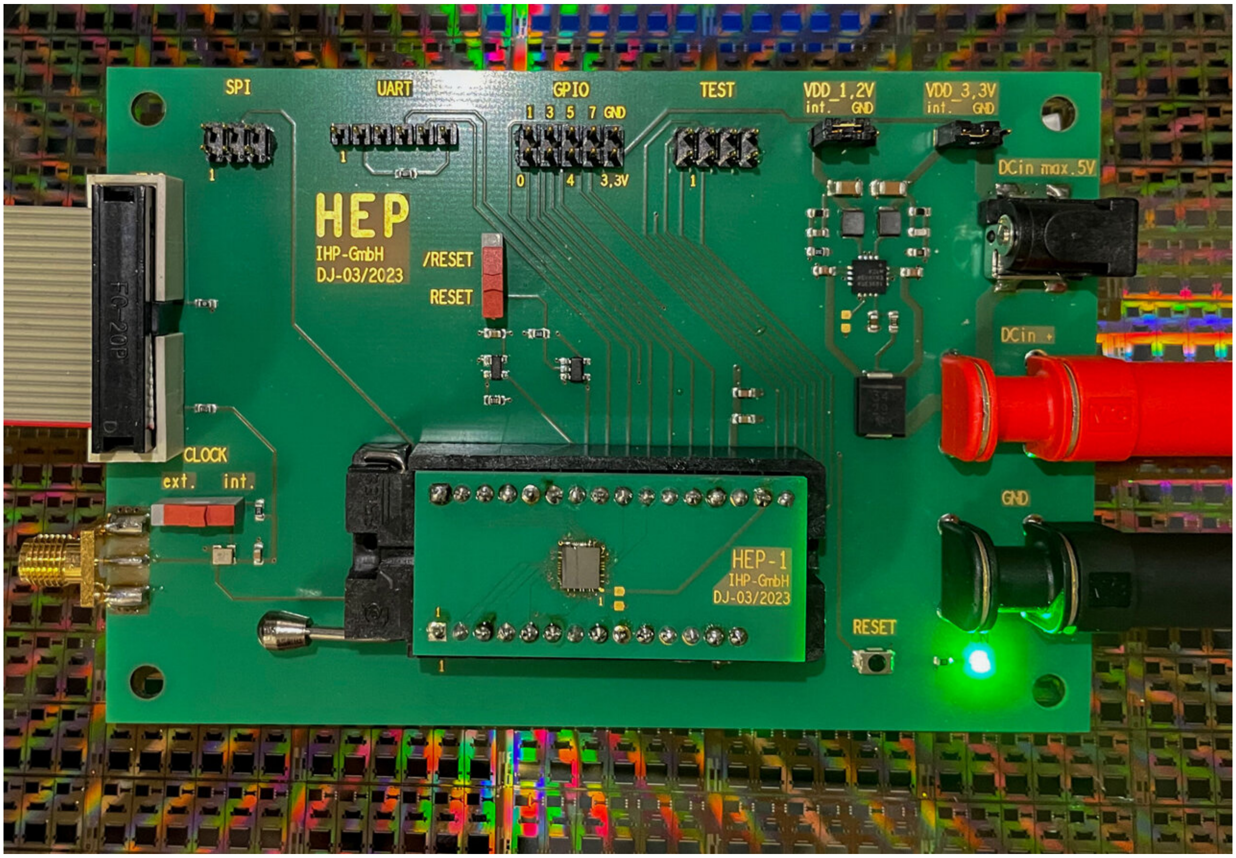
TechXplore

Standards in the field of open source hardware: Open tools used for a security chip

October 20 2023, by Franziska Wegner



The security chip (at the middle of the bottom) is built in flip-chip technology on an auxiliary board and plugged into a standard socket on the main board. The main board handles communication with other components. Credit: Franziska Wegner

The HEP research project has presented an open, flexible design for a security chip. The project, "Hardening the value chain through open source, trusted EDA tools and processors (HEP)," uses open source, free components and tools to manufacture a chip at the IHP fab—the Leibniz-Institute for High Performance Microelectronics. The easy accessibility of the used process sets new standards for development times and significantly reduces the learning curve for chip design.

With the tools and designs used, the research consortium was able to define, design and manufacture a prototypical security chip within two years.

The hardware security module (HSM) produced in this way provides, among other things, a crypto accelerator and tamper-resistant security functions. The development tools used in the process were integrated into a common development environment and expanded to include missing functionality. The Google-driven Open Titan project is similar, but HEP is the first European project. HEP is particularly characterized by a very short development cycle.

Security chips are essential for many suppliers of electronic devices, from the smallest personal devices to automobiles. They perform cryptographic operations and are intended to prevent manipulation, malfunctions and accidents. These chips should be open, flexibly adaptable and as mathematically proven secure as possible.

Given global value chains with numerous players, the supply of such cost-efficient components is a major challenge. Open source designs, where the so-called source code is made public for third-party review, offer a versatile alternative here, as long as their security can be ensured with the circuit design tools (EDA). The research consortium is working on this in the HEP project, which is part of the German Federal Ministry of Education and Research's "Trustworthy Electronics" initiative

(Vertrauenswürdige Elektronik).

In detail, the following results have been developed and implemented within the HEP project:

- Extension of the SpinalHDL language: The research consortium has extended the open hardware description language SpinalHDL to enable the semi-automated implementation of security properties. This prevents security-relevant steps from being deleted as superfluous during the subsequent chip design steps.
- Formal verification of the VexRiscv processor: The correct functioning of the VexRiscv processor, a RISC-V design, has been largely proven mathematically by using formal verification methods.
- Development of an open source crypto accelerator: The security and performance of the processor have been enhanced with the development of an open-source crypto accelerator.
- Development of open masking: Cryptographic calculations could possibly be tracked through side channels, such as power consumption, and keys could be calculated from this. This is countered with a newly developed, semi-automated, open masking tool.
- Integration of real, in Europe manufacturable, process specific data (PDK) of the IHP into Openlane: Openlane is an open tool chain promoted by independent developers, Google, efabless and initially also by DARPA to convert a hardware description into three-dimensional chip designs. Openlane, for its part, is partly made up of open, European tools, such as Yosys and Klayout. However, the results of Openlane must be adapted to the factory-specific processes in order for the chip to function properly. These specifications are described in the so-called PDK (Process Design Kit). For the first time, HEP used a European PDK with the open Openlane, the latter improved for this purpose.

- The work in the HEP project has laid the foundation for the first European PDK specifically designed for open tools.
- Integration of the management of a hardware security module into a crypto driver for Autosar (AUTomotive Open System ARchitecture).

By implementing these achievements for a security chip, the researchers have set new standards for the security and development cycles of open hardware.

Detlef Boeck from project partner Elektrobit said, "As an industry partner, it was important for us to integrate the components developed in the HEP project into the Autosar environment of EB tresos."

René Rathfelder from project partner IAV added, "The risks and threats posed by the increasing complexity of systems are becoming more sophisticated. We want to take advantage of the opportunity to work on open cybersecurity developments at an early stage in order to be able to incorporate these into all our areas of activity in the future."

Dr.-Ing. Norbert Herfurth from IHP said, "As project coordinator, I am very grateful for our highly motivated and capable consortium. It is impressive what can be achieved in such a short period of time when everyone is passionate about what they do."

The manufactured security chip works, but for design-open security products, an open, non-volatile memory and an open, physical random number generator are currently still missing—the project partners are working on solutions for both. The code for installation on an FPGA has been made publicly available.

The demonstrated flow shows that the design of microchips with open tools is accessible, comes at low costs and is quickly usable for everybody—students, SMEs, as well as industry. The papers have been published as part of the *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* and the *2023 Design, Automation & Test in Europe Conference & Exhibition (2023)*.

More information: Fabian Buschkowski et al, EasiMask-Towards Efficient, Automated, and Secure Implementation of Masking in Hardware, *2023 Design, Automation & Test in Europe Conference & Exhibition (2023)* (2023). DOI: 10.23919/DATE56975.2023.10137330

Arnd Weber et al, Verified Value Chains, Innovation and Competition, *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (2023). DOI: 10.1109/CSR57506.2023.10224911

github.com/Chair-for-Security-Engineering/EASIMask

Provided by Leibniz-Institut für innovative Mikroelektronik

Citation: Standards in the field of open source hardware: Open tools used for a security chip (2023, October 20) retrieved 27 April 2024 from https://techxplore.com/news/2023-10-standards-field-source-hardware-tools.html