

Secure Systems Group



Univ.Prof. Priv.-Doz. DDI Dr. Stefan Rass

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:

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)

Finding Biases in Training Data

Context

- AI is often used to “objectivize” things to avoid human error
- However, data can contain biases that are unwanted
- Challenge: can we find them “systematically”

Bachelor Thesis

- Implement a fuzzy-rule based regression model* to explain data using “customizable if-then” rules
- Prior work available, but all prototype implementations are proprietary (we would like to have a code that is open and free to use for research)

* Cichy, C., Rass, S., 2019. A Fuzzy-Approximation Approach to Explainable Data Quality Assessment, in: Proceedings of the 34th International Business Information Management Association Conference (IBIMA). pp. 3919–3931.

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
- 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)

Plausibly deniable Clustering Implementation

Context

- Clustering algorithms can, in many cases, be customized
- Supplying a manipulated metric* to a clustering algorithm can arbitrarily change the outcome (to any desired result)
- Applicability of theoretical results is somewhat limited due to roundoff errors and scalability

Bachelor Thesis

- Overview of clustering algorithms, with experimental trials of whether one can “forge” the outcome based on an attack in the literature
- Experimental implementation of the methods with “arbitrary precision arithmetic libraries” (GNU) to study scalability under this extension

* Rass S, König S, Ahmad S, Goman M. Metricizing the Euclidean Space towards Desired Distance Relations in Point Clouds [Internet]. arXiv; 2022 online: <http://arxiv.org/abs/2211.03674>

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

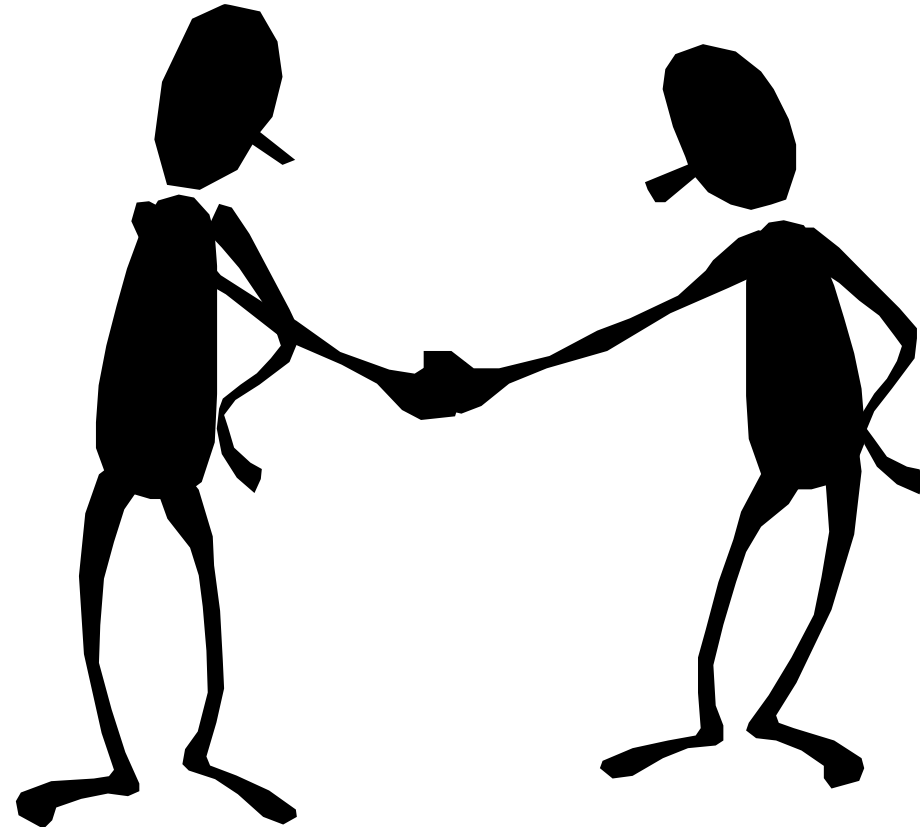
- Find a GPL (or comparable) licensed implementation of Schoof's algorithm written in Java (or callable from Java)
- Integrate the algorithm into the FFapl programming language/interpreter* (language extension or built-in function)

* <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!



Appendix



Univ.Prof. Priv.-Doz. Dr. DDI Stefan Rass

Team Members

- Chair: Univ.-Prof. Priv.-Doz. Dipl.Ing. Dipl.Ing. Dr. techn. Stefan Rass
- PostDoc Researcher: Dr. Maksim Goman
- Ph.D. Researcher: Shahzad Ahmad, MSc
- Administration: Karin McQuillian
- Technical Administration: Andrei Naddour

Security in Artificial Intelligence

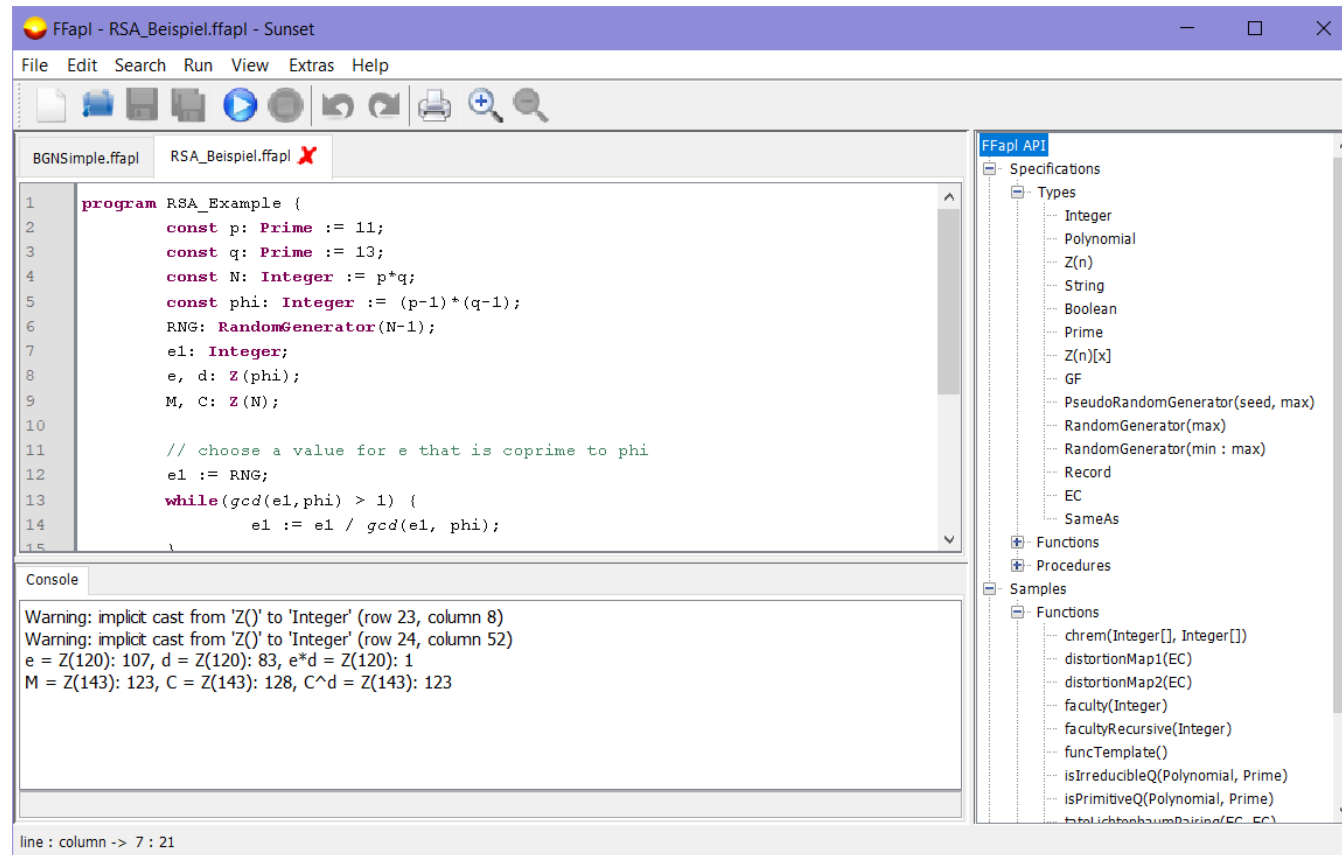
- **Example*: Unsupervised Learning** – Manipulating Clustering algorithms

Point no.	y_1	y_2	random class	by k -means	by DBSCAN
1	18,4875	-7,4766	2	2	1
2	9,1751	2,223	3	3	2
3	-0,5026	9,942	2	2	1
4	-4,2728	-1,1626	1	1	3
5	-8,7678	5,5768	3	3	2
6	-13,2171	-6,7889	1	1	3
7	4,8107	-4,9768	3	3	2
8	-5,5598	4,0152	2	2	1
9	-7,7993	4,3651	2	2	1
10	21,8574	2,3408	3	3	2

* Rass S, König S, Ahmad S, Goman M. Metricizing the Euclidean Space towards Desired Distance Relations in Point Clouds [Internet]. arXiv; 2022 online: <http://arxiv.org/abs/2211.03674>

Sunset/FFapl Crypto Language

- Teaching and prototyping cryptographic systems – A Crypto-Programming Language (open source @ github)



The screenshot shows the FFapl IDE interface. The main editor displays the following code:

```
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 }
```

The console output shows the following results:

```
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
```

The right sidebar shows the FFapl API with sections for Specifications, Types, Functions, Procedures, and Samples. The Types section includes Integer, Polynomial, Z(n), String, Boolean, Prime, Z(n)[x], GF, PseudoRandomGenerator(seed, max), RandomGenerator(max), RandomGenerator(min : max), Record, EC, and SameAs. The Functions section includes chrem(Integer[], Integer[]), distortionMap1(EC), distortionMap2(EC), faculty(Integer), facultyRecursive(Integer), funcTemplate(), isIrreducibleQ(Polynomial, Prime), isPrimitiveQ(Polynomial, Prime), and isLightbaumPairing(EC, EC).