



BMBF-Verbundprojekt: VE-VIDES

Förderkennzeichen: 16ME0253

Projektlaufzeit: 01.03.2021 bis 31.8.2024

Zuwendungsempfänger: Universität Ulm (UUlm)

Aufgabenbereich: A2

Titel: Sachbericht zum Abschluss des Teilprojekts „Fingerprints rekonfigurierbarer Schaltungen“ im Verbundvorhaben „*Designmethoden und HW/SW-Co-Verifikation für die eindeutige Identifizierbarkeit von Elektronikkomponenten*“

Art: Bericht

Fälligkeit: 28.2.2025

Erstelldatum: 07.02.2025

Autoren: Maurits Ortmanns, Holger Mandry, Universität Ulm

Ansprechpartner: Maurits Ortmanns
Institut für Mikroelektronik
Universität Ulm

Albert-Einstein-Allee 43

89081 Ulm

Telefon: +49 (0)7 31 / 50 26200

Fax: +49 (0)7 31 / 50 26222

e-mail: maurits.ortmanns@uni-ulm.de

Internet: <http://www.uni-ulm.de/in/mikro>

Inhalt

INHALT.....	3
1 KURZE DARSTELLUNG DES PROJEKTS.....	4
1.1 AUFGABENSTELLUNG.....	4
1.2 ZIELE.....	4
1.3 RANDBEDINGUNGEN UND VORAUSSETZUNGEN.....	5
1.4 PLANUNG UND ABLAUF DES VORHABENS.....	5
1.5 WISSENSCHAFTLICHER UND TECHNISCHER STAND VOR PROJEKTSTART.....	6
1.6 ZUSAMMENARBEIT MIT ANDEREN STELLEN.....	7
2 EINGEHENDE DARSTELLUNG DES TEILPROJEKTS UNI ULM.....	8
2.1 VERWENDUNG DER ZUWENDUNG UND ERZIELTE ERGEBNISSE.....	8
2.2 WICHTIGSTE POSITIONEN DES ZAHLENMÄßIGEN NACHWEISES.....	11
2.3 NOTWENDIGKEIT UND ANGEMESSENHEIT DER GELEISTETEN ARBEIT.....	11
2.4 VORAUSSICHTLICHER NUTZEN, INSBESONDERE VERWERTBARKEIT DER ERGEBNISSE IM SINNE DES FORTGESCHRIEBENEN VERWERTUNGSPLANS.....	11
2.5 WÄHREND DER DURCHFÜHRUNG DES VORHABENS BEKANNT GEWORDENE FORTSCHRITTE BEI ANDEREN STELLEN.....	12
2.6 ERFOLGTE VERÖFFENTLICHUNGEN DER ERGEBNISSE.....	12

1 Kurze Darstellung des Projekts

1.1 Aufgabenstellung

Die zunehmende Komplexität und Vernetzung elektronischer Systeme führt nicht nur zu erweiterten Funktionalitäten, sondern eröffnet auch zahlreiche Angriffsflächen. Solche Angriffe können erhebliche Folgen für Personen, Produktionsprozesse und Anlagen haben. Ein zentrales Angriffsszenario besteht in elektronischen oder physikalischen Attacken auf integrierte Schaltungen, um geistiges Eigentum zu entwenden oder die Funktionalität sowie gespeicherte Daten zu manipulieren.

Die Aufgabenstellung im Verbundprojekt VE-VIDES war, potenzielle Sicherheitslücken bereits in der Designphase systematisch zu identifizieren und elektronische Systeme durch automatisiert erzeugte, zuverlässige Schutzmechanismen vor Angriffen zu sichern. Dabei liegt der Fokus auf der Vertrauenswürdigkeit der System-Hardware (HW) sowie der direkten Schnittstelle zu sicherheitskritischen Software- und Firmware-Komponenten. Im Rahmen des Teilprojekts der Universität Ulm sollten zuverlässige elektronische Fingerprints aus rekonfigurierbaren digitalen Schaltungen, sogenannten Field Programmable Gate Arrays (FPGA), extrahiert werden. Dazu wird eine Bibliothek mit Architekturen für Fingerprintgeneratoren entwickelt. Die Entwurfsumgebung umfasst verschiedene Module, darunter die Erzeugung zufälliger Ausgangswerte (Source of Randomness), die Quellcodierung (Sourcecoding), Fehlerkorrekturmechanismen sowie Hashing-Verfahren.

Ein wesentliches Merkmal dieser Fingerprintgeneratoren ist ihre Robustheit gegenüber äußeren Einflüssen. Hierfür werden innovative Methoden erforscht, um den zusätzlichen Fehlerkorrekturaufwand auf ein Minimum zu reduzieren und somit die Gesamtkomplexität der Implementierung möglichst gering zu halten

1.2 Ziele

Durch innovative Entwurfsmethoden, die Bereitstellung einer Architekturbibliothek sowie Maßnahmen zur Erhöhung der Robustheit soll die strukturelle Vertrauenswürdigkeit eines Systems gezielt gesteigert werden.

Ein zentraler Bestandteil eines „Trusted Execution Environment“ (TEE), das als Vertrauensanker im System fungiert, ist die eindeutige Identifizierbarkeit. Diese sollte durch die Bereitstellung von Hardware-Fingerprints (im Arbeitspaket A2.4 von VE-VIDES) ermöglicht werden und stelle eine essenzielle Maßnahme dar, um Angriffe und Manipulationen zu erkennen.

Das zentrale Problem dieses Teilprojekts lag in der Entwicklung einer klar definierten, robusten Entwurfsmethodik sowie eines effektiven Ansatzes zur Erhöhung der Widerstandsfähigkeit gegenüber zeitlichen Schwankungen der Fingerprints – Aspekte, die in vielen wissenschaftlichen Arbeiten bislang nicht hinreichend adressiert wurden.

Neben der Erforschung von FPGA-Fingerprint-Architekturen, die schwer durch maschinelles Lernen oder Seitenkanalangriffe auslesbar oder vorhersagbar sind, sollte eine Architekturbibliothek entwickelt werden. Um die interne Verschleierung der Fingerprints zu erhöhen, wurde eine Rekonfigurierbarkeit der Architekturen avisiert, die selbst zufallsbasiert erfolgt.

Da elektronische Fingerprints stark von Umgebungsfaktoren wie Temperaturveränderungen und Alterung beeinflusst werden, sollte zusätzlich untersucht werden, wie diese Abhängigkeiten durch gezielte Architekturauswahl oder geeignete Korrekturverfahren minimiert werden können.

1.3 Randbedingungen und Voraussetzungen

Das Verbundvorhaben war so aufgebaut, dass alle Teilnehmer der Wertschöpfungskette vertreten

waren. Die beabsichtigten Arbeiten an der Universität Ulm fokussierten dabei auf eine Schlüsselkomponente moderner Elektroniksysteme, dem sogenannten FPGA. Kernkompetenz des Instituts für Mikroelektronik der Universität Ulm im Gesamtverbund war die Expertise beim Entwurf physikalisch unklonbarer Funktionen.

1.4 Planung und Ablauf des Vorhabens

Das Verbundvorhaben startete am 01.03.2021 in Kooperation mit Fraunhofer Institut IIS/EAS, IMMS gemeinnützige GmbH, OFFIS, OneSpin Solutions GmbH, Robert Bosch GmbH, Siemens AG, Synopsys GmbH, TU Chemnitz, Volkswagen car.SW Org Wolfsburg AG, X-FAB Global Services. Das Verbundprojekt war in folgende Teilprojekte aufgeteilt:

1. AP1: Anforderungen an Vertrauenswürdigkeit von IP und Designflow
2. AP2: Vertrauenswürdige Design-Strukturen
3. AP3: Verifikation der Vertrauenswürdigkeit
4. AP4: Demonstrator-Entwicklung und System-Integration
5. AP5: Prozess und Monitoring über die Lieferketten

Der wesentliche Beitrag der Universität Ulm lag dabei im Teilprojekten 2.4. Fingerprinting. Die Aufgaben wurden dafür in folgenden Arbeitspaketgruppen (APG) eingeteilt:

AP2.4: Identifikation von Systemkomponenten mit Fingerprints:

- 2.4.6 *Automatisierte Charakterisierungsverfahren für FPGA Fingerprints*
- 2.4.7 *Design-, Verifikations- und Evaluationsflows für Fingerprints*
- 2.4.8 *Bibliothekskomponenten für FPGA Fingerprints*
- 2.4.9 *Rekonfigurierbarkeit von FPGA Fingerprint Architekturen*
- 2.4.10 *Stabilisierung von FPGA Fingerprints*
- 2.4.11 *Integration in eine Demonstrator Umgebung*

Die sich ergebenden Meilensteine für den Projektpartner Uni Ulm waren dabei:

Meilenstein	Quartal	Inhalt
D03-2D	Q03	Design- und Evaluationsflow für FPGA und MEMS basierte Fingerprints
D06-2C	Q06	Erster Entwurf für Fingerprinting-Komponenten
D10-2C	Q10	Evaluation der MEMS- und FPGA Fingerprints
D12-2D	Q12	Bericht zur Identifikation von Systemkomponenten mit Fingerprints

Zusammenfassend hat ein Grund für eine Verzögerung in vielen Arbeitspaketen geführt: Wegen Personalfindung konnte Mitarbeiter 1 nicht zum 1.10.2021, sondern erst mit 3-monatiger Verspätung zum 1.1.2022 eingestellt werden, wodurch sich mehrere Verschiebungen der aufeinander aufbauenden Arbeitspakete ergaben. Aus diesem Grund wurde seitens des Projektträgers einer kostenneutralen Projektverlängerung bis zum 31.08.2024 zugestimmt.

Zusammenfassend kann gesagt werden, dass alle Meilensteine vollständig in der Projektlaufzeit erreicht wurden. Die FPGA Systeme stehen prototypisch bereit und können den Verbundpartnern zur Verfügung gestellt werden.

1.5 Wissenschaftlicher und technischer Stand vor Projektstart

Fingerprints von Bauelementen werden in der Literatur vielfach im Themengebiet der Physical Unclonable Functions (PUF) beschrieben. Solche Fingerprints sind sowohl in passiven Strukturen wie Beschichtungen zu finden, werden aber am ehesten als elektronische PUF als Schaltungen auf Si-Chips realisiert. Dabei werden technologische Toleranzen im Herstellungsprozess ausgenutzt, um eine Quelle für eindeutige Zufälligkeit zu finden. Nach geeigneter Aufarbeitung dieser zufälligen Quelle kann mit geeigneter Digitalisierung ein einzigartiger Bitstring erzeugt werden [2]. Sogenannte schwache PUFs lesen diesen Bitstring als eindeutiges Erkennungsmuster aus und werden zum Beispiel zur Identifikation nutzbar gemacht. Sogenannte starke PUFs benötigen zudem einen digitalen Eingang, aufgrund dessen eine Vielzahl digitaler zufälliger Bitstrings erzeugt wird, was z.B. für kryptografische Schlüssel nutzbar ist. Eine wichtige Eigenschaft bei der Erzeugung der zufälligen, aber einmaligen Bitstrings zur Identifikation ist deren Unempfindlichkeit gegenüber Umgebungsschwankungen wie Temperatur und Alterung, deren Stabilität bei wiederholter Auslese, sowie deren eindeutige Unterscheidbarkeit von Device zu Device. Es gibt dabei vollständige elektronische (SRAM, DRAM, FPGA, Coating, ...), optische, RF-, oder auch auf sensorischen Strukturen basierende Quellen von Zufälligkeit. Die Identifikation von Systemkomponenten aufgrund von devicespezifischen Fingerprints bietet die Möglichkeit, zufällige und nicht reproduzierbare Schaltungsvariationen für die Generierung einer eindeutigen ID zu nutzen. Insbesondere rekonfigurierbare digitale Schaltungen wie FPGAs bieten dabei die Möglichkeit, die Hardware sowohl funktional als auch zur Gewinnung einer ID zu verwenden [3]. Der Stand der Technik zeigt dabei hauptsächlich Möglichkeiten, die Lern- und damit Angreifbarkeit dieser ID zu verkleinern [4]. Ebenfalls existieren Implementierungen, um den Platz- und Energieverbrauch zu minimieren [5] sowie die Noise-Anfälligkeit zu reduzieren [6]. Ein weiterer Forschungsschwerpunkt ist die Bildung von Strong PUFs auf FPGAs [7] z.B. auch zur Erzeugung vieler auswählbarer Fingerprints. Eine Stabilisierung gegenüber Umgebungsvariablen [8], eine geschlossene Entwurfsmethodik zur Integration von Fehlerkorrektur in Soft- oder Hardware [9] sowie die mehrwertige Auslese zur Erhöhung der Entropie (d.h. große zufällige Bitstrings aus wenig Hardware [10] sind erst unzureichend untersucht und nicht im Stand der Technik etabliert, und bedürfen für eine breite Anwendung dieser Verfahren weiterer auf die Anwendung fokussierter Forschung.

[2] Christoph Böhm, Maximilian Hofer: "Physical Unclonable Functions in Theory and Practice", Springer, 2013

[3] Andreas Herkle, Holger Mandry, Joachim Becker, Maurits Ortmanns, "In-depth Analysis and Enhancements of RO-PUFs with a Partial Reconfiguration Framework on Xilinx Zynq-7000 SoC FPGAs", 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, DOI: 10.1109/HST.2019.8740832

[4] Fatemeh Ganji, Shahin Tajik, Jean-Pierre Seifert, "Why Attackers Win: On the Learnability of XOR Arbiter PUFs", Trust and Trustworthy Computing. Trust 2015, DOI: 10.1007/978-3-319-22846-4_2

[5] R. Likhithashree, Divya Kiran, "Design of Power-Efficient Ring Oscillator based Physically Unclonable Functions for FPGA", 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India, DOI: 10.1109/ICEECCOT46775.2019.9114656

[6] Abhranil Maiti, Patrick R Schaumont, "Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive", 2011, Journal of Cryptology DOI: 10.1007/s00145-010-9088-4

[7] Zouha Cherif, Jean-Luc Danger, Sylvain Guilley, Lilian Bossuet, "An Easy-to-Design PUF Based on a Single Oscillator: The Loop PUF", 2012 15th Euromicro Conference on Digital System Design, Izmir, Turkey, DOI: 10.1109/DSD.2012.22

[8] Chi-En Yin, Gang Qu, "Temperature-aware cooperative ring oscillator PUF", 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, CA, USA, DOI: 10.1109/HST.2009.5225055

[9] Holger Mandry, Andreas Herkle, Ludwig Kürzinger, Sven Muelich, Joachim Becker, Robert F.H. Fischer, Maurits Ortmanns, "Modular PUF Coding Chain with High-Speed Reed-Muller Decoder", 2019 IEEE International Symposium on Circuits and Systems (ISCAS), DOI: 10.1109/ISCAS.2019.8702484

[10] Holger Mandry, Andreas Herkle, Sven Muelich, Joachim Becker, Robert F. H. Fischer, Maurits Ortmanns, "Normalization and Multi-Valued Symbol Extraction from RO-PUFs for Enhanced Uniform Probability Distributions", 2020, IEEE Transactions on Circuits and Systems II, DOI: 10.1109/TCSII.2020.2980748

1.6 Zusammenarbeit mit anderen Stellen

Das gesamte Verbundprojekt wurde in Zusammenarbeit mit den genannten Verbundpartnern bearbeitet. Wie in der Teilprojekt-Aufteilung beschrieben, erfolgte die Haupttätigkeit der Uni Ulm in den Arbeitspunkten AP2.4, welches die Identifikation von Systemkomponenten mit Fingerprints zum Ziel hatte. Eine Abstimmung von Verfahren dazu fand überwiegend mit TU Chemnitz statt, wo ähnliche Ziele auf Grundlage von MEMS-Sensoren avisiert wurden. In Telefonkonferenzen wurden Entwürfe und Arbeitsfortschritte gegenseitig überprüft und korrigiert, um eine optimale Implementierung gewährleisten zu können. Weitere spontane Treffen fanden mit dem Verbundpartner BOSCH statt, um über verschiedene PUF Architekturen zu diskutieren.

Eine Abstimmung mit den übrigen Verbundpartnern fand während der regelmäßigen Verbundtreffen statt. Durch den zustande gekommenen Austausch konnte die fachliche Expertise aller Projektpartner optimal eingesetzt werden.

2 Eingehende Darstellung des Teilprojekts Uni Ulm

2.1 Verwendung der Zuwendung und erzielte Ergebnisse

AP2.4.6, Physikalisch Unklonbare Funktionen und daraus abgeleitete Fingerprints müssen mehrere charakteristische Merkmale aufweisen, um als eindeutige Identifizierungsmerkmale nutzbar zu sein. Aufgrund der großen Menge an benötigten Daten, um statistisch signifikante Aussagen erhalten zu können, ist eine manuelle Auswertung nicht umsetzbar. Daher wurden im Zuge dieses Beitrages diverse Methodiken zur Bewertung der Eigenschaften auf ihre Anwendbarkeit evaluiert und in einer gemeinsamen Plattform zur automatischen Charakterisierung implementiert. Hierbei standen FPGAs als Hardware im Vordergrund, insbesondere was Metriken bezüglich Rechenzeit und Platzverbrauch betrifft.

AP2.4.7, da Fingerprintgeneratoren nicht nur aus der Source of Randomness, sondern noch aus weiteren verarbeitenden Kettengliedern, wie beispielsweise Codierung, Fehlerkorrektur oder Hashing, besteht, wurden diese in einem ersten Schritt identifiziert. Daraufhin wurde eine modulare Fingerprintgenerator-Kette für FPGAs entworfen. Diese bildet die einzelnen Verarbeitungsschritte als einzelne Module ab und erlaubt somit den Austausch und eine unabhängige Bewertung einzelner Komponenten der Kette. Die Modularisierung erlaubt die nachträgliche Ergänzung, um weitere nötige Verarbeitungsschritte, ohne die bestehenden Komponenten anpassen zu müssen. Zur schnellen Entwicklung und Bewertung von Algorithmen kann jedes Modul unabhängig in Hardware oder Software implementiert werden. Parallel dazu wurde im Zuge einer studentischen Abschlussarbeit ein zusätzliches Framework entwickelt, welches den Angriff auf Fingerprints mittels maschineller Lernverfahren erlaubt. Über Modelle der internen Architektur ist es hierbei möglich verschiedene Architekturen zu simulieren und deren Angreifbarkeit zu bewerten.

In **AP2.4.8** wurden speziell für FPGAs geeignete Fingerprintgeneratoren evaluiert. Die limitierte Kontrolle über das interne Routing stellte dabei eine besondere Herausforderung dar. In einem ersten Schritt wurden „weak“ Ring-Oszillator-PUFs implementiert und ausgewertet. Eine weak PUF besitzt keinen Challenge-Eingang und liefert immer dasselbe Bitmuster am Ausgang und wird daher als Fingerprintgenerator genutzt. Die Struktur einer Ringoszillator PUF ist besonders für FPGAs geeignet, da ein symmetrisches Routing nicht benötigt wird. Mithilfe der Plattformen aus den Arbeitspaketen 2.4.6 und 2.4.7 konnte diese PUF Architektur implementiert und evaluiert werden.

Im weiteren Verlauf wurden verschiedene Ansätze zur mehrwertigen Auslese der einzelnen Zellen entworfen und evaluiert. Diese ermöglichten es mehrere Bits je Ringoszillator Zelle zu extrahieren, und dies verringerte den benötigten Ressourcenverbrauch auf dem FPGA deutlich. Mithilfe des modularen Ansatzes aus Arbeitspaket 2.4.7 war es möglich, schnell mehrere Verfahren gegeneinander zu vergleichen. Diese erlaubten es die Anzahl der extrahierten Bits je Zelle zu verdreifachen.

Schwankungen im Ausleseprozess erzeugen Fehler in den extrahierten Bits. Um diese Fehler zu korrigieren, wurde ein Fehlerkorrektur-Code in Software und Hardware implementiert. Dies erlaubte es je nach Anwendung langsame aber platzsparende Software oder schnellere jedoch mehr FPGA-Komponenten benötigende Hardware zu benutzen. Zusätzlich erlaubt eine Wahl der Code-Parameter eine Justierung der Mächtigkeit des Codes.

In einem weiteren Schritt wurde eine Eye-Opening Arbiter PUF als weitere Fingerprintgenerator-Architektur entworfen und implementiert. Diese neuartige Architektur kombiniert die schnelle Auslese der bekannten Arbiter-PUF-Architektur mit den selbststabilisierenden Eigenschaften der Ringoszillator-PUF. Durch die neue Architektur konnte die Auslesegeschwindigkeit je Bit verzehnfacht werden. Ein zusätzlicher Challenge-Eingang erlaubt die Extraktion mehrerer unabhängiger PUF-Responen aus einer Hardware-Komponente, was den benötigten Platzverbrauch je Bit weiter reduzierte.

AP2.4.9 Jede PUF liefert für verschiedene Challenges unterschiedliche, aber eindeutige Responses. Die Paare aus Challenge und zugehöriger Response werden Challenge-Response-Pair (CRP) genannt. Aus einem bekannten Satz CRPs lassen sich mithilfe maschineller Lernverfahren weitere CRPs vorhersagen und somit die PUF brechen. Dieser Angriff wird begünstigt, da in PUFs oft lineare Abhängigkeiten in der internen Struktur existieren, welche gut durch neuronale Netze lernbar sind. Im Stand der Technik wird die Lernbarkeit der PUF meist mit dem Prediction-Error des neuronalen Netzes über die Anzahl der im Training verwendeten CRPs dargestellt. Der Prediction-Error beschreibt hierbei den Fehler, den das neuronale Netz nach dem Training bei der Vorhersage der PUF-Bits macht. Dabei wird ein Wert von 0.5 (entspricht 50 %) angestrebt, was zufälligem Erraten der Response entspricht. Gleichzeitig soll dieser Wert für eine möglichst große Anzahl an CRPs erreicht werden, da davon auszugehen ist, dass ein Angreifer nicht alle CRPs sammeln kann. Um dies zu verhindern, wurde im Rahmen dieses Beitrags untersucht, wie durch Rekonfiguration die Lernbarkeit einer PUF erschwert werden kann.

Um dieses Ziel zu erreichen, wurde ein rundenbasiertes System mit mehreren Substitutions- und Permutations-Stufen implementiert. Die Substitutions-Stufen „scrambeln“, d.h. zerwürfeln dabei die eingehende Challenge mit mehreren Bits aus Weak-PUFs mittels XOR-Operationen. Die XOR-Operation hat den Vorteil, dass aus ihrem Ausgang nicht auf die genaue Eingangskombination rückgeschlossen werden kann. Die Weak-PUFs wurden aus den in Arbeitspaket 2.4.8 entwickelten Ringoszillator-PUFs abgeleitet. In einem ersten Testlauf konnte das „angreifende“ neuronale Netz auch mit 10^7 CRPs nicht ausreichend trainiert werden, um die PUF vorherzusagen. Bei einer Standard-Arbiter-PUF genügen hierfür bereits wenige tausend CRPs. D.h. die Sicherheit wurde durch diese Maßnahme um mehrere Größenordnungen verbessert. In zukünftig geplanten Arbeiten soll dieses Verfahren flächenmäßig reduziert und an die Eye-Opening Arbiter PUF angepasst werden.

In einem zweiten Ansatz wurde die zweite PUF-Primitive aus Arbeitspaket 2.4.8, die Eye-Opening Arbiter PUF, gegen Angriffe mittels maschinellen Lernens geschützt. Mittels des Ansatzes einer Lattice-PUF Struktur war es möglich den Prediction-Error für 10^7 bisher evaluierte CRPs auf dem idealen Wert von 0.5 zu halten. Hierbei wird eine Challenge abschnittsweise verarbeitet und mit der PUF-Response verrechnet. In einem weiteren Schritt konnte das Verfahren verbessert werden, um möglichst wenig Hardware zu benötigen.

Im Laufe des Projektes wurde ein weiterer Angriffsvektor mittels sogenannter Seitenkanalanalysen als Gefahrenquelle identifiziert. Dabei schneidet ein Angreifer den Energieverbrauch der Schaltung über einen gewissen Zeitraum mit und kann dadurch Rückschlüsse auf internes Verhalten und Frequenzen der verwendeten Ringoszillatoren ziehen. Dies erlaubt die Berechnung der geheimen Fingerprints. Lange Oszillationszeiten, die für stabile PUF-Responses nötig sind, erhöhen dabei die Genauigkeit des Angriffs. Um dem Entgegenzuwirken wurde eine neue Architektur implementiert, die es erlaubt laufende Oszillationen zu unterbrechen, ohne die bereits ermittelte Frequenzdifferenz zu verlieren. Dabei war es möglich, die aktiven Phasen so kurz zu wählen, dass der Angreifer keine verwertbare Information mehr extrahieren konnte. Gleichzeitig bleibt die geheime Information für die Anwendung erhalten.

AP2.4.10 Im Zuge des Arbeitspaketes wurden die Veränderungen der Antworten der PUF Strukturen aus Arbeitspaket 2.4.8 gegenüber Temperaturschwankungen evaluiert und deren Einfluss minimiert.

Die verwendeten Ringoszillator PUF-Zellen zeigen auf FPGAs ein nichtlineares Verhalten über Temperatur, welches zu einer Änderung der PUF Antwort und somit einer wachsenden Fehlerrate bei Temperaturschwankungen führt. Durch Interpolation mit Polynomen verschiedener Grade wurde dieses Verhalten nachgebildet. Mithilfe dieser Polynome als sogenannte „Helper Daten“ ist es möglich, den Einfluss der Temperatur auf eine aktuelle Auslese algorithmisch zu minimieren und somit die Komplexität einer weiteren Fehlerkorrektur zu verbessern. Da diese Helper Daten keinerlei Rückschlüsse auf die geheime Information der PUF Auslese zulassen dürfen, wurde ein Algorithmus gefunden, der nur den gespeicherten Verlauf des Polynoms benötigt. Die sicherheitskritische Information wird dann nur aus der aktuellen Messung abgeleitet.

Für die Eye-Opening-Arbiter PUF konnte ein weiteres stabilisierendes Verfahren entwickelt werden. Hierzu wurde die selbststabilisierende Eigenschaft der PUF Architektur ausgenutzt. Die PUF oszilliert, bis eine eindeutige Entscheidung getroffen werden kann. Instabilere Zellen, welche stärker von äußeren Schwankungen beeinflusst werden, benötigen mehr Zeit, um eine finale Entscheidung zu treffen. Hier konnte ein Algorithmus entwickelt werden, der diese Zellen on-board, ohne externe Analyse, identifiziert und markiert. Durch sogenanntes Blanken (d.h. markiertes Nicht-Nutzen) der entsprechenden Zellen für den abgeleiteten Fingerabdruck lässt sich dieser gegenüber Temperaturschwankungen stabilisieren.

AP2.4.11 Um die evaluierten Architekturen flexibel auf verschiedenen FPGAs einsetzen zu können, wurde der Sourcecode durch Parametrisierung individuell anpassbar gemacht.

Für das Auslesen und Fingerprint-Generierung eines kompletten FPGA mittels RO-PUF, stehen Skripte zur Bitstream Erzeugung auf verschiedenen Boards zur Verfügung. Zur Auswertung wurde ein Python-Skript geschrieben, das über UART mit dem FPGA kommuniziert. Die EoA-PUF lässt sich in bestehenden FPGA code integrieren. Diese Bibliothek kann den Verbundpartner damit zur Nutzung zur Verfügung gestellt werden.

Damit sind alle Projektziele im Teilprojekt der Universität Ulm erreicht.

2.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Für das Teilprojekt des Projektpartners Uni Ulm wurde ein **Budget von 281.622,00€** zur Verfügung gestellt. Das Projekt wurde über das geplante Projektende am 28.02.2024 hinaus kostenneutral bis zum 31.08.2024 verlängert, um die Verzögerungen, die sich durch Probleme der Personalfindung ergaben, zu kompensieren.

Die geplanten Kosten wurden mit entstandenen Ausgaben von 277.873,13€ nicht überschritten.

Genehmigten 217.220,00€ standen verausgabten 261.920,66€ Personalkosten in Pos. 0812 gegenüber. Es wurden damit in diesem Bereich die geplanten Kosten überschritten, was an mehreren Faktoren lag: Da weniger wissenschaftliche Hilfskräfte gefunden werden konnten als ursprünglich geplant, wurde zeitweise ein dritter Mitarbeiter eingestellt, um die Projektziele zu erreichen. Dies war ebenso hilfreich, um trotz des durch Personalfindung verzögerten Projektstarts alle Projektziele zu erreichen. Darüber hinaus wurde zur Erreichung der Projektziele eine kostenneutrale Verlängerung des Projekts bis zum 31.8.2024 beantragt und genehmigt. Dies führte zusammengekommen zu einer Überbuchung von Position 0812 und Unterbuchung von Position 0822.

Neben den Doktorandenstellen wurden auch Hilfswissenschaftler im Volumen von 10.804,67€ im Projekt beschäftigt. Dem gegenüber stehen genehmigte Beschäftigungsentgelte von 34.042,00€.

Außerdem konnten im Projekt eine große Zahl von Bachelor- und Masterarbeiten betreut und abgeschlossen werden, von welchen Resultate auch in das Projekt einfließen.

Es war im Projekt die Anschaffung von 350 gleichwertigen FPGA Boards zur experimentellen Validierung der FPGA-Fingerprints geplant. Diese waren in 0843 in Höhe von 19.610,00€ beantragt. Aufgrund des Chip-Mangels in Folge der Corona-Pandemie konnten zeitnah zum Projektstart keine gleichwertigen Boards in ausreichender Stückzahl beschafft werden. Alternativ wurde auf vorhandene Boards des Fraunhofer AISEC (Projektpartner im Projekt VE-FIDES) zurückgegriffen. Der dadurch entstandene Mehraufwand wurde durch zusätzliche Mitarbeiter aufgefangen. Die gebuchten 2.878,55€ entfallen auf ein FPGA-Board zur Seitenkanalanalyse, sowie mehrerer Kleinteile und Verbrauchsmaterialien.

Beantragten 10.750€ stehen verausgabten 2.269,25€ Reisekosten (0846) gegenüber. Da Projekttreffen und Konferenzen vermehrt online abgehalten wurden, sind die Reisekosten insgesamt geringer ausgefallen, als im Voraus kalkuliert.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Alle im Arbeitsplan vorgesehenen Entwicklungsaufgaben des Projektpartners Uni Ulm wurden **vollends abgeschlossen und erfolgreich publiziert**. Die entwickelten Schaltungen stellen einen sichtbaren Fortschritt im Stand der Technik für FPGA Fingerprints dar, da sie sowohl die Stabilität, als auch die Resistenz gegen Angriffe erhöhen.

2.4 Voraussichtlicher Nutzen, insbesondere Verwertbarkeit der Ergebnisse im Sinne des fortgeschriebenen Verwertungsplans

Die Arbeitsergebnisse des Projektpartners Uni Ulm aus VE-VIDES stehen den Projektpartnern zur Verfügung. Es konnten wissenschaftliche Publikationen erzielt werden. Es sind weitere geplante Publikationen nach Projektabschluss im Review-Prozess. Es wurden zahlreich Studierende im Bereich der Hardware Security, des FPGA Design und verwandter Themen im Rahmen des Verbundprojekts und ihrer Abschlussarbeiten und Hilfswissenschaftlertätigkeit ausgebildet.

2.5 Während der Durchführung des Vorhabens bekannt gewordene Fortschritte bei anderen Stellen

Es wurden in den vergangenen Jahren vielfältige Publikationen im FPGA PUF Bereich getätigt, welche beispielsweise die Fehlerrate durch komplexe korrigierende Codes verbessern.

Das Hauptziel der Universität Ulm im Projekt VE-VIDES war es hingegen die PUF- und Fingerprint-auslesen selbst stabiler zu machen und somit einfache und ressourcenarme korrigierende Codes verwenden zu können.

Auf diese Weise sind im Projekt praktisch relevante Problemstellungen behandelt worden, die andernorts oftmals vernachlässigt werden.

2.6 Erfolgte Veröffentlichungen der Ergebnisse

Wissenschaftliche Fachzeitschriften:

Konferenzbeiträge:

Ein Konferenzbeitrag ist kürzlich auf der IEEE ICECS 2024 angenommen worden.

Veröffentlichung in Fachjournal:

Ein Fachjournalartikel ist bei der IARC TCHES für die Veröffentlichung akzeptiert.

Dieser Block kennzeichnet das Ende des Dokuments

Kurzbericht

Die Automatisierung mithilfe intelligenter, elektronischer Systeme durchdringt unsere Wirtschaft und Gesellschaft immer mehr. Komplexe Systeme wie beispielsweise das hochautomatisierte Fahren oder intelligente Maschinen machen unser Leben und Arbeiten immer effizienter und angenehmer. Sie stellen aber auch eine potenzielle Gefahr dar, weil diese Systeme heute nicht von Anfang an mit dem klaren Ziel der Vertrauenswürdigkeit entwickelt werden. Ein Angriff auf das System beeinträchtigt potenziell die beabsichtigte Funktionalität und kann so zu wirtschaftlichen, technischen und körperlichen Schäden führen. Der Projektvorschlag setzt den Fokus der Innovation auf die Absicherung von Hardware gegen sicherheitskritische Angriffe (Cyber Security) und berücksichtigt zudem die unmittelbare Schnittstelle zu vertrauenswürdigen Software-/Firmware-Komponenten. Die steigende Komplexität von elektronischen Systemen und ihre starke Vernetzung ermöglichen nicht nur mehr Funktionalität, sondern auch eine Vielzahl von Möglichkeiten für Angriffe auf diese Systeme, die kritische Auswirkungen auf Personen, Produktion und Anlagen haben können. Ein wesentliches Angriffsszenario auf Elektroniksysteme ist z.B. elektronische oder physikalische Angriffe auf integrierte Schaltungen, um geistiges Eigentum zu stehlen, oder Funktionalität bzw. Daten zu modifizieren. Das Gesamtvorhaben VE-VIDES zielt darauf ab, potenzielle Sicherheitslücken bereits im Design systematisch zu identifizieren und Elektroniksysteme mithilfe automatisiert erzeugter, zuverlässiger Mechanismen vor Angriffen zu schützen. Um diesem Problem zu begegnen, war das Ziel des Teilprojekts elektronische Fingerprints zuverlässig von rekonfigurierbaren digitalen Schaltungen, sog. Field Programmable Gate Arrays (FPGA), zu extrahieren. Dabei sollte eine Bibliothek von Architekturen für solche Fingerprintgeneratoren entstehen, wobei für die verschiedenen zu implementierenden Blöcke, die Source of Randomness, das Sourcecoding, die Fehlerkorrektur und das Hashing, eine Entwurfsumgebung realisiert werden sollten. Eine wichtige Eigenschaft solcher Fingerprintgeneratoren ist, dass sie gegenüber Umgebungseinflüssen unempfindlich sind. Hierfür sollten neuartige Methoden entwickelt werden, welche die zusätzlich benötigte Fehlerkorrektur möglichst rudimentär halten, um damit die Gesamtkomplexität der Realisierung möglichst gering zu halten.

Im Rahmen des geförderten Projektes sind von der Universität Ulm mehrere sogenannte Physikalisch Unklonbare Funktionen zur Fingerprint Extraktion entworfen, implementiert und stabilisiert worden. Zunächst wurde eine modulare Entwicklungs- und Evaluierungsplattform für FPGAs entworfen und implementiert. Diese ermöglicht einen ebenenübergreifenden Design-, Verifikations- und Evaluationsflow verschiedenster PUF-Architekturen auf FPGAs. Durch einen modularen Aufbau ist es hierbei möglich die einzelnen Arbeitsschritte einer kompletten PUF-Fingerprinting Kette einzeln sowohl in Hardware als auch in Software zu implementieren und evaluieren. In einem weiteren Schritt wurde diese Plattform genutzt, um verschiedene PUF- und Fingerprint-Architekturen zu implementieren und auf ihre Eigenschaften zu untersuchen. Mithilfe von Ringoszillator basierten PUFs war es somit möglich ganze FPGAs eindeutig zu identifizieren. Im weiteren Verlauf des Projekts war es möglich, die extrahierten Fingerprints zu verbessern. Durch neue Quantisierungsverfahren konnten mehrere Bits pro Ringoszillator-Zelle extrahiert werden, was den Flächenverbrauch pro Bit deutlich reduziert hat. Des Weiteren wurde das Temperaturverhalten der Ringoszillatoren untersucht. Dieses hat Einfluss auf die Stabilität, da sich Frequenzänderungen über Temperatur auf die Response auswirken. Durch ein neu entwickeltes Verfahren mittels polynomialer Interpolation war es möglich, den Einfluss der Temperatur auf die Response zu minimieren, so dass eine folgende Fehlerkorrektur weniger Komplexität benötigt. Im Zuge des Projekts wurde von der Universität Ulm eine weitere hybride Architektur erstmalig implementiert. Diese Eye-Opening-Arbiter PUF vereint die vorteilhaften Eigenschaften zweier bereits bekannter Architekturen: Die schnelle Auslese der Arbiter-PUF mit der stabilisierenden



Eigenschaft der Ringoszillator basierten PUF. Durch weitere Analysen konnten die speziellen Eigenschaften dieser neuen Architektur auch dazu genutzt werden, eine automatische Detektion verbleibender instabiler Zellen zu finden. Dies erlaubt eine on-board Identifizierung dieser Zellen, ohne eine aufwändige externe Analyse. Somit ist es auch nicht mehr nötig zur Charakterisierung die geheime Information aus dem Chip zu extrahieren.

Ein weiterer Forschungsschwerpunkt war die Resistenz der Architekturen gegen Angriffe von außen. Hierbei sind maschinelle Lernverfahren ein sehr prominentes Problem, da sie mit wenigen Auslesen Kenntnisse über die internen linearen Abhängigkeiten erlangen und somit weitere Responses vorhersagen können. Im Rahmen des Projekts wurden zwei Ansätze zum Schutz der entworfenen PUF-Architekturen vor Angriffen mit maschinellen Lernverfahren implementiert und erfolgreich evaluiert. Ein zweiter Angriffsvektor sind sogenannte Seitenkanalanalysen. Dabei kann der Angreifer über Analyse des Stromverbrauchs auf die internen Rechenoperationen, beziehungsweise im Fall von Ringoszillatoren auf deren Frequenz rückschließen. Somit können Fingerprints gebrochen werden. Um dem entgegen zu wirken, wurde eine neue Art von Ringoszillator entwickelt. Diese erlaubt es die laufenden Oszillationen zu unterbrechen und somit die Frequenzanalyse zu verwischen.

Die entwickelten Konzepte und FPGA Designs stehen nach erfolgreicher Testung den Projektpartnern zur Verfügung.

Von der Universität Ulm sind alle Arbeitspunkte des Projektes vollumfänglich bearbeitet und erfolgreich abgeschlossen worden. In diesem Rahmen ist eine große Anzahl von Bachelor- und Masterarbeiten bearbeitet worden.

Die erzielten Ergebnisse sind erfolgreich in publiziert worden, bisher unter anderem im IACR TCHES sowie IEEE ICECS, welche im vorliegenden Themenkomplex als renommierte Fachjournale/konferenzen gelten.