HiWi Job Advertisement

(Student Assistant)

TECHNISCHE UNIVERSITÄT DARMSTADT

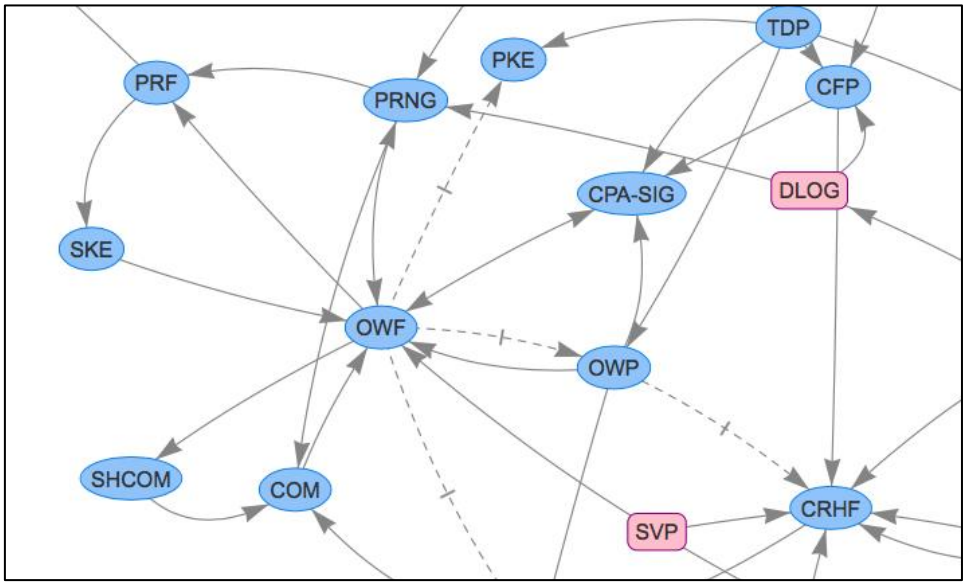
Visualizing the Relations between Cryptographic Primitives

Context: Many cryptographic primitives have been proposed over the last decades and an enormous amount of research has been dedicated to understanding implications and separations between them. For example, it has been shown that one-way functions are necessary and sufficient for constructing digital signature and symmetric encryption schemes. At the same time, one-way functions seem insufficient for constructing public key encryption schemes or collision-resistant hash functions.

Task: The goal of this project is to visualize known relations between cryptographic primitives. The idea is to present the relations in a graph, where the nodes are the primitives and arrows between them represent their relations (see the figure below). The task will involve reviewing literature and implementing the graph visualization using HTML and Javascript.

Requirements: HTML, Javascript, Cryptography, Cryptoplexity (preferred).

Contact: If you are interested in working on this topic and have the required skills, please contact: Matthias Geihs <mgeihs@cdc.tu-darmstadt.de>, Office S2-02 B209, Cryptography and Computer Algebra, Group of Prof. J. Buchmann.



https://www-old.cdc.informatik.tu-darmstadt.de/~mgeihs/relations/

Date: 2018-07-30

CROSSING

Fachbereich Informatik