Bundesministerium
der Verteidigung

# Wehrwissenschaftliche Forschung Jahresbericht 2021

Wehrwissenschaftliche Forschung für deutsche Streitkräfte

BUNDESWEHR

TORR Dipl.-Ing. Stefan Kolm
Wehrtechnische Dienststelle für Informationstechnologie
und Elektronik (WTD 81)
Greding

wtd81210@bundeswehr.org

Dipl.-Ing. Thomas Kuhn
HTV Halbleiter-Test & Vertriebs-GmbH
Bensheim

info@HTV-GmbH.de

# Design informationssicherer Field Programmable Gate Arrays (FPGAs)

**Die Wehrtechnische Dienststelle für Informationstechnologie und Elektronik (WTD 81) hat mit der Fa. HTV Halbleiter-Test & Vertriebs-GmbH FPGAs (Field Programmable Gate Arrays) analysiert, um die Funktionalität der sicheren Kryptobibliothek Botan (eine sog. Secure Sockets Layer Bibliothek) auf einem Prozessor vom Typ Zynq UltraScale+ umzusetzen.**

Im Einzelnen wurden Krypto-Algorithmen aus der Bibliothek Botan in eine VHDL-Hardwarebeschreibungssprache (VHDL: Very High Speed Integrated Circuit Hardware Description Language) implementiert und deren fehlerfreie Funktionsweise evaluiert. Die Funktionsweise der Algorithmen umfasst die Verschlüsselung, Authentifikation und Erzeugung von sog. Hashwerten. Die realisierten Algorithmen konnten erfolgreich in ein spezielles Protokoll (TLS 1.3) integriert werden, das auf einem FPGA vom Typ Zynq UltraScale+ MPSoC in Betrieb genommen wurde.

FPGAs sind integrierte Schaltkreise der Digitaltechnik und kommen in vielen Gebieten der digitalen Elektronik zum Einsatz. Aufgrund ihrer hohen Flexibilität und Parallelität werden sie gerne als Co-Prozessoren für CPUs (z. B. zur Berechnung kryptographischer Algorithmen) eingesetzt, um deren Performanz zu beschleunigen. Auch als programmierbare Logik-Bausteine in der Informationstechnik gewinnen sie immer stärker an Bedeutung. Aus diesem Grund haben die beiden großen CPU-Hersteller (Intel und AMD) in den vergangenen Jahren die beiden marktführenden FPGA-Hersteller (Xilinx und Altera) aufgekauft.



Als Hardware-Plattform wurde das UltraZed-SOM-Board (Embedded System On Modul, SOM) mit einem Zynq UltraScale+ MPSoC-FPGA (Multiprocessor System on a Chip, MPSoC) der Firma Xilinx gewählt (vgl. Abb. 1).

Damit einzelne Bereiche sich in der FPGA-Logik nicht gegenseitig beeinflussen können (z. B. in einem Flugzeug die Steuerung der Beleuchtung und des Triebwerks), wurden Mechanismen zur physikalischen Trennung der einzelnen Bereiche untersucht. Es konnte gezeigt werden, dass über den Isolation Design Flow (IDF) des FPGA-Herstellers Xilinx ein Verfahren angeboten wird, das eine physikalische Trennung (engl. fence) unterschiedlicher Daten bzw. Algorithmen ermöglicht (vgl. Abb. 2).

Zukünftig wird dies immer wichtiger, um FPGAs im Betrieb mit partieller Rekonfiguration umzuladen und eine gleichzeitige Nutzung unterschiedlicher Anwendungen zu ermöglichen.

Für die Entwicklung kryptographischer Algorithmen oder Protokolle werden fehlerfreie Testdaten (Testvektoren) benötigt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) begleitet und evaluiert dafür Botan. Es ist für viele Einsatzszenarien und Anwendungen mit erhöhtem Sicherheitsbedarf (z. B. VS-NfD) geeignet.

Für die Evaluation der Algorithmen wurde in Zusammenhang mit der Umsetzung einer universellen Testumgebung auch eine universelle Schnittstelle entwickelt. Mit deren Hilfe können die für die FPGA-Logik entwickelten kryptographischen Algorithmen leicht an das Prozessorsystem angeschlossen werden (vgl. Abb. 3).

In einer einfachen C  oder einer Python-Anwendung im Linux Betriebssystem PetaLinux konnten die Daten dann aus der universellen Testumgebung an den jeweiligen Algorithmus übertragen werden.

Partielle Rekonfiguration wurde eingesetzt, um im laufenden Betrieb unterschiedliche Algorithmen in den FPGA laden und testen zu können. In der Entwicklungsumgebung Vivado können über einen speziellen PR-Wizard Bereiche für die partielle Rekonfiguration in der FPGA-Logik reserviert und passende partielle Bitströme erzeugt werden. Diese können anschließend mit dem FPGA-Manager in PetaLinux in den FPGA geladen werden. Mit der Anwendung Bootgen ist darüber hinaus auch eine verschlüsselte Übertragung von Bitströmen möglich.

Die Erzeugung von Algorithmen für die FPGA-Logik erfolgte mit der Programmiersprache VHDL und Vivado sowie dem Software Development Kit (SDK) von Xilinx. Die simulierten Signale eines VHDL-Algorithmus zeigt beispielhaft Abb. 4.

Auf dem UltraZed-SOM Board wurde das TLS 1.3 Protokoll erfolgreich umgesetzt und davon einige Algorithmen zur Beschleunigung in die FPGA-Logik ausgelagert. Unter anderem wurden AES-256-GCM, AES-128-CCM (vgl. Abb. 5) und SHA-3 in VHDL erfolgreich implementiert.

Abb. 1: UltraZed SOM

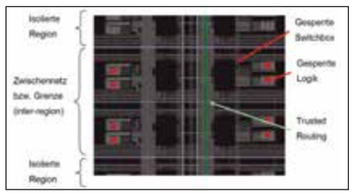


Abb. 2: Isolation Design Flow (IDF)

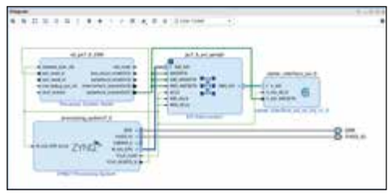

Abb. 3: Block-Design – Anschluss des VHDL-Algorithmus über die universelle Schnittstelle (cipher_interface) an das Prozessorsystem (ZYNQ)

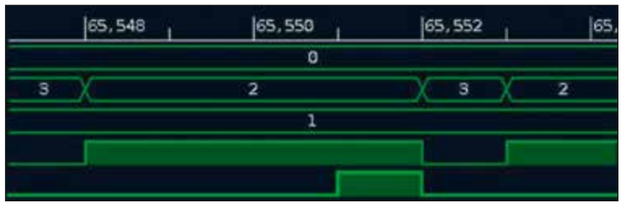


Abb. 4: Signalanalyse im Waveform-Window (Vivado von Xilinx)

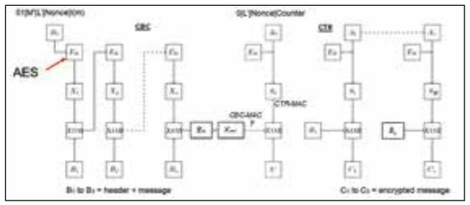


Abb. 5: AES-CCM – Beispiel zum Ablaufplan eines kryptographischen Algorithmus