SecForCARs

security for connected automated cars

Security **For C**onnected, **A**utonomous ca**Rs**

– Schlussbericht –

Zuwendungsempfänger:	Technische Universität München
Förderkennzeichen:	16KIS0795
Laufzeit des Vorhabens:	01.04.2018-31.03.2021; verlängert bis 31.12.2021
Verantwortlicher:	Prof. Dr.-Ing. Georg Sigl
Autoren:	Christoph Frisch, Lars Tebelmann, Michael Pehl

Kurzdarstellung des Vorhabens

Vor dem Hintergrund eines rapide steigenden Vernetzungsgrades von Fahrzeugen und des sich abzeichnenden Trends zu hoch automatisierten und autonomen Fahrzeugen („Connected, Autonomous caRs“ = CARs), müssen IT-Sicherheit (Security) und die möglichen Folgen für die funktionale Sicherheit (Safety) gemeinsam betrachtet werden. Im Fokus stehen bei CARs die verteilten Regelkreise startend vom Sensor über die in den Steuergeräten zu verarbeitenden Sensordaten bis zu den Aktuatoren. Im vernetzten Fahrzeug wird neben den eigenen Sensoren auch auf Informationen von externen Sensoren und auf weitere Dienste über Kommunikationsnetze zugegriffen. Diese Prozesse erzeugen besondere Herausforderungen für die Automotive Security. Entstehende Schwachstellen müssen durch einen systematischen Security Entwurfsprozess bereits beim Systemdesign eliminiert werden. Um mögliche Schwachstellen aufzudecken, sind Sicherheitstests als elementarer Bestandteil des Entwicklungsprozesses bei CARs mehr noch als bei heutigen Fahrzeugen unverzichtbar. Solche Tests sind wichtiger Bestandteil einer Security- und Safety-Analysemethodik, welche die Grundlage für die Entwicklung von Sicherheitsarchitekturen und Sicherheitsmechanismen bildet. Beide Aspekte wurden im Projekt SecForCARs eng gekoppelt untersucht und genutzt für die Entwicklung entsprechender Architekturen und Mechanismen sowie Testumgebungen für Entwicklung und Evaluation von Testmethodik und –tools.

Aufgabenstellung

Der Lehrstuhl für Sicherheit in der Informationstechnik der Technischen Universität München forschte im Projekt „Security For Connected, Autonomous caRs” (SecForCARs) insbesondere zu möglichen Mechanismen für die Sicherheitsarchitektur und Sensor-Sicherheit, sowie zur Absicherung der in SecForCARs entwickelten Plattform und ihrer/deren Kommunikation mit anderen Komponenten. Das übergeordnete Ziel des Lehrstuhls war, in Zusammenarbeit mit den Partnern, Sicherheitsmechanismen für die Authentifizierung von Sensoren gegenüber der Engine Control Unit (ECU) zu entwickeln. Dazu wurden auf Physical Unclonable Functions (PUFs) basierende Protokollen verwendet, die den Schwerpunkt der Forschung am Lehrstuhl für Sicherheit in der Informationstechnik in diesem Projekt bildeten.

Voraussetzungen unter denen das Vorhaben durchgeführt wurde

Ebenso wie in vielen anderen Bereichen des Internet-of-Things (IoT) bzw. von vernetzten Sensor-Aktor-Systemen stellt die Entwicklung selbstfahrender Fahrzeuge größte Herausforderungen an die IT-Sicherheit. Da im Fahrzeugbereich Security und Safety eng miteinander verbunden sind, kommt der Absicherung aller Komponenten eines CARs eine erhöhte Bedeutung zu. So ist beispielsweise beim Austausch von Komponenten zu gewährleisten, dass diese etwaigen Sicherheitsanforderungen in Sinne der Safety umsetzen und diese nicht durch minderwertige Ersatzteile unterwandern.

Der Lehrstuhl für Sicherheit in der Informationstechnik forscht dabei u.a. an PUF-basierten Hardwaresicherheitsankern und deren Resistenz gegenüber physikalischen Angriffen, mit dem Ziel sensible Geräte gegen Angriffe abzusichern. Weiterhin zielt die Forschung im Gebiet von Fehlerkorrektur und PUF-Protokollen auf eine Integration von PUFs in Sicherheitsarchitekturen.

Die am Lehrstuhl für Sicherheit in der Informationstechnik vorhandene Expertise in den Bereichen PUFs und Seitenkanalangriffe wurde genutzt um Aspekte der funktionalen Sicherheit von Sensoren als Basis für vertrauenswürdige vernetzte, hoch automatisierte Fahrzeuge, sowie die PUF-Forschung selbst voranzubringen. Die Umsetzung der Forschungsergebnisse in einem Demonstrator lässt die Ergebnisse greif- und analysierbar werden.

In das Projekt sind von Seiten der Technischen Universität München insbesondere Erkenntnisse aus den BMBF-Projekten SIBASE, ARAMiS und ALESSIO eingeflossen. Arbeiten aus diesem Projekten wurden weiterentwickelt, wie etwa die Arbeiten im Bereich der PUFs.

Planung und Ablauf des Vorhabens

Das Verbundprojekt SecForCARs wurde von seinen Partnern ursprünglich auf drei Jahre geplant, es erfolgte eine kostenneutrale Projektverlängerung auf vier Jahre. Die Arbeiten waren dabei auf die sechs Teilprojekte

- AP1: Systemmodell
- AP2: Security und Safety Analysemethodik für CARs
- AP3: Sicherheitsarchitektur und -mechanismen für CARs
- AP4: Demonstratoren
- AP5: Fachlicher Austausch und vorbereitende Arbeiten zur Standardisierung
- AP6: Projektadministration

aufgeteilt. Die Technische Universität München beteiligte sich hierbei an den Teilprojekten

- AP1, welches mit dem gesamten Konsortium bearbeitet wurde,
- AP3, welches gemeinsam vor allem mit der Infineon Technologies AG, ESCRYPT GmbH, Mixed Mode GmbH und Robert Bosch GmbH bearbeitet wurde,
- AP4 und AP5, an welchen ebenfalls das gesamte Konsortium beteiligt war.

Der ursprüngliche zeitliche Ablauf des Projekts mit Beteiligung der Technischen Universität München ist in folgendem Gantt-Chart dargestellt:

			Jahr 1				**Jahr 2**				**Jahr 3**			
AP	**Beschreibung**	**P**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
AP	Systemmodell	**1**												
AP1.1	Use Cases und Bedrohungsszenarien	1												
AP 3	Sicherheitsarchitektur und -	**28**												
AP3.	Sicherheitsarchitektur	1												
AP3.	Sensor-Sicherheit	9												
	TAP3.2.1	2												
	TAP3.2.2	3												
	TAP3.2.3	3												

	TAP3.2.4	1												
AP3.3	Sichere Plattform und Kommunikation	18												
	TAP3.3.1	5												
	TAP3.3.2	5												
	TAP3.3.3	5												
	TAP3.3.4	3												
AP	Demonstratoren	**6**												
AP4.3	Demonstrator Mechanismen	6												
AP 5	Fachlicher Austausch und vorbereitende	**1**												

Wissenschaftlicher und technischer Stand zu Beginn des Vorhabens

Physical Unclonable Functions

Physical Unclonable Functions (PUFs) messen Fertigungsschwankungen, die als eindeutiges Merkmal für ein Objekt angesehen werden können, und erlauben es, aus diesen produktspezifischen und nicht reproduzierbaren Schwankungen ein Geheimnis abzuleiten. Diese Idee wurde erstmals 1983 in [1] aufgebracht und 2001 in der ersten optischen PUF (die unter der Bezeichnung „Physical Oneway Function“ beschrieben wurde) in [2] umgesetzt. Eine deutlich einfachere Integration in moderne elektronische Schaltungen erlauben silizium-basierte PUFs. Ein erstes Konzept dazu wurde 2002 zusammen mit dem Begriff „Physical Unclonable Function“ in [3] eingeführt. Es folgten zahlreiche Entwicklungen von PUF-Strukturen, über die [4] sowie die Arbeit in [5] einen guten Überblick geben.

Im Bereich der Nachbearbeitung von PUF-Daten wurden in den letzten Jahren zahlreiche Verfahren für die Fehlerkorrektur bzw. zur Erzeugung von für die Fehlerkorrektur notwendigen Helper Daten entwickelt (z.B. [6] [7] [8] [9]). Hierbei standen im Fokus der Arbeiten primär die Minimierung des Flächenbedarfs und die Minimierung des für Helper Daten benötigten Speichers. Erst jüngere Arbeiten (z.B. [10]) gehen auch auf das Problem des in PUFs vorhandenen Bias ein. Im Bereich der Quantisierung von analogen PUF Daten wurden bspw. in [11] neue Ideen entwickelt.

Für PUFs ergeben sich zwei primäre Anwendungsszenarien: Einerseits können PUFs, die ein Challenge-Response Verhalten aufweisen, zur Identifikation und Authentifikation eingesetzt werden. Andererseits können PUFs zur sicheren Schlüsselspeicherung herangezogen werden.

Schlüsselspeicher mittels Physical Unclonable Functions

Bezüglich des geplanten Anwendungsszenarios sowie der zu entwickelten Protokolle stellt bspw. die Arbeit in [12] eine Schließberechtigungslösung auf Basis von Smartphones und der NFC-Übertragungstechnik vor. Die Arbeit ermöglicht die flexible Verwaltung, d.h. Zuweisung und Widerruf von Schließberechtigungen für definierte Schlösser. In [13] werden neben anderen Alternativen auch Physical Unclonable Functions (PUFs) zur sicheren Speicherung von Schlüsseln im Car-to-X Szenario präsentiert. In den Arbeiten von [14] [15] wurden inhärente PUF-Instanzen in bereits existierender Standard-Hardware gefunden und für Sicherheitsanwendungen als Hardware-Anker genutzt. Zahlreiche Arbeiten beschäftigen sich

mit PUFs als Krypto-Primitive für Client- sowie Server-Authentifizierung [16] [17] [18] und der Geräte-Identifikation [19]. Weitere PUF-basierte Protokolle sind bspw. in [20] [21] zu finden. Wichtige Arbeiten zum beweisbar sicheren Löschen von Daten auf entfernten Geräten findet man in [22] [23].

Hardware-Angriffe auf Physical Unclonable Functions

Auf Challenge-Response Verfahren für PUFs sowie die dort relevanten Angriffe, welche Methoden des maschinellen Lernens (z.B. [24] [25]) verwenden, wird hier nicht weiter eingegangen, da die Forschung in diesem Projekt nicht auf diese Art von Protokollen fokussiert ist. Auf dem Gebiet der Hardwareangriffe für PUFs wurden in den letzten Jahren einerseits Angriffe vorgestellt, die Photonenemissionen beim Schaltvorgang nutzen um das Geheimnis aus verschiedenen PUF Typen auszulesen und PUFs mit Hilfe von FIBs (Focused Ion Beams) sogar zu klonen (z.B. [26] [27]). Andererseits wurden Angriffe und Gegenmaßnahmen für Angriffe vorgestellt, die versuchen das Geheimnis einer PUF anhand der elektromagnetischen Abstrahlung zu extrahieren (z.B. [28] [29]). Ein Fehlerangriff auf PUFs ist in [30] beschrieben. [31] gibt einen Überblick über relevante Angriffe.

Bekannte Konstruktionen, Verfahren und Schutzrechte

Eine ausführliche Lizenz- und Patentrecherche zu PUFs lag der TUM aus dem BMBF-Projekt SIBASE vor und konnte entsprechend für das Projekt SecForCARs genutzt werden. Auf Basis der vorliegenden Ergebnisse war einerseits nicht zu erwarten, dass die bei der TUM geplanten Arbeiten im Projekt durch anderweitige wissenschaftliche oder technische Ergebnisse gefährdet werden. Andererseits wurden die in SIBASE geförderten Ergebnisse direkt für das Projekt SecForCARs genutzt.

Fachliteratur und benutzte Informations- und Dokumentationsdienste

Ein Auszug der verwendeten Literatur ist diesem Dokument und ebenso den im Rahmen des Projekts entstandenen Veröffentlichungen beigefügt. Dabei wurden überwiegend Datenbanken der Forschungsverlage IEEE Xplore Digital Library, ACM Digital Library, Springer Link verwendet. Zusätzlich wurden diese durch freie Datenbanken, wie Cryptology ePrint Archive oder arXiv ergänzt.

Zusammenarbeit mit anderen Stellen

Im Projekt SecForCARs gab es in über die gesamte Laufzeit eine intensive Zusammenarbeit der Partner. Die Technische Universität München hat hierbei regelmäßig an Telefonkonferenzen sowie Treffen der Partner teilgenommen. Die Ergebnisse wurden bereits während des Projekts in Form eines internen Workshops präsentiert. Diese Zusammenarbeit wurde insbesondere auch durch Treffen innerhalb der Teilprojekte gefördert.

Die Zusammenarbeit der Technischen Universität München war insbesondere mit Mixed Mode GmbH sehr intensiv, um eine PUF als Teil eines sicheren Systems zu implementieren. Daneben wurde auch mit Robert Bosch GmbH und der Infineon Technologies AG eng zusammengearbeitet mit dem Ziel, eine PUF in Radarsensoren zu integrieren. So war es möglich die an der Technischen Universität München entwickelten PUF-Protokolle und Konzepte mit den Anforderungen der Industriepartner abzugleichen und gemeinsam mit den Partnern Publikationen zu veröffentlichen.

Eine weitere Zusammenarbeit mit den Partnern findet bereits statt. So kooperiert, um nur einige Beispiele zu nennen, der Lehrstuhl für Sicherheit in der Informationstechnik der Technische Universität München im Projekt Aquorypt (16KIS1017K) ebenfalls mit der Infineon Technologies AG, der Siemens AG, der Giesecke+Devrient Mobile Security GmbH und dem Fraunhofer Institut für angewandte und integrierte Sicherheit. Im Projekt APRIORI (16KIS1389K) besteht weiterhin eine Kooperation mit der Mixed Mode GmbH, der Siemens AG und dem Fraunhofer Institut für angewandte und integrierte Sicherheit, im Projekt RESEC (16KIS1009) mit der Infineon Technologies AG und im Projekt VE-FIDES (16ME0257) arbeitet der Lehrstuhl unter anderem mit der Siemens AG und der Infineon Technologies AG zusammen.

Eingehende Darstellung

Erzielte Ergebnisse

Die erzielten Ergebnisse lassen sich in zwei wesentliche Bereiche unterteilen: zum einen in die Weiter- sowie Neuentwicklung, Umsetzung und Demonstration von kryptographischen Protokollen in einem automotiven Kontext. Ziel ist hierbei die Absicherung innerhalb des Autos zwischen verschiedenen Komponenten wie zweier Sensoren oder eines Sensors zur ECU, aber auch zwischen mehreren Autos oder Auto zu Infrastruktur. Grundlegender Bestandteil ist eine PUF. Zum anderen in die Analyse zusammen mit neuen Evaluierungsmethoden und Konzepten, die die Sicherheit einer PUF-Anwendung und damit der gesamten Plattform erhöhen.

Sichere Protokolle für Anwendungen im Automotive-Bereich

Bei diesem inhaltlichen Schwerpunkt hat die Technische Universität München verschiedene Ansätze erforscht, um sichere Kommunikation eines Autos umsetzen zu können. Im Rahmen des Projekts ist ein grundlegend neues PUF-Protokoll namens KeLiPUF für einen Schlüsselaustausch entwickelt worden. Dieses erreicht in einer praktischen Umsetzung eine leichtgewichtige Realisierbarkeit, die es dadurch für In-Car Kommunikation relevant macht.

Ähnlich wie bei dem Kerberos-Protokoll [32], ist eine dritte vertrauenswürdige Instanz der Ausgangspunkt, um für zwei Kommunikationspartner einen gemeinsamen Schlüssel einzurichten. Diese Instanz ist beispielsweise ein OEM, der Scheinwerfer mit PUFs im Auto installiert. Der Schlüssel für die sichere Kommunikation ist dabei eng an die jeweilige PUF der beiden Gesprächspartner geknüpft, aus denen in geeigneter Weise der gleiche Schlüssel für die Verwendung von symmetrischer Kryptographie abgeleitet wird. Der Vorteil von PUFs gegenüber der Realisierung eines Schlüsselspeichers in einem nichtflüchtigen Speicher (engl.: Non-Volatile Memory (NVM)) ist dabei, dass eine PUF sowohl sicherer gegen das reine Auslesen eines Schlüssels ist als auch kostengünstiger in System mit beschränkten Ressourcen umgesetzt werden kann.

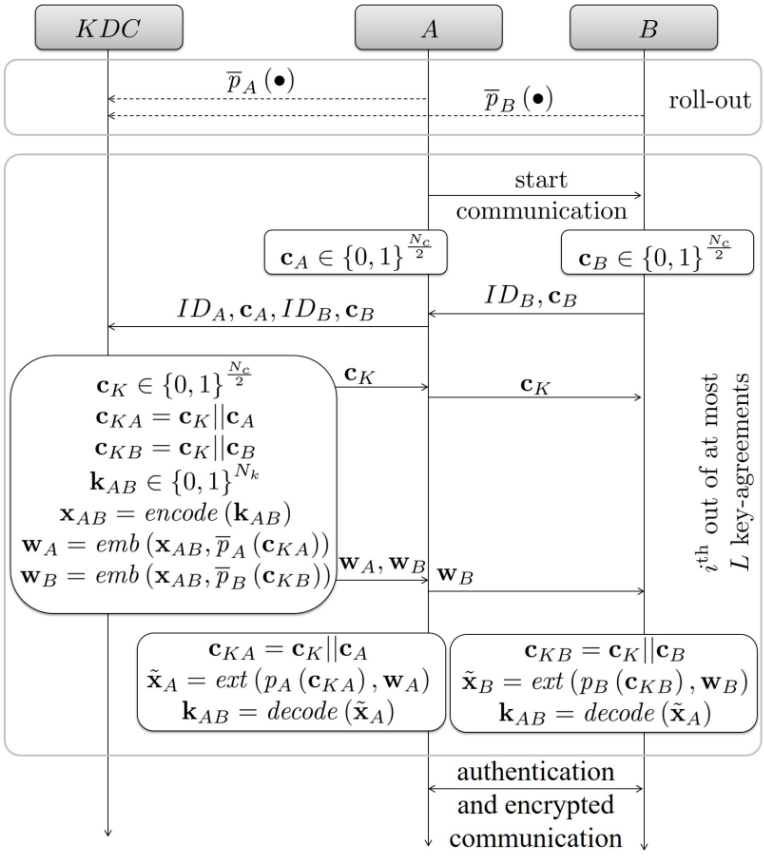


Abbildung 1: Protokollfluss von KeLiPUF

Das in SecForCARs neu entwickelte PUF-Protokoll KeLiPUF funktioniert dabei wie in Abbildung 1 dargestellt: Ziel ist es, dass zwei Instanzen A und B (beispielsweise ein im Auto verbauter Sensor und die ECU) einen gemeinsamen Schlüssel festlegen können, der eine verschlüsselte Kommunikation erlaubt. In der PUF-typischen Roll-Out Phase, erhält das Key Distribution Center (KDC) von A und B ihr jeweiliges PUF-Modell, mit dem es das Challenge-Response Verhalten abbilden kann. Zu einem späteren Zeitpunkt (eben dann, wenn A und B eine verschlüsselte Kommunikation starten wollen), werden von A und B entsprechende Identifizierungs-Marken sowie jeweils eine Hälfte einer zufälligen PUF Challenge an das KDC geschickt. Das KDC seinerseits ergänzt beide Challenge-Hälften mit einer eigenen zufälligen Challenge-Hälfte zu einer vollständigen Challenge. Grund für das Aufteilen einer Challenge in zwei Hälften ist, dass alle drei Parteien an der Challenge-Bildung beteiligt sind. Dadurch wird verhindert, dass ein Angreifer frühere Challenges wiederholen kann. Nachdem die Challenges für A und B vervollständigt wurden, legt das KDC einen zufälligen gemeinsamen Schlüssel für A und B fest. Ausgehend von den jeweiligen modellierten PUF-Antwort von A und B gemäß der entsprechenden Challenge, kann die PUF-Antwort aufgrund der XOR-Struktur mittels der Helferdaten auf den Schlüssel abgebildet werden. Schickt nun seinerseits das KDC die individuellen Helferdaten an A und B, so können sie mit ihrer eigenen PUF-Antwort den gemeinsamen Schlüssel ableiten. Aufbauend auf diesen Schlüssel ist nun die verschlüsselte Kommunikation sicher, bei der durch das KDC sogar A und B gegenüber einander authentifiziert sind.

Neben diesem neuen Konzept runden zwei weitere Untersuchungen KeLiPUF im Rahmen von SecForCARs ab: eine Diskussion und Analyse verschiedener Angriffsvektoren zusammen mit entsprechenden Gegenmaßnahmen erlauben ein tiefergehendes Verständnis für den erzielten Sicherheitsmechanismus. Daneben zeigt eine Umsetzung des Protokolls auf zwei FPGAs, die an einen Computer als KDC angeschlossen sind, dass in der Tat ein leichgewichtiges Protokoll erreicht wurde. Diese Ergebnisse wurden auf der escar Europe 2019 einem breiten Fachpublikum präsentiert [33]. Die escar (Embedded Security in Cars) ist eine führende Konferenz für Automotive Cyber Security.

Eine weitere Untersuchung auf Seiten der Technischen Universität München für sichere Kommunikation für Automotive widmet sich der Umsetzung von Post-Quantum Kryptographie. Da der Einsatz von Quantencomputern in naher Zukunft aktuelle Verschlüsselungsalgorithmen untergräbt, sind neue Verfahren notwendig, die trotz Quantencomputern Sicherheit bieten. Selbige Verfahren sind dementsprechend auch für Automotive gefordert und es muss evaluiert werden, wie sie sinnvoll implementiert werden kann. Es zeigt sich, dass NewHope als ein solches Verfahren geeignet ist und das unter Berücksichtigung strenger Anforderungen bezüglich Performanz, Sicherheitsstandards und limitierter Ressourcen. Als Plattform zur Analyse der Implementierung dient dabei ein AURIX Mikrocontroller, da er insbesondere bei vielen Anwendungen im Automobilbereich herangezogen wird. Verbunden wird die Implementierung mit geeigneten Optimierungsmaßnahmen, die dafür im Rahmen des Projekts entwickelt wurden. Wie KeLiPUF wurden die Ergebnisse auf der escar Europe 2019 präsentiert [34]. Diese Arbeiten auf dem Gebiet der Post-Quanten Sicherheit, die im Projekt SecForCARs als Nebenergebnis zu betrachten sind, bilden unter anderem die Grundlage für weiterführende Forschung im Projekt Aquorypt (16KIS1017K).

Zusätzlich zu den obigen Forschungsergebnissen, konnte in enger Zusammenarbeit mit Infineon Technologies AG ein Schutzmechanismus erarbeitet werden, der Radarsensoren eines Autos absichert. Heutzutage sind Radarsensoren bereits elementarer Bestandteil eines Autos. Die Relevanz steigt noch weiter beim autonomen Fahren, in dem Radarsensoren beispielsweise für Abstandsmessungen die Sicherheit gewährleisten müssen. Dabei wurden im regen Austausch mit Projektpartnern vor allem zwei Gefahren identifiziert, gegen die das neu entworfene Konzept vorgeht. Einerseits handelt es sich bei Radarsensoren und der damit verbundenen Nachverarbeitung von Daten um Produkte, bei denen führende Hersteller mit hochwertiger Qualität hervortreten. Diese hochwertigen Produkte müssen dementsprechend gegen einen unrechtmäßigen Austausch geschützt werden. Ein weiteres Problem ist die Anfälligkeit von Radarsensoren auf analoger Ebene gegen sogenannte Spoofing Angriffe. Bei diesen schickt ein Angreifer speziell gefertigte Signale an einen Radarsensor mit dem Ziel, dass der Radarsensor seine Umgebung nicht richtig wahrnimmt. So ist es einerseits möglich, dass reale Objekte nicht vom Radarsensoren erkannt werden, andererseits können dem Radarsensor Objekte vorgegaukelt werden, die in der Realität nicht vorhanden sind. In beiden Fällen ist dadurch die Sicherheit gefährdet. Der von der Technischen Universität München und der Infineon Technologies AG entwickelte Ansatz basierend auf PUFs ist in der Lage sowohl dem Austausch als auch Spoofing Angriffen entgegen zu wirken.

Da eine PUF als grundlegender Baustein für das Konzept identifiziert worden ist, gilt es, diese in einem Radarsensor zu verankern. Zusammen mit der Robert Bosch GmbH wurde im Projekt SecForCARs erforscht, ob sich aus einem Radarsensor direkt geheime Information ableiten lässt. Dazu wurden von der Robert Bosch GmbH erhobene Daten analysiert und auf ihren nutzbaren Entropiegehalt untersucht. Unter nutzbarer Entropie ist hierbei der durch Fertigungsschwankungen verursachte Zufall abzüglich durch Rauschen verursachte Störeffekte bezeichnet. Eine Randbedingung war hierbei, dass das System des Sensors nicht verändert werden durfte. Diese Arbeiten haben zu dem Ergebnis geführt, dass die Ableitung eines Geheimnisses aus dem Radarsensor selbst unter diesen Randbedingungen nicht zielführend erscheint. Im Gegensatz dazu bietet sich beispielsweise der SRAM eines AURIX Mikrocontrollers als Entropiequelle an, woraus eine SRAM-PUF resultiert. Analysen, die – aufgrund der hohen benötigten Chip-Zahl – auf einem XMC Micro Controller mit dem weiter unten beschriebenen und in SecForCARs entwickelten Spatial Context Tree Weighting Ansatz entwickelt wurden, stützen diese Behauptung. Der für das folgende Protokoll verwendete AURIX ist nicht nur in dem zusammen mit der Infineon Technologies AG betrachteten Radarsensor verbaut, sondern auch darüber hinaus im Automotive Kontext verbreitet. somit zeigt eine Implementierung auf einem AURIX die breite Anwendbarkeit des vorgestellten Schutzmechanismus. Der aus der PUF abgeleitete Schlüssel wird bei dem verwendeten Protokoll zum einen in einem Challenge-Response Protokoll zur Authentifizierung des Radarsensors verwendet. Hierbei schickt die ECU eine zufällige Bitsequenz an den Radarsensor. Dieser verschlüsselt die erhaltene Nachricht und schickt sie an die ECU. Erhält nun die ECU, die ebenfalls im Besitz des geheimen PUF-Schlüssel ist, nach der Entschlüsselung wieder die ursprüngliche Bitsequenz, so handelt es sich um den richtigen Radarsensor mit dem richtigen Schlüssel. Ist dies nicht der Fall, so wurde ein illegitimer Sensor eingebaut und ein derartiger Austausch wird von der ECU erkannt. Zum anderen wird der PUF Schlüssel gegen Spoofing verwendet. Dabei ist die Idee, eine Art Fingerabdruck in ausgehende Signal des Radarsensors einzuprägen. Falls dieser Fingerabdruck nicht mehr im eingehenden Signal enthalten ist, handelt es sich um ein Störsignal und das Signal kann verworfen werden. Die technische Herausforderung und dahingehend zentraler Forschungsgegenstand war, eine geeignete Art zu entwickeln, wie der Fingerabdruck in das Radarsignal eingebracht werden kann. Die Lösung ist eine Phasenmodulation des Signals, die von dem PUF-Geheimnis abhängt. Wichtig ist dann, sobald das eingehende Signal eintrifft, dass in einer Nachbereitung der Fingerabdruck durch geeignete Signalverarbeitung extrahiert wird. Dabei darf jedoch in keiner Weise die normal angedachte Funktionalität des Radarsensors wie die Abstands- oder Geschwindigkeitsbestimmung beeinträchtigt werden. An diesem Gesichtspunkt zeigt sich außerdem deutlich, dass der im Rahmen von SecForCARs vorgeschlagene Ansatz dem Stand der Technik voraus ist. Bisher war das Erkennen von Spoofing Angriffen auf analoger Ebene immer von Nachteilen wie Kosten oder sogar von einer kurzen Unterbrechung der Radarfunktionalität gekennzeichnet. Durch den neuartigen Ansatz können deshalb Verbesserungen in Bezug auf die Sicherheit in diesem Fall von Radarsensoren erzielt werden. Aktuell ist das Konzept bei der escar Europe 2022 eingereicht [35]. Außerdem erscheint ein Video zu dem Demonstrator auf dem für SecForCARs angelegten Youtube-Kanal verbunden mit anderen Social Media Plattformen. Es ist anzumerken, dass zur Nutzbarmachung des SRAM eines AURIX für PUF-Anwendungen ein tiefes Verständnis des Controllers erforderlich

ist und verschiedene Implementierungstricks notwendig sind. Die Mixed Mode GmbH trug neben der Infineon Technologies AG dazu bei, entsprechende Schwierigkeiten aus dem Weg zu räumen.

Neben der genannten Implementierung eines SRAM basierten Ansatzes auf einem AURIX, wurden im Rahmen des Projektes auch weitere bekannte Protokolle auf SRAM Basis mit einem XMC implementiert und untersucht. Diese Untersuchungen erfolgten primär im Rahmen verschiedener Arbeiten. Das im Rahmen dieser Arbeiten entstandene PUF-System bildet die Grundlage für weitere Forschung und wurde unter anderem auch dem Fraunhofer Institut für angewandte und integrierte Sicherheit zur Verfügung gestellt, wo es eine wesentliche Komponente des in [43] veröffentlichten Ansatzes bildet.

Untersuchung von Schutzmechanismen

Eine PUF ist zentraler Baustein für die oben genannten Ansätze der kryptographischen Protokolle. Um bei einer Anwendung in einem größeren Rahmen die Sicherheit zu gewährleisten, ist es deswegen von zentraler Bedeutung, die Sicherheit und damit verbunden die Qualität einer PUF zu evaluieren. Diese Untersuchungen bilden neben den Protokollen einen zweiten Schwerpunkt der Technischen Universität München in SecForCARs.

Eine Möglichkeit, PUFs zu kategorisieren, ist die Anzahl an möglichen Konfigurationen, im Folgenden als Challenges bezeichnet, die angelegt werden können. Die daraus resultierende Gruppierung unterscheidet PUFs mit nur einer möglichen Challenge wie einer SRAM-PUF und PUFs, die viele Challenges zulassen. PUFs, die viele Challenges zulassen, sind dabei insbesondere Modellierungsangriffen mittels Machine-Learning ausgesetzt, die ausnutzen, dass reale PUFs – anders als ideale PUFs – Korrelationen bei Responses auf verschiedene Challenges aufweisen. Diese Zusammenhänge können mittels Machine Learning aufgegriffen werden, wenn viele Paare an Challenges und zugehörigen Responses bekannt sind. Gemäß dem Stand der Technik wurde bisher davon ausgegangen, dass in den öffentlichen Helferdaten solche Zusammenhänge nicht erkennbar sind. Forschungsergebnisse beim SecForCARs-Projekt haben jedoch gezeigt, dass die Helferdaten durchaus eine Vulnerabilität darstellen können.

Um Fehler einer PUF-Response bedingt durch Rauschen korrigieren zu können, werden fehlerkorrigierende Codes verwendet. Die intrinsische Struktur dieser Codes spiegelt sich dann in den Helferdaten wider, sodass entlang dieser Codestruktur Bits einer PUF Response in einen Zusammenhang gestellt werden können. Genau diese Zusammenhänge können in ein Siamesisches Neuronales Netz eingespeist werden, um letztendlich nur aus öffentlich bekannten Daten eine PUF modellieren zu können. Dieses Modell bricht die PUF, da ein Angreifer nun die Responses bestimmen kann und somit das daraus abgeleitete Geheimnis kennt. Die Bedeutung dieses Angriffs liegt in seiner neuen Vorgehensweise, die eine bisher nicht untersuchte Schwachstelle von PUFs, die viele Challenges erlauben, aufdeckt. Davon betroffen ist beispielsweise das im Rahmen von SecForCARs vorgestellte Protokoll KeLiPUF. Gleichzeitig mit dem Angriff ist jedoch auch untersucht worden, wie in einem sicheren System mit derartigen Schwachpunkten umgegangen werden kann: ein geradliniger Ansatz ist es hierbei, die Anzahl an Challenge-Response-Paaren zu beschränken, sodass die Datenmenge nicht ausreicht, um mittels Machine Learning die PUF abzubilden. Ein weiterer Ansatz ist es

durch geeignete Wahl der Fehlerkorrekturcodes die Komplexität der zugrundeliegenden Struktur so weit zu erhöhen, dass eine Modellierung praktisch unverhältnismäßig aufwendig wird. Die erzielten Erkenntnisse sind im Rahmen der CHES 2021 veröffentlicht [36]. Für das im Projekt SecForCARs entwickelte Protokoll KeLiPUF ist die Konsequenz aus der Existenz dieses Angriffs, dass die maximale Anzahl möglicher Challenge-Response Paare – und damit die Anzahl der ausgehandelten Schlüssel – beschränkt werden muss. Die genaue Anzahl möglicher Schlüsse hängt von der Güte der PUF und dem verwendeten Code ab und kann bei der Verwendung aktueller PUF Primitive und Fehlerkorrekturansätze mit bis zu einigen 100 erwartet werden.

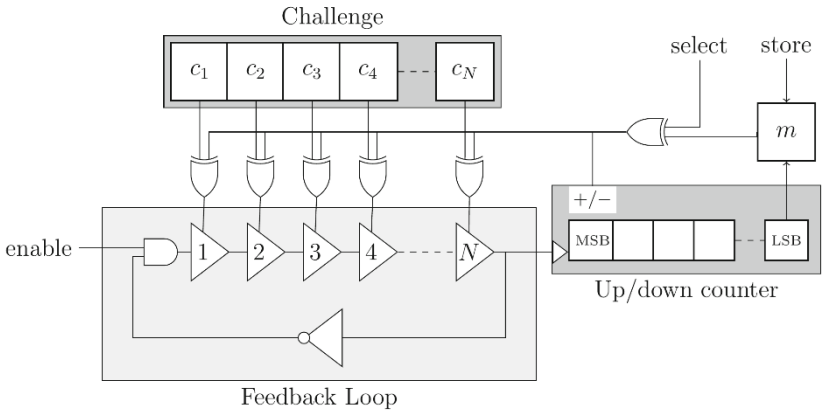
Die Qualität der in einem System verwendeten PUF spiegelt sich insbesondere in der nutzbaren Entropie wieder, die gleichsam ein Maß für die Zufälligkeit einer rauschfreien PUF-Response ist. Eine ideale PUF weist keinerlei Bias- oder Korrelationseffekte und auch keine Abhängigkeiten höherer Ordnung auf und hat somit volle Entropie. In der Praxis, ist dies nicht der Fall. Daher sind Verfahren nötig, um die Entropie aufbauend auf echten Daten zu bestimmen. Da die zugrundeliegenden Wahrscheinlichkeitsverteilungen nicht bekannt sind, ist es nicht möglich, die Entropie direkt zu berechnen. Ein gängiges Vorgehen des Stands der Technik ist es dementsprechend, die PUF-Response zu komprimieren, beispielsweise mit dem Verfahren des „Context Tree Weighting“. Hierbei wird eine zufällige Sequenz (also eine PUF-Response) untersucht. Nachteil dieses Verfahrens ist jedoch im PUF-Kontext, dass PUF-Daten nicht einer eindimensionalen Sequenz entsprechen, sondern vielmehr einer zwei-dimensionalen Struktur. Das Ergebnis bisherige Verfahren, die diese Struktur nicht berücksichtigen hängt in der Konsequenz davon ab, wie die Daten bei der Kompression angeordnet werden und überschätzen in der Folge die Entropie der PUF, spiegeln also eine zu hohe Qualität vor. Als Ergebnis von Forschungsarbeit im Rahmen des SecForCARs Projektes hat die Technische Universität München dahingehend das bisherige Verfahren des Context Tree Weighting zu einem Spatial Context Tree Weighting erweitert, sodass es die räumliche Zweidimensionalität von PUF Daten abbildet. Diese neue Dimension erlaubt es, Zusammenhänge und Einflüsse von PUF Responses, die zu räumlich nah beieinanderliegenden PUF-Instanzen auf einem eingebetteten Gerät gehören, näher umzusetzen und somit genauere Abschätzungen der Entropie zu erzielen. Diese Forschung erfolgte in Kooperation mit dem Fraunhofer Institut für angewandte und integrierte Sicherheit und diente im Projekt SecForCARs insbesondere dazu, die Nutzbarkeit des SRAM von Micro Controllern als SRAM PUFs weiter zu analysieren. Die Arbeit ist in [37] veröffentlicht.

Eine weitere Art von Angriff ist Microprobing. Dabei kontaktiert ein Angreifer mittels einer Nadel-Probe eine Leitungen auf einem Chip und versucht auf diese Weise, sensible Daten zu erfahren. Von solchen Angriffen sind insbesondere Busleitungen betroffen, wenn diese sicherheitskritische Information transportieren. Da ein solcher Angriff eine Bedrohung für sichere Plattformen darstellt, ist im Rahmen von SecForCARs ein Verfahren erforscht worden, das derartige Angriffe erkennen kann und im Vergleich zum bisherigen Stand der Technik einige Vorteile aufweist: so ist der Mehraufwand für eine Kalibrierung reduziert und längere Busleitungen können abgesichert werden. Als Grundidee zur Erkennung werden Ringoszillatoren an die Busleitung angeschlossen. Kontaktiert ein Angreifer mit einer Messsonde eine Busleitung, so ändert sich die Leitungskapazität und in Folge davon die

Frequenz, mit der der entsprechende Ringoszillator schwingt. Diese Schwankung wird detektiert, wodurch Microprobing entgegengewirkt werden kann. Im Rahmen einer mit der Infineon Technologies AG entstandenen Forschung wurde dieses Konzept ausgearbeitet und mit Hilfe von Simulationen analysiert. Für das Projekt SecForCARs ist diese Arbeit insbesondere relevant, da es bei sehr sicheren Chips nicht ausreicht, das Geheimnis selbst z.B. mit einer PUF geschützt zu speichern; auch der Informationsfluss auf dem Chip muss gegen sehr starke Angreifer, die die Sicherheit auch invasiven Angriffen korrumpieren wollen, geschützt werden. Die Ergebnisse sind der Forschungsgemeinschaft im Rahmen einer Publikation zur Verfügung gestellt [38]. Im Forschungsprojekt VE-FIDES (16ME0257) wurde die in SecForCARs entwickelte Idee aufgegriffen und weiter untersucht.

Wichtiger als die Schaltung gegen invasive Eingriffe zu schützen ist es, die PUF gegen nicht-invasive Eingriffe zu härten. Auch eine PUF, die maximale (nutzbare) Entropie liefert ist wertlos, wenn die geheime Information mit einfachen Mitteln ausgelesen werden kann. Die Technische Universität München hat deshalb in SecForCARs den Schutz von PUF-Primitiven gegen Seitenkanalangriffe untersucht, um so die Güte der PUF auch in dieser Hinsicht bewerten zu können. Außerdem wurden Gegenmaßnahmen gegen solche Angriffe entwickelt. Bei Seitenkanalangriffen zieht ein Angreifer aus Messungen, im vorliegenden Fall der Leistungsaufnahme einer Schaltung, Rückschlüsse über verarbeitete geheime Daten. Im Rahmen des SecForCARs-Projekts wurde dabei die Loop PUF [39] untersucht und verbessert. Dieses PUF-Primitiv besteht aus einer Reihe von Verzögerungsgliedern, die durch Rückkopplung einen Oszillator bilden. In jedem Verzögerungsglied kann über ein Challenge-Bit einer von zwei Pfaden ausgewählt werden; die Gesamtverzögerung bzw. –frequenz des Loop PUF-Oszillators ist damit abhängig von der gewählten Challenge. Aus dem Vorzeichen der Differenz zweier Frequenzen wird jeweils ein PUF-Response Bit abgeleitet. Die Technische Universität München konnte zeigen, dass diese Konstruktion von einem Angreifer mit Zugriff auf das Frequenzspektrum ausgenutzt werden kann, um die geheime PUF Response auszulesen. Problematisch ist dabei vor allem, dass die Challenges sequentiell ausgewertet werden, d.h. die Seitenkanalinformation zeitlich trennbar ist.

Abbildung 2: Schema der selbst-geschützten Loop PUF mit „zeitliche Maskierung“-Gegenmaßnahme.



Zur Absicherung gegen den Angriff wurde das neuartige Schutzverfahren zur „zeitlichen Maskierung“ (engl.: „Temporal Masking“) entwickelt, das auf der COSADE 2020 vorgestellt wurde [40] und in Abbildung 2 dargestellt ist: Das Rauschen des Frequenzzählers wird

verwendet um die Reihenfolge der verwendeten Challenges zu randomisieren. Ein Angreifer kann zwar weiterhin den Seitenkanal beobachten, aufgrund der ihm unbekannten Reihenfolge der Challenges ist es aber nicht mehr möglich auf das Vorzeichen der Differenz (und damit das geheime PUF Response Bit) zu schließen. Ein besonderer Vorteil dieser Methode ist dabei der geringe Mehraufwand: der benötigte Zufall wird aus der PUF selbst generiert statt — wie bei anderen Gegenmaßnahmen üblich — auf einen zusätzlichen Zufallszahlengenerator zuzugreifen. Damit ist diese Gegenmaßnahme besonders kostengünstig und die Loop PUF schützt sich selbst.

Weiterhin wurde das sogenannte „Two-Metric Helper Data“-Verfahren (TMHD) [41] in Kombination mit der Loop PUF und der „zeitliche Maskierung“-Gegenmaßnahme auf Seitenkanalschwächen untersucht. Das TMHD erlaubt die Zuverlässigkeit der abgeleiteten PUF Bits zu erhöhen und damit Ressourcen wie Fehlerkorrektur einzusparen. Dazu werden die PUF Response Bits nicht aus dem Vorzeichen einer Frequenzdifferenz abgeleitet, sondern der Betrag der Freqenzdifferenz wird einbezogen: in einem sogenannten „Enrollment“-Schritt werden Helferdaten (engl.: Helper Data) über den Betrag und das Vorzeichen der Differenz gespeichert. Dabei werden zwei Zonen bzw. Metriken (engl.: Two-Metric) unterschieden. Die Helferdaten werden auf dem Gerät gespeichert und lassen keinen Rückschluss auf die PUF Response zu. Bei Schlüsselableitung werden die Helferdaten dann mit dem Betrag und Vorzeichen rekombiniert und eine rauscharme PUF-Response kann abgeleitet werden. Die Technische Universität München konnte anhand von Messungen und theoretischen Betrachtungen nachweisen, dass die Helferdaten in Kombination mit Seitenkanalbeobachtungen erlauben, die Entropie der PUF Response stark zu reduzieren. Auch die „zeitliche Maskierung“-Gegenmaßnahme verhindert diese Angriffe nicht, da sie nur das Vorzeichen schützt. Um Seitenkanalangriffe zu unterbinden, wurden zwei Gegenmaßnahmen entwickelt, die die Sequenz aller Challenges (anstelle der Reihenfolge zweier Challenges) randomisieren.

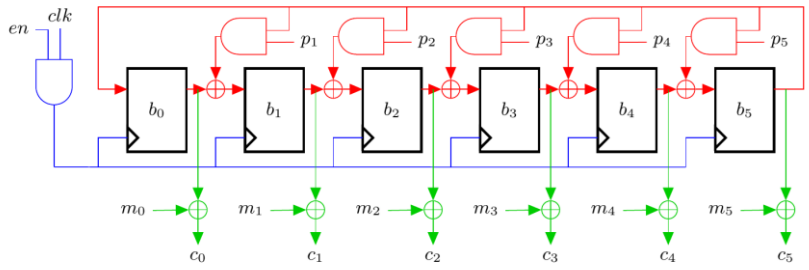
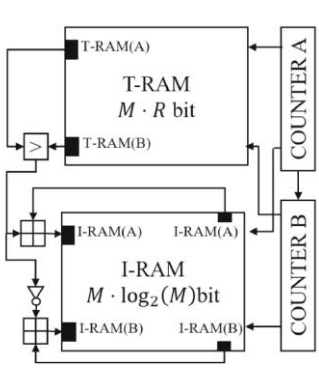


Abbildung 3: Kombinierte Gegenmaßnahmen mit geringer Komplexität zum Schutz des "Two-Metric Helper Data"-Verfahrenes.

Die Kombination verschiedener leichtgewichtiger Gegenmaßnahmen wie LFSR-basierte Pseudo-Randomisierung, Maskierung und Shifting in Abbildung 3 erzeugt einen geringen Mehraufwand, die generierte Sequenz der Challenges lässt sich mit einer geeigneten Rate-Strategie aber anhand mehrmaliger Seitenkanalbeobachtung ermitteln. Interessanterweise führt die Kombination verschiedener Methoden sogar zu einer Reduktion des Schutzniveaus. Dieses Ergebnis könnte auch für den Entwurf von Gegenmaßnahmen in anderen Bereichen einbezogen werden.



Algorithm 1: Permutation Generator

Choose M R-bit distinct random numbers r_i
Store r_i to `T-RAM`.
for `A` in 0 to $M-1$ **do**
  for `B` in `A`+1 to M **do**
    if `T-RAM(A)` > `T-RAM(B)` **then**
      increment `I-RAM(A)`
    else
      increment `I-RAM(B)`
    end if
  end for
end for
return Sequence in `I-RAM`.

Abbildung 4: Blockdigramm des Permutationsgenerators zum Schutz des "Two-Metric Helper Data"-Verfahrens.

Als Alternative mit einem dedizierten Zufallszahlengenerator wurde der in Abbildung 4 abgebildete Permutationsgenerator vorgestellt. Die zufällig gezogenen Zufallszahlen werden von dem Permutationsgenerator geordnet und die Indizes kodieren die Challenge-Sequenz. Durch die Verwendung echter Zufallszahlen gibt es keine Rate-Strategie aus mehrmaligen Seitekanalbeobachtungen und die Gegenmaßnahme bietet einen kompletten Schutz. Als Nachteil besteht neben dem erhöhten Aufwand zur Zufallszahlengenerierung die nicht-deterministische Laufzeit für mehrfach gezogenen Zufallszahlen. Die Analyse und Gegenmaßnahmen mit Vor- und Nachteilen wurden der wissenschaftlichen Gemeinschaft auf der COSADE 2021 vorgestellt [42]. Es ist zu erwähnen, dass die in SecForCARs entstandenen Arbeiten in diesem Bereich die Grundlage für das Projekt APRIORI (16KIS1389K) darstellen, in dem diese Forschung derzeit weiter vorangetrieben wird, und auch im Projekt VE-FIDES (16ME0257) Berücksichtigung finden.

Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse entsprechend des Verwertungsplans

Die Ergebnisse fließen in den Lehrbetrieb an der Technischen Universität München ein. Insbesondere werden Ergebnisse aus dem Bereich PUFs in der Lehrveranstaltung „Physical Unclonable Functions“ verwendet. Außerdem werden die Ergebnisse aus dem Projekt in der Ringvorlesung „Systemsicherheit“ berücksichtigt. Die Ergebnisse dienen weiter als Basis für weitere Forschungskooperationen. So wurden die Ergebnisse bezüglich Post-Quantenverfahren insbesondere im Projekt Aquorypt (16KIS1017K) weiterverwendet. Forschung bezüglich der Protokolle und Radarsensoren findet insbesondere im vom Bayerischen StMWi geförderten Projekt 6G Future Lab Bavaria Berücksichtigung und wird dort verwendet und weiter vorangetrieben, wobei Erkenntnisse bezüglich der Protokolle auch für das Projekt VE-FIDES (16ME0257) eine wesentliche Rolle spielen. Die Forschung bezüglich der Bewertung von PUFs wird im Rahmen eines Forschungsauftrags des Fraunhofer Instituts für Angewandte und Integrierte Sicherheit weiter fortgeführt und findet dort Berücksichtigung. Ergebnisse zur Konstruktion von PUFs sowie von Angriffen bilden die Grundlage für zahlreiche verschiedene Arbeiten in den Projekten VE-FIDES und APRIORI (16KIS1389K). Weitere Projekte, die die Forschungsergebnisse berücksichtigen, sind in der Anbahnung. Die in SecForCARs durchgeführte Forschung wurde außerdem in bereits in 7 Publikationen der Fachöffentlichkeit vorgestellt, eine achte Publikation ist zur Begutachtung eingereicht. Diese

Veröffentlichungen untermauern das Interesse der Öffentlichkeit an dem Projekt und zeigen somit dessen Nutzen. Insgesamt lässt sich also feststellen, dass die Mitarbeit am Projekt SecForCARs nicht nur für den Lehrstuhl für Sicherheit in der Informationstechnik einen deutlichen Mehrwert darstellt, sondern darüber hinaus auch klar zum Fortschritt des Standes der Wissenschaft und Technik beigetragen hat.

Während des Vorhabens bekanntgewordene Fortschritte auf dem Gebiet des Vorhabens bei anderer Stelle

Es sind keine Fortschritte auf dem Gebiet des Vorhabens bekannt geworden, die das Projekt gefährdet haben.

Erfolgte Veröffentlichungen der Ergebnisse

- Michael Pehl, Christoph Frisch, Peter Christian Feist, Georg Sigl: „KeLiPUF: a key-distribution protocol for lightweight devices using Physical Unclonable Functions". 17thescar Europe: embedded security in cars, 2019, DOI: https://doi.org/10.13154/294-6676

- Tim Fritzmann and Jonas Vith and Johanna Sepulveda: "Post-quantum key exchange mechanism for safety critical systems". 17thescar Europe: embedded security in cars, 2019. DOI: https://doi.org/10.13154/294-6653

- Seyed Hamidreza Moghadas and Michael Pehl. "ROPAD: a fully digital highly predictive ring oscillator probing attempt detector." 2020 57th ACM/IEEE Design Automation Conference (DAC). IEEE, 2020.

- Emanuele Strieder, Christoph Frisch, and Michael Pehl. "Machine Learning of Physical Unclonable Functions using Helper Data: Revealing a Pitfall in the Fuzzy Commitment Scheme". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(2). 10.46586/tches.v2021.i2.1-36

- Michael Pehl, Tobias Tretschok, Daniel Becker, and Vincent Immler "Spatial Context Tree Weighting for Physical Unclonable Functions." 2020 European Conference on Circuit Theory and Design (ECCTD). IEEE, 2020.

- Lars Tebelmann, Jean-Luc Danger, and Michael Pehl. "Self-Secured PUF: Protecting the Loop PUF by Masking." Constructive Side-Channel Analysis and Secure Design, Springer International, 2020. https://doi.org/10.1007/978-3-030-68773-1_14

- Lars Tebelmann, Ulrich Kühne, Jean-Luc Danger, and Michael Pehl. „Analysis and Protection of the Two-Metric Helper Data Scheme". Constructive Side-Channel Analysis and Secure Design, 2021. https://doi.org/10.1007/978-3-030-89915-8_13

Geplante Veröffentlichungen der Ergebnisse

- Christoph Frisch, Sanchita Vishwa, Bernhard Greslehner-Nimmervoll, Jochen Koszescha, and Michael Pehl „Chirping PUFs: Protection of Radar Sensors against Spoofing through Physical Unclonable Functions", escar Europe 2022.

Literaturverzeichnis

[1] D. W. Bauder, „An Anti-Counterfeiting Concept for Currency Systems," Sandia National Labs, Albuquerque, 1983.

[2] R. Pappu, „Physical One-Way Functions," Massachusetts Institute of Technology, Cambridge, Massachussets, 2001.

[3] B. Gassend, D. Clark, M. van Dijk und S. Devadas, „Silicon Physical Random Functions," in *ACM Conference on Computer and Communications Security (CCS)*, 2002.

[4] C. Böhm und M. Hofer, Physical Unclonable Functions in Theory and Practice, Springer, 2013.

[5] R. Maes und I. Verbauwhede, „Physically Unclonable Functions: A Study on the State of the Art and Future Directions," in *Towards Hardware-intrinsic Security*, Springer, 2010, pp. 3-37.

[6] Y. Dodis, R. Ostrovsky, L. Reyzin und A. Smith, „Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," in *Advances in Cryptology - EUROCRYPT*, 2004.

[7] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi und P. Tuyls, „Efficient Helper Data Key Extractor on FPGAs," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2008.

[8] R. Maes, P. Tuyls und I. Verbauwhede, „A soft decision helper data algorithm for SRAM PUFs," *IEEE International Symposium on Information Theory (ISIT),* pp. 2101-2105, June 2009.

[9] R. Maes, P. Tuyls und I. Verbauwhede, „Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs," *Workshop on Cryptographic Hardware and Embedded Systems (CHES),* pp. 332-347, September 2009.

[10] R. Maes, V. van der Leest, E. van der Sluis und F. Willems, „Secure Key Generation from Biased PUFs," *CHES,* 2015.

[11] O. Günlü und O. Iscan, „DCT Based Ring Oscillator Physical unclonable Functions," *ICASSP,* 2014.

[12] A. Dmitrienko, A.-R. Sadeghi, S. Tamrakar und C. Wachsmann, „SmartTokens: Delegable Access Control with NFC-Enabled Smartphones," *TRUST,* 2012.

[13] M. Feiri, J. Petit und F. Kargle, „Efficient and Secure Storage of Private Keys for Pseudonymous Vehicular Communication," *CyCAR,* 2013.

[14] A. Schaller, T. Arul, V. van der Leest und S. Katzenbeisser, „Lightweight Anti-counterfeiting Solution for Low-End Commodity Hardware Using Inherent PUFs," *Trust and Trustworthy Computing,* 2014.

[15] F. Kohnhäuser, A. Schaller und S. Katzenbeisser, „PUF-Based Software Protection for Low-End Embedded Devices," *Trust and Trustworthy Computing,* 2015.

[16] P. Tuyls und L. Batina, „RFID-Tags for Anti-Counterfeiting," *CT-RSA,* 2006.

[17] P. Tuyls, G. Schrijen, F. Willems, T. Ignatenko und B. Skoric, „Secure Key Storage with PUFs," in *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer, 2007.

[18] P. Tuyls und B. Skoric, „Strong Authentication with Physical Unclonable Functions," in *Security, Privacy, and Trust in Modern Data Management*, Springer, 2007.

[19] A. Maiti, R. Nagesh, A. Reddy und P. Schaumont, „Physical Unclonable Functions and True Random Number Generators: a Compact and Scalable Implementation," in *GLSVLSI*, 2009.

[20] S. Kleber, R. van der Heijden, H. Kopp und F. Kargl, „Terrorist Fraud Resistance of Distance Bounding Protocols Employing Physical Unclonable Functions," in *NetSys*, 2015.

[21] J. Petit, C. Bosch, M. Feiri und F. Kargl, „On the Potential of PUF for Pseudonym Generation in Vehicular Networks," in *VNC*, 2012.

[22] D. Perito und G. Tsudik, „Secure Code Update for Embedded Devices via Proofs of Secure Erausure," in *Computer Security - ESORICS*, Springer, 2010.

[23] G. Karame und W. Li, „Secure Erasure and Code Update in Legacy Systems," in *Trust and Trustworthy Computing*.

[24] U. Rührmair, J. Solter, F. Sehnke, X. Xu, V. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson und S. Devadas, „PUF Moderling Attacks on Simulated and Silicon Data," *IEEE Transactions on Information Forensics and Security,* pp. 1876-1891, November 2013.

[25] F. Ganji, S. Tajik und S. J.-P., „Why Attackers Win: On the Learnability of XOR Arbiter PUFs," in *Trust and Trustworthy Computing*, 2015.

[26] C. Helfmeier, C. Boit, D. Nedospasov und S. J.-P., „Cloning Physical Unclonable Functions," *IEEE International Symposium on Hardware-Oriented Security and Trust,* pp. 1-6, June 2013.

[27] S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, C. Helfmeier, J.-P. Seifert, C. Boit und H. H.-W., „A Complete and Linear Physical Characterization Methodology for Arbiter PUF Family," *Cryptology ePrint Archive,* 2015.

[28] D. Merli, D. Schuster, F. Stumpf und G. Sigl, „Semi-invasive EM attack on FPGA RO PUFs and countermeasues," *Proceedings of the Workshop on Embedded Systems Security (WES),* pp. 2:1-2:9, Oktober 2011.

[29] D. Merli, F. Stumpf und G. Sigl, „Protecting PUF Error Correction by Codeword Masking," *Cryptology ePrint Archive,* 2013.

[30] S. Tajik, H. Lohrke, F. Ganji, J.-P. Seifert und C. Boit, „Fault Attacks on Physically Unclonable Functions," in *FDTC*, 2015.

[31] C. Helfmeier, D. Nedospasov, S. Tajik, C. Boit und J.-P. Seifert, „Physical Vulnerabilities of Physically Unclonable Functions".

[32] J. Kohl und C. Neumann, „The Kerberos Network Authentication Service (V5)," in *RFC 1510*, 1995.

[33] M. Pehl, C. Frisch, C. P. Feistel und G. Sigl, „KeLiPUF: A Key-distribution Protocol for Lightweight Devices Using Physical Unclonable Funtions," in *escar Europe*, 2019.

[34] T. Fritzmann, J. Vith und J. Sepulveda, „Post-quantum key exchange mechanism for safety critical systems," in *escar Europe*, 2019.

[35] C. Frisch, S. Vishwa, B. Greslehner-Nimmervoll, J. Koszescha und M. Pehl, „Chirping PUFs: Protection of Radar Sensors against Spoofing through Physical Unclonable Functions," in *eingereicht für escar Europe*, 2022.

[36] E. Strieder, C. Frisch und M. Pehl, „Machine Learning of Physical Unclonable Funtions Using Helper Data: Revealing a Pitfall in the Fuzzy Commitment Scheme," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2021.

[37] M. Pehl, T. Tretschok, D. Becker und V. Immler, „Spatial Context Tree Weighting for Physical Unclonable Functions," in *European Conference on Cicuit Theory and Design (ECCTD)*, 2020.

[38] S. Moghadas und M. Pehl, „ROPAD: A Fully Digital Highly Predictive Ring Oscillator Probing Attempt Detector,“ in *Design Automation Conference (DAC)*, 2020.

[39] Z. Cherif, J. Danger, S. Guilley und L. Bossuet, „An Easy-to-Design PUF Based on a Single Oscillator: The Loop PUF,“ in *Euromicro Conference on Digital System Design*, 2012.

[40] L. Tebelmann, J. Danger und M. Pehl, „Self-Secured PUF: Protecting the Loop PUF by Masking,“ in *Constructive Side-Channel Analysis and Secure Design*, 2020.

[41] J. Danger, S. Guilley und A. Schaub, „Two-Metric Helper Data for Highly Robust and Secure Delay PUFs,“ in *International Workshop on Advances in Sensors and Interfaces (IWASI)*, 2019.

[42] L. Tebelmann, U. Kühne, J. Danger und M. Pehl, „Analysis and Protection of the Two-Metric Helper Data Scheme,“ in *Constructive Side-Channel Analysis and Secure Design*, 2021.

[43] A. Miguel Garcia und M. Hiller, „Lightweight Authentication and Encryption for Online Monitoring in IIoT Environments”, in *Foundations and Practice of Security*, 2022.