Pressemitteilung

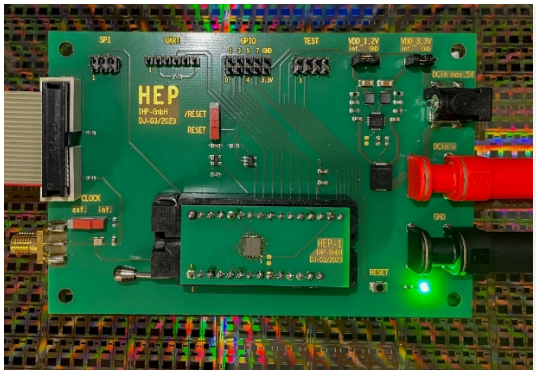
20. Oktober 2023

Leibniz Institute for high performance microelectronics

Offene Werkzeuge zur Herstellung eines Sicherheitschips genutzt

Forschungskonsortium setzt Maßstäbe im Bereich Open Source-Hardware

Frankfurt (Oder). Das Forschungsprojekt HEP hat ein offenes, flexibles Design für einen Sicherheitschip vorgestellt. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt „**H**ärtung der Wertschöpfungskette durch quelloffene, vertrauenswürdige **E**DA-Tools und **P**rozessoren (HEP)" verwendet quelloffene, kostenlose Komponenten und Werkzeuge für die Herstellung eines Chips im IHP – Leibniz-Institut für innovative Mikroelektronik. Die leichte Zugänglichkeit des erprobten Ablaufs setzt neue Maßstäbe für Entwicklungszeiten und verringert den Lernaufwand beim Thema Chipdesign deutlich. Mit den verwendeten Tools und Designs war es dem Forschungskonsortium möglich, innerhalb von zwei Jahren einen prototypischen Sicherheitschip zu definieren, zu entwerfen und zu fertigen. Das so gefertigte Hardware Security Module (HSM) stellt unter anderem einen Krypto-Beschleuniger sowie manipulationssichere Sicherheitsfunktionen zur Verfügung. Die dabei verwendeten Tools wurden in eine gemeinsame Entwicklungsumgebung integriert und um fehlende Funktionalität erweitert. Das von Google getriebene Open Titan-Projekt ist ähnlich gelagert, aber mit HEP existiert jetzt das erste europäische Projekt. HEP zeichnet sich besonders durch einen sehr kurzen Entwicklungszyklus aus.



Der gefertigte Sicherheitschip (Mitte unten) ist auf einer Hilfsplatine aufgebaut und in einem Standardsockel auf die Hauptplatine gesteckt. Die Hauptplatine realisiert die Kommunikation mit anderen Bauteilen.
© IHP 2023/Franziska Wegner

Sicherheitschips sind für viele Anbieter elektronischer Geräte, von den kleinsten persönlichen Geräten bis hin zu Automobilen, essenziell. Sie führen kryptographische Operationen aus und sollen Manipulationen, Fehlfunktionen und Unfälle verhindern. Diese Chips sollten offen, flexibel anpassbar und mathematisch bewiesenermaßen sicher sein. Angesichts globaler Wertschöpfungsketten mit zahlreichen Akteuren stellt die Versorgung mit derartigen kosteneffizienten Komponenten eine große Herausforderung dar. Quelloffene Designs, bei denen der sogenannte Source Code zur Überprüfung durch Dritte bekannt gemacht wird, bieten hier eine vielseitige Alternative, solange ihre Sicherheit mit den Werkzeugen zum Schaltungsentwurf (EDA) gewährleistet werden kann. Hieran arbeitet das Forschungsprojekt HEP, das im Rahmen der Initiative „Vertrauenswürdige Elektronik" vom BMBF gefördert wird.

IHP GmbH • Innovations for High Performance Microelectronics | Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25 • 15236 Frankfurt (Oder) • Tel.: +49 335 5625 0 • E-Mail: ihp@ihp-microelectronics.com

Leibniz Gemeinschaft

Pressemitteilung

Leibniz Institute for high performance microelectronics

Im Einzelnen sind folgende Ergebnisse im Rahmen des Projektes HEP entwickelt und implementiert worden:

- Erweiterung der SpinalHDL-Sprache: Das Forschungskonsortium hat die offene Hardware-Beschreibungssprache SpinalHDL erweitert, um die halbautomatisierte Implementierung von Sicherheitseigenschaften zu ermöglichen. Dadurch wird ausgeschlossen, dass während der nachfolgenden Schritte zum Chipdesign sicherheitsrelevante Schritte als überflüssig gelöscht werden.
- Formale Verifikation des VexRiscv-Prozessors: Die korrekte Funktion des VexRiscv-Prozessors, eines RISC-V Designs, wurde mittels formaler Verifikation mathematisch weitgehend bewiesen.
- Entwicklung eines quelloffenen Crypto-Beschleunigers: Die Sicherheit und Leistung des Prozessors wurden mit der Entwicklung eines quelloffenen Crypto-Beschleunigers erhöht.
- Entwicklung offener Maskierung: Kryptografische Berechnungen könnten evtl. durch Seitenkanäle, wie den Stromverbrauch, verfolgt und hieraus Schlüssel berechnet werden. Mit einem neu entwickelten, halbautomatisierten, offenen Tool zur Maskierung wird dem entgegengewirkt.
- Integration von realen, in Europa herstellbaren, prozessspezifischen Daten (PDK) des IHP in Openlane: Openlane ist eine von unabhängigen Entwicklern, Google, efabless und anfangs auch durch die DARPA geförderte offene Toolkette, um eine Hardware-Beschreibung in dreidimensionale Chipdesigns umzuwandeln. Openlane besteht seinerseits teilweise aus offenen, europäischen Tools, wie Yosys und Klayout. Die Ergebnisse von Openlane müssen jedoch an die fabrikationsspezifischen Prozesse angepasst werden, damit der Chip einwandfrei funktioniert. Diese Spezifikationen sind im sogenannten PDK (Process Design Kit) beschrieben. Erstmals wurde in HEP ein europäisches PDK mit dem offenen Openlane verwendet, letzteres wurde hierfür verbessert.
- Die Arbeiten im Projekt HEP haben den Grundstein für das erste europäische, speziell für offene Tools entwickelte PDK gelegt.
- Integration des Managements eines Hardware Security Module in einen Crypto-Driver für Autosar (AUTomotive Open System ARchitecture).

Durch die Implementierung dieser Errungenschaften für einen Sicherheitschip haben die Forschenden neue Maßstäbe für die Sicherheit und Entwicklungszyklen von offener Hardware gesetzt.

Detlef Boeck vom Projektpartner Elektrobit: „Als Industriepartner war es uns wichtig, die im Rahmen des HEP-Projekts entwickelten Komponenten in die Autosar-Umgebung von EB tresos zu integrieren.“

René Rathfelder vom Projektpartner IAV: „Die Risiken und Bedrohungen durch die zunehmende Komplexität der Systeme werden immer ausgeklügelter. Die Möglichkeit,

Pressemitteilung

Leibniz Institute for high performance microelectronics

frühzeitig an offenen Cybersecurity-Entwicklungen mitarbeiten zu können, wollen wir nutzen, um diese zukünftig in allen unseren Tätigkeitsbereichen einbringen zu können."

Dr.-Ing. Norbert Herfurth vom IHP: „Als Projektkoordinator bin ich sehr dankbar für unser hochmotiviertes und fähiges Konsortium. Es ist beeindruckend, was in einer solch kurzen Zeitspanne erreicht werden kann, wenn alle mit Leidenschaft bei der Sache sind."

Der hergestellte Sicherheitschip funktioniert, aber für design-offene Sicherheitsprodukte fehlen z. Z. noch ein offener, nichtflüchtiger Speicher und ein offener, physikalischer Zufallszahlengenerator – die Projektpartner arbeiten an Lösungen für beides. Der Code für die Installation auf einem FPGA wurde öffentlich zur Verfügung gestellt. Der erprobte Ablauf zeigt, dass das Entwerfen von Microchips, unter Verwendung von offenen Tools, für jedermann – Studenten, KMUs und Großindustrie – zugänglich, preiswert umsetzbar und schnell verfügbar sein kann.

Über das Projekt:
Das Projekt HEP wird vom IHP – Leibniz-Institut für innovative Mikroelektronik geleitet.

Zu den weiteren Partnern gehören:

- IAV GmbH Ingenieurgesellschaft Auto und Verkehr
- Elektrobit Automotive GmbH
- Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
- Fraunhofer-Institut für Sichere Informationstechnologie SIT
- Hochschule RheinMain
- Ruhr-Universität Bochum, Lehrstuhl für Security Engineering
- Technische Universität Berlin, Department Security in Telecommunications

Assoziierte Partner sind:

- CARIAD SE (A Volkswagen Group Company)
- HENSOLDT Cyber GmbH
- Hyperstone GmbH
- Robert Bosch GmbH
- Swissbit Germany AG

Förderkennzeichen: ME1ZEUS012

Weiterführende Informationen:
http://hep-alliance.org/Project/
https://github.com/VE-HEP/VE-HEP-HW-SW
https://github.com/IHP-GmbH/IHP-Open-PDK

Pressemitteilung

Leibniz Institute for high performance microelectronics

Publikationen:

Buschkowski, Fabian; Sasdrich, Pascal; Güneysu, Tim: Easimask – Towards Efficient, Automated, and Secure Implementation of Masking in Hardware. Date 2023, April 19, 2023.
https://ieeexplore.ieee.org/document/10137330
https://github.com/Chair-for-Security-Engineering/EASIMask

Weber, Arnd; Guilley, Sylvain; Rathfelder, René; Stöttinger, Marc; Grawunder, Torsten; Lüth, Christoph; Malenko, Maja; Reith, Steffen; Puccetti, Armand; Seifert, Jean-Pierre; Herfurth, Norbert; Heiser, Gernot; Sankowski, Hagen: Verified Value Chains, Innovation and Competition. IEEE CSR 2023.
https://ieeexplore.ieee.org/document/10224911
https://trustworthy.systems/publications/papers/Weber_GRSGLMRPSHHS_23.pdf

Wissenschaftlicher Ansprechpartner des IHP:

Dr.-Ing. Norbert Herfurth
Wissenschaftler Department Technology
IHP GmbH – Innovations for High Performance Microelectronics/
Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25
15236 Frankfurt (Oder)
Telefon: +49 (335) 5625 525
E-Mail: herfurth@ihp-microelectronics.com

PR-Ansprechpartnerin des IHP:

M.A. Franziska Wegner
Public Relations
IHP GmbH – Innovations for High Performance Microelectronics/
Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25
15236 Frankfurt (Oder)
Telefon: +49 (335) 5625 205
E-Mail: wegner@ihp-microelectronics.com

Über das IHP:

Das IHP ist ein Institut der Leibniz-Gemeinschaft und betreibt Forschung und Entwicklung zu siliziumbasierten Systemen, Höchstfrequenz-Schaltungen und -Technologien einschließlich neuer Materialien. Es erarbeitet innovative Lösungen für Anwendungsbereiche wie die drahtlose und Breitbandkommunikation, Sicherheit, Medizintechnik, Industrie 4.0, Mobilität und Raumfahrt. Das IHP beschäftigt ca. 365 Mitarbeiterinnen und Mitarbeiter. Es verfügt über eine Pilotlinie für technologische Entwicklungen und die Präparation von Hochgeschwindigkeits-Schaltkreisen mit 0,13/0,25 µm-SiGe-BiCMOS-Technologien, die sich in einem 1500 m² großen Reinraum DIN EN ISO 14644-1 3 befindet.

www.ihp-microelectronics.com