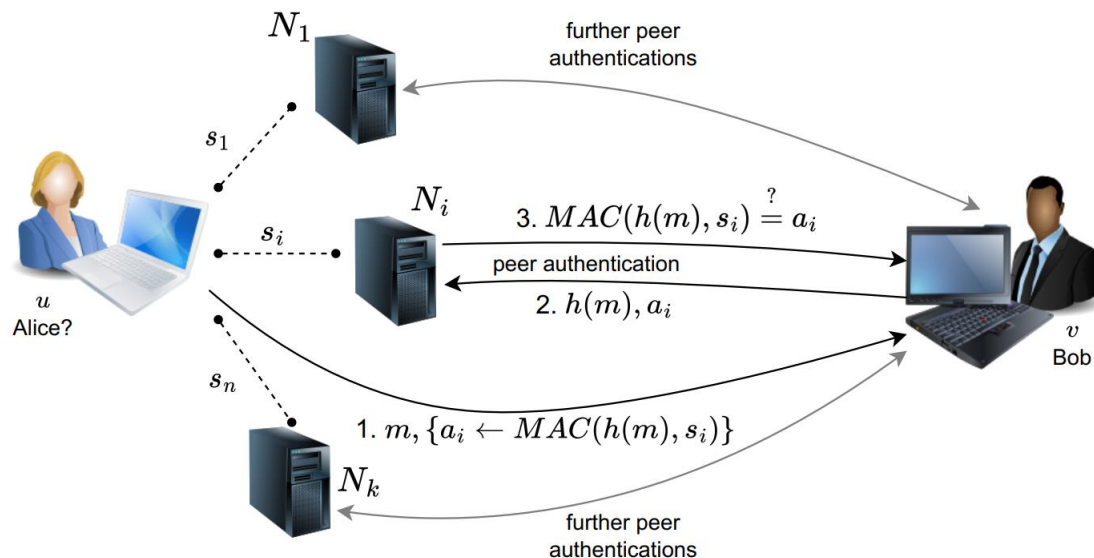
Context

- Post-Quantum secure communication by all-classical means
- Applicable in (future) quantum networks

Bachelor Thesis

Implement small chat-clients that act as senders, receivers and relays of short text messages, supporting

- multipath transmission
- and multipath-authentication



Bachelor Theses (some topics, but suggestions are very welcome)

Writer-Anonymity with help of AI

Context

- Writing texts can, even without the author mentioning a name, leak out who wrote the text (by style, wording, ...)
- AI is known to be quite powerful in generating texts automatically, based on some (little) input

Bachelor Thesis

- Overview of text-generation methods using AI (e.g., ChatGPT and others)
- Overview of “author-attributing” methods
- Experimental implementation of text-generation using AI
- Example testing of author attributing against the artificially generated texts

Bachelor Theses (some topics, but suggestions are very welcome)

“LLM-proof” Questionnaires

Context

- We have some evidence that empirical studies (questionnaires) have been filled in with LLMs
- If this becomes more frequent, it would be “catastrophic” for all empirical research

Bachelor Thesis

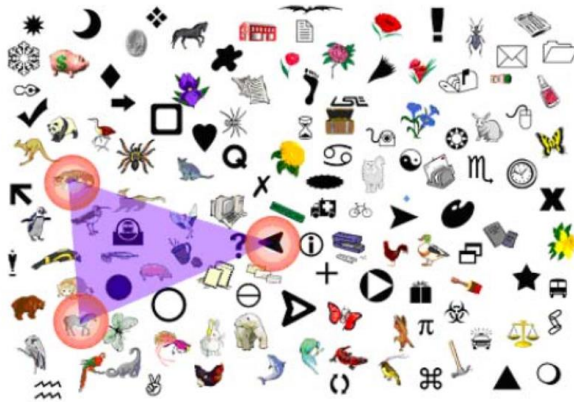
- Overview of techniques to create “barriers” for LLMs (such as CAPTCHAs and others)
- Collection of ideas and discussion about how a questionnaire could be designed to be “LLM-proof”

Bachelor Theses (some topics, but suggestions are very welcome)

Survey of Graphical Passwords

Context

- Standard passwords may be continuously replaced by two-factor authentication,
- Yet still, entering a passcode remains in many cases a necessity
- Shoulder-surfing resilient schemes exist, but are not too-well known



Bachelor Thesis

- Overview of techniques for graphical passwords
- Implementation of some selected such techniques for experimental purposes

Bachelor Theses (some topics, but suggestions are very welcome)

Doodle with automatic calendar blockers

Context

- Doodle polls are convenient, but have a significant disadvantage:
- If the time to complete the poll is too long, the individual calendars start to fill themselves, thus annihilating the options offered

Bachelor Thesis

Implementation of a Doodle-like webservice that

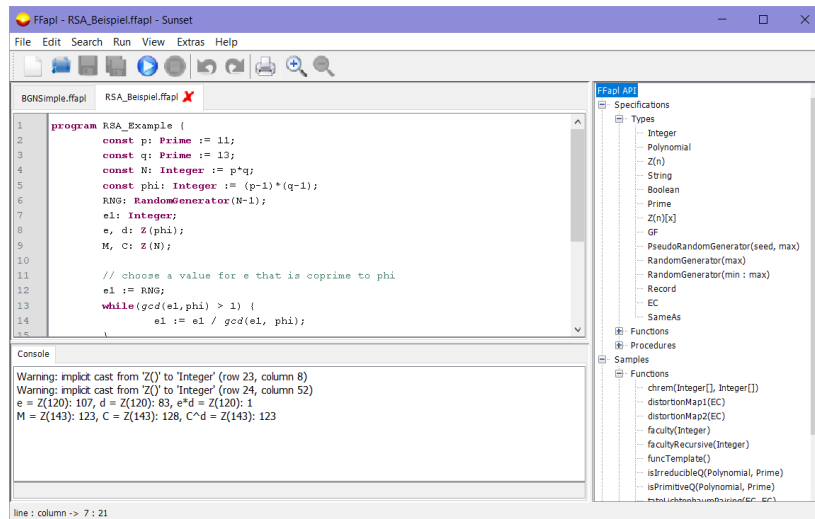
- has a nice visual intuitive interface (like Doodle and others have)
- Supports an “Excel”-format import (CSV, xlsx, ...) of date options (to spare lots of clicking)
- Additionally emails a participant a calendar-importable file (vCalendar or similar) as “date blockers” in people’s calendars + “cancel” events once the final date is fixed

Bachelor Theses (some topics, but suggestions are very welcome)

Extensions to our Crypto Programming Language

Context

- We have a working prototype of a crypto-programming language
- ...which could need more features



```
1 program RSA_Example {
2   const p: Prime := 11;
3   const q: Prime := 13;
4   const N: Integer := p*q;
5   const phi: Integer := (p-1)*(q-1);
6   RNG: RandomGenerator(N-1);
7   e1: Integer;
8   e, d: Z(phi);
9   M, C: Z(N);
10
11  // choose a value for e that is coprime to phi
12  e1 := RNG;
13  while(gcd(e1, phi) > 1) {
14    e1 := e1 / gcd(e1, phi);
15  }
```

Warning: implicit cast from 'Z()' to 'Integer' (row 23, column 8)
Warning: implicit cast from 'Z()' to 'Integer' (row 24, column 52)
e = Z(120): 107, d = Z(120): 83, e*d = Z(120): 1
M = Z(143): 123, C = Z(143): 128, C^d = Z(143): 123

Bachelor Thesis

- Extending the GUI
- Extending the language
- ...other features that you may propose

Bachelor Theses (some topics, but suggestions are very welcome)

BibTex Fixing Tool

Context

- Parse purely textual literature pointers into Bibtex-Format
- Authors names can be tricky in Bibtex concerning their formatting:
 - Lastname, Firstname
 - Firstname Lastname
 - F. Lastname
 - Etc.
- This incurs much manual labor to properly format for a paper's bibliography
- ... and could be tool-supported

Bachelor Thesis

- Implement a parser for the @author field in Bibtex-files that “harmonizes” the name formatting of authors
- Do other “cleanups” and sanity checks if necessary, such as surrounding URLs with `\url{...}`, or finding and replacing special characters (like ä, ö, ...) with their Latex macros, checking correctness of URLs, ...
- Implementable as a command-line tool or with GUI (up to you)

Bachelor Theses (some topics, but suggestions are very welcome)

Schoof's Algorithm implemented in Java

Context

- Elliptic curves are widely used in cryptography
- A frequent question is the number of elements that an elliptic curve contains
- Schoof's algorithm** provides a method to answer this question, but is generally difficult to use
- We would like to make Schoof's algorithm "easily accessible"

Bachelor Thesis

- Find a GPL (or comparable) licensed implementation of Schoof's algorithm written in Java (or callable from Java)
- Integrate the algorithm into the FFapl programming language/interpreter* (language extension or built-in function)

* <https://github.com/stefan-rass/sunset-ffapl>

** https://en.wikipedia.org/wiki/Schoof%27s_algorithm

In case of interest...

...just drop me a line at
stefan.rass@jku.at and
I will be happy to explain further details to you!

