

The joy of hardware implementation using ChatGPT

Advisor: **Aikata**





DATE: November 20, 2024

Motivation

Language models like ChatGPT, and Bard are in the limelight. We are already witnessing several papers using them as a tool not just for coding or debugging, but sometimes even for writing the paper itself. Hardware implementations generally come out as one of the toughest methods to implement cryptographic schemes. This is because hardware definition languages are quite low-level compared to C or Python. However, dedicated hardware implementations offer superior performance.

So, via this thesis, we would explore how ChatGPT can help ease the hardware implementations. This is pretty much an open research topic and there isn't a fixed path that has to be followed. We will figure this out through experimentation and discussions.

Goals and Tasks

-  Get familiar with ChatGPT feasible optimizations. [2-Weeks]
-  A quick research of existing methods. [2-weeks]
-  Implement and analyze. [2-Month]
-  Suggest best ways based on this analysis. [2-weeks]

Literature

- > Madhav Nair, Rajat Sadhukhan, and Debdeep Mukhopadhyay
Generating Secure Hardware using ChatGPT Resistant to CWEs
<https://eprint.iacr.org/2023/212.pdf>
- > Alvaro Cintas-Canto, Jasmin Kaur, Mehran Mozaffari-Kermani, and Reza Azarderakhsh
ChatGPT vs. Lightweight Security: First Work Implementing the NIST Cryptographic Standard ASCON

Courses & Deliverables

- Introduction to Scientific Working**
Short report on background
Short presentation
- Bachelor Project**
Project code and documentation
- Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Interest in the topic area
- > Basic knowledge of programming.

Advisor Contact

aikata@iaik.tugraz.at