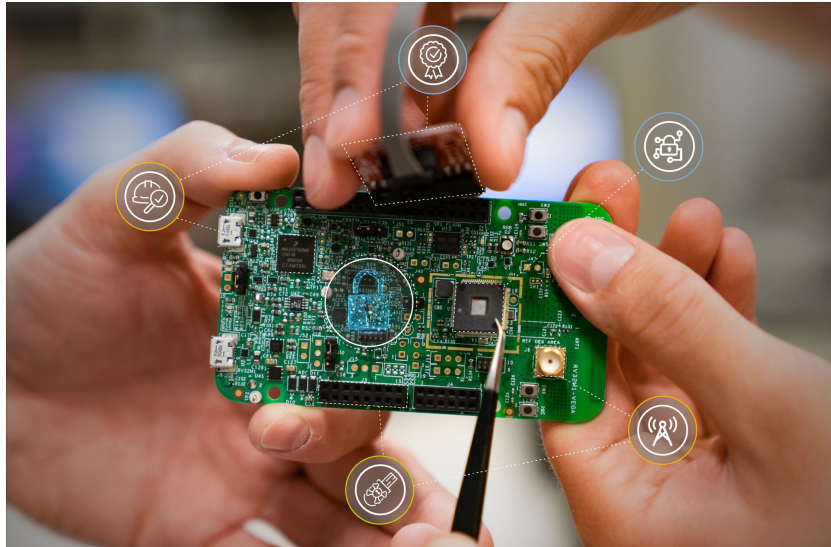


VE-Jupiter

Eindeutige Identifizierbarkeit für vertrauenswürdige Mikroelektronik mit Chiplets

Sachbericht von NXP



NXP Semiconductors Germany GmbH (Projektkoordination)

Beiersdorfstraße 12, 22529 Hamburg

Dr.-Ing. Marc Gourjon

marc.gourjon@nxp.com, Tel.: +49 (0) 1514 1400665

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 16ME0231K gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Förderkennzeichen: 16ME0231K
Laufzeit: 01.03.2021 - 31.08.2024
Datum: 16.10.2024

Vorwort

Dieser Bericht beschreibt die erzielten Ergebnisse des BMBF-Verbundprojektes “VE-Jupiter” beim Projektpartner NXP Semiconductors Germany GmbH (NXP).

Konsortium

Das Projekt wurde in Zusammenarbeit der folgenden Projektpartner durchgeführt:

- NXP Semiconductors Germany GmbH (Konsortialführer)
- Aerospace Data Security GmbH (ASDS), vormals DSI Datensicherheit GmbH
- Technische Universität Darmstadt – Fachgebiet Eingebettete Systeme und ihre Anwendungen (ESA)
- Universität zu Lübeck – Institut für Technische Information (ITI)
- Universität zu Lübeck – Institut für IT-Sicherheit (ITS)

Inhaltsverzeichnis

1	Ausführlicher Sachbericht	4
1.1	Verwendung der Zuwendung	4
1.1.1	Arbeitspaket AP1 : Ebenenübergreifende Maßnahmen	4
1.1.2	Arbeitspaket AP2 : Security Atoms	5
1.1.3	Arbeitspaket AP3 : Entwurf und Entwicklung von iTrustlets	5
1.1.4	Arbeitspaket AP4 : A&U-Sicherung im Lebenszyklus	7
1.1.5	Arbeitspaket AP5 : A&U-Prüfung Analog	9
1.1.6	Arbeitspaket AP6 : “Secure-by-Design”-EDA-Werkzeuge	9
1.1.7	Arbeitspaket AP7 : Demonstrator & Evaluation	12
1.2	Wichtigste Positionen des zahlenmäßigen Nachweises	13
1.3	Notwendigkeit und Angemessenheit der geleisteten Arbeit	14
1.4	Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse bzw. Erfahrungen	15
1.5	Während der Durchführung des Vorhabens bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen	16
1.6	Erfolgte und geplante Veröffentlichungen der Ergebnisse	17

1 Ausführlicher Sachbericht

Die im Rahmen des Teilvorhabens von NXP in VE-Jupiter durchgeführten Arbeiten werden im Folgenden detaillierter dargestellt.

1.1 Verwendung der Zuwendung

NXP leistet Beiträge zu mehreren Komponenten von VE-Jupiter, beginnend mit der Sicherheitsdefinition, die sowohl praxisnahen Angriffen als auch den industriellen Sicherheitsschemata entspricht (**AP1**). Schwerpunkte der technischen Beiträge sind zum einen die verteilte und interoperable Prüfung von Authentizität und Unversehrtheit (A&U) mit iTrustlet-ausgestattetem Intellectual Property (IP) auf Ebene des Gesamtsystems (**AP4**) sowie die entsprechende Entwicklung der iTrustlet-Technologie, die die dafür notwendigen Voraussetzungen erfüllt (**AP3**).

Zum anderen ermöglicht die verlässliche Absicherung von IP und iTrustlet-Hardware (HW) mittels automatisierter Verifikation (**AP6**) die Prüfung flexibler Sicherheitslevel, sodass die Entwicklungsprozesse agiler gestaltet werden können. Die Schwerpunkte von NXP erleichtern die zukünftige Integration der VE-Jupiter-Ergebnisse in komplexe system on a chips (SoCs) in sicherer Form, sodass trotz möglicher Angriffe während des Lebenszyklus die vertrauenswürdige Prüfbarkeit von A&U gewährleistet bleibt. In Kombination mit den Ergebnissen der Projektpartner wird eine umfassende Resistenz gegen hochgradige Angriffe (**AP2**) und eine erweiterte Prüfbarkeit vertrauenswürdiger Elektronik ermöglicht (**AP5**). Abschließend wird die Praxisrelevanz in der industriellen Produktentwicklung und -fertigung sowie in den damit verbundenen Liefer- und Fertigungsketten durch einen Demonstrator nachgewiesen, und die Ergebnisse werden verbessert (**AP7**).

1.1.1 Arbeitspaket AP1: Ebenenübergreifende Maßnahmen

Das Ziel des Arbeitspakets ist unter anderem die Definition der Angriffs- und Bedrohungsmodelle in Bezug auf die in VE-Jupiter zu entwickelnden Gegenmaßnahmen sowie die Abstimmung mit den Projektpartnern für den in **AP7** zu entwickelnden Demonstrator. Die Arbeiten in diesem Arbeitspaket konnten erfolgreich abgeschlossen werden. Die Angriffs- und Bedrohungsmodelle wurden in Form eines internen

Berichts unter den Projektpartnern ausgetauscht. Für den Demonstrator wurde eine kontinuierliche Integrationsphase festgelegt und die Pulpissimo-Plattform auf einem Field-programmable gate array (FPGA) als gemeinsame Basis ausgewählt. Die erarbeitete Spezifikation des FPGA-basierten Demonstrators wurde im Verlauf des Projekts aufgrund globaler Lieferengpässe angepasst.

1.1.2 Arbeitspaket AP2: Security Atoms

NXP untersucht in **AP2.4** die Verwendbarkeit der vom Partner ASDS erforschten Security Atoms. Aufgrund von Verzögerungen beim Tapeout der Security Atoms konnte NXP während der Projektlaufzeit nur Rückmeldungen zum Konzept geben, die durchweg positiv ausfielen. Eine Anwendbarkeit für Teile von Hochsicherheitsprodukten, wie beispielsweise Secure Elements, scheint angesichts des Zugewinns an Sicherheit und Vertrauenswürdigkeit machbar, wobei die Integration der spezifischen Toolchain in die Hochsicherheitsumgebungen von NXP möglicherweise eine Hürde darstellt.

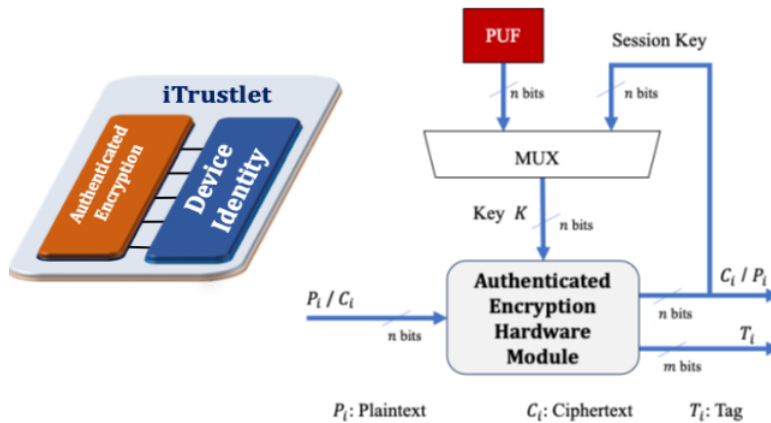
1.1.3 Arbeitspaket AP3: Entwurf und Entwicklung von iTrustlets

In diesem Arbeitspaket erforscht NXP Technologien für iTrustlets mit minimalem Hardwareaufwand und entwickelt einen Technologieträger zur Evaluation.

Es wurde eine HW-Sicherheitsarchitektur und die Zertifizierungsanforderungen eines iTrustlets basierend auf einem Ring-Oszillator basierendem Physically Unclonable Functions (PUF) analysiert. Basierend auf den Ergebnissen wurde eine iTrustlet-Architektur spezifiziert. Neben den Sicherheits- und Zertifizierungsanforderungen wurde auch spezieller Fokus auf den Flächen- und Energiebedarf des iTrustlets gelegt, um auch Anwendungen in Systemen mit eingeschränkten Flächen- und Energieanforderungen zu ermöglichen. Spezieller Fokus der Sicherheitsarchitektur lag auf der Analyse der Anforderungen für die initiale iTrustlet-Authentisierung und der Definition eines entsprechenden Authentisierungsmechanismus. Der Aufbau der iTrustlets ist in Abbildung 1 dargestellt.

In Kooperation mit ITI wurden kryptografische Dienste zur Verwendung in iTrustlets evaluiert und ausgewählt. Für die Architektur eines iTrustlets wurde letzten Endes eine Kombination aus PUF und einer HMAC verwendet. Die Hardware-Realisierung dieses kryptografischen Dienstes wurde unter Berücksichtigung der Vertrauens-

Abbildung 1: Aufbau der kryptografischen Komponenten eines iTrustlets.



Provisionierung aus **AP4** und der in **AP1** definierten Angriffsszenarien konzipiert und spezifiziert. Die Hardware-Implementierung des kryptografischen Dienstes wurde anschließend erfolgreich für den FPGA-Demonstrator umgesetzt.

Als Basis für die Systemintegration und Definition der HW-Schnittstellen wurde ein RISV-V Pulpissimo-System ausgewählt, um die Systemintegration zu demonstrieren und um mit akzeptablem Aufwand die Funktionalität des iTrustlets demonstrieren und die Eigenschaften bzgl. Laufzeiten und benötigten SW-Ressourcen durchführen zu können. Das iTrustlet-IP und dessen Integration in das Pulpissimo-System wurden entsprechend der Spezifikation vorgenommen und anschließend verifiziert. Dabei wird das iTrustlet direkt mit der Peripherie (AXI) und die zu schützende IP mit dem iTrustlet verbunden. Der IP-Zugriff wird durch das iTrustlet gesteuert und erfolgt nur, wenn die Authentizität und Unversehrtheit des iTrustlets gewährleistet und geprüft ist. Das Gesamtsystem wurde um ein Secure Element als Master-iTrustlet, verbunden und über eine SPI-Schnittstelle, erweitert. Das Secure-Element wurde in einem Bindungsverfahren mit dem integrierten iTrustlet verbunden und ein sicherer Austausch von Informationen konnte erfolgreich verifiziert werden.

Des Weiteren wurde das iTrustlet mit der in **AP4** entwickelten Lebenszyklus-Manager-Hardware-IP verbunden und im weiteren Verlauf des Projekts evaluiert. Die Verwendbarkeit in den verschiedenen Anwendungsszenarien wurde basierend auf Simulationen bestätigt und charakterisiert. Auch die Entwicklung und Erprobung der zuvor realisierten iTrustlet-Komponenten mit Fokus auf größenoptimierte kryptografische Dienste und Speicherung der Credentials wurde planmäßig durchgeführt.

Für die zu entwickelnde Evaluationsplattform hat sich auf Basis der in **AP1** und **AP6** entwickelten Angriffsmodelle eine gesteigerte Relevanz für Forschung an elektromagnetische Fehlerinjektion (EMFI) ergeben. Daher wurde die Evaluationsplattform von Laserbasierte Fehlerinjektion (LFI) in Rücksprache mit dem Projektträger auf EMFI umgeplant und anschließend aufgebaut. Alle Komponenten konnten in Betrieb genommen werden und eine Charakterisierung der EMFI-Quelle (Injektionsspule) wurde vorgenommen. Verbesserung und Erweiterung der Evaluationsplattform fanden im weiteren Verlauf des Projekts statt um nach Abschluss von **AP6** die Konstruktionen bzw. Modelle durch physikalische Messungen zu validieren.

1.1.4 Arbeitspaket AP4: A&U-Sicherung im Lebenszyklus

In **AP4** hat NXP Methoden, Prozesse und IP erforscht, die im Produktlebenszyklus nach Ende der Fertigung die Prüfung von A&U mit starkem Vertrauen ermöglichen. Dies basiert auf der in **AP3** entwickelten iTrustlets-Technologie, wobei mehrere Vertrauensendpunkte (iTrustlets) und eine zentrale Verwaltung (Master-iTrustlet) integriert wurden.

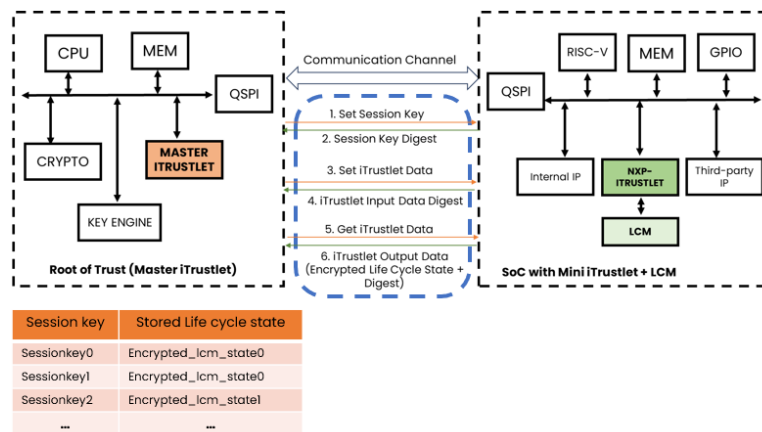
Der gesamte Produktlebenszyklus von Halbleiter- und Elektronikprodukten wurde analysiert und ein Lebenszyklus-Modell entwickelt, das speziell die Produktionstest- und Provisionierungsphase berücksichtigt. Die typischen Lebenszyklusphasen wurden in Pre-Silicon, Post-Silicon und Field Usage unterteilt, wobei jede Phase detailliert betrachtet wurde. Aus den gesammelten Erkenntnissen wurden eine generische Lebenszyklus-Management-Architektur entwickelt um die systemweite Authentizität und Integrität sicherzustellen. Besonderer Fokus lag dabei auf dem Schutz der Lebenszyklus-Übergänge gegen Manipulationen. Daraus wurde eine HW/SW-Architektur zur Lebenszyklus-Kontrolle unter Verwendung des in **AP3** realisierten iTrustlets spezifiziert.

Anschließend wurde die Sicherheitsarchitektur basierend auf der Lebenszyklusmanagement-Architektur und den in **AP1** definierten Angriffsszenarien weiter verbessert. Die Komponenten des Lebenszyklusmanagers wurden detailliert spezifiziert. Sie beinhalten Authentifizierungsprotokolle, Integritätsprüfungen sowie einen Sicherheitsbrennmechanismus (fuses) zur Verhinderung von Rollback-Angriffen. Dabei wird der Zugriff auf den Lebenszyklusmanager durch ein iTrustlet geschützt. Es wurden zwei Sicherheitskonzepte untersucht: ein HW/SW-Co-Design und ein Konzept, bei dem

alle sicherheitsrelevanten Komponenten mit einem iTrustlet ausgestattet sind. Die sichere Verbindung zwischen dem iTrustlet und dem Master-iTrustlet gewährleistet die Authentizität und Integrität der Lebenszyklusmanager-IP (LCM-IP).

Zur Evaluation wurde das SE050 Secure Element von NXP als Root of Trust für die Bereitstellung von Vertrauen für die einzelnen Systemkomponenten verwendet. Das Secure Element ist nach Common Criteria EAL 6+ und FIPS 140-2 zertifiziert und bietet starken Schutz gegen komplexe Angriffsszenarien. Es ermöglicht eine sichere Schlüsselgenerierung und ist über ein sicheres Bindungsverfahren mit dem iTrustlet und anderen vertrauenswürdigen Komponenten verbunden.

Abbildung 2: Sicheres Bindungsprotokoll und sichere Kommunikation zwischen Master-iTrustlet und Life-Cycle-Manager mit iTrustlet.



Anschließend wurden Kommunikationsprotokoll zur sicheren Bindung zwischen iTrustlet und Master-iTrustlet definiert und Lösungen zur Kommunikation zwischen dem Vertrauensanker, dem iTrustlet und anderen Komponenten des Systems entwickelt. Das I2C-Kommunikationsprotokoll wurde als HW-Kommunikationskanal zwischen den Komponenten verwendet. Aufgrund nicht funktionsfähiger Schnittstellen in der Open-Source-Plattform PULPissimo war eine Implementierung eines dedizierten SPI-Kommunikationsprotokolls erforderlich, was zu einer Verzögerung im Projekt führte. Das SPI-Protokoll stellt eine stabile Kommunikation zwischen dem FPGA (PULPissimo + iTrustlet) und dem Root of Trust sicher. Die Integration des LCM mit dem iTrustlet gemäß dem in **AP4** vorgeschlagenen Konzept wurde erfolgreich umgesetzt und ist in Abbildung 2 dargestellt.

1.1.5 Arbeitspaket AP5: A&U-Prüfung Analog

In diesem Arbeitspaket waren keine Beiträge von NXP geplant.

1.1.6 Arbeitspaket AP6: “Secure-by-Design”-EDA-Werkzeuge

AP6 befasst sich mit der Forschung an Werkzeugen und Werkzeugflüssen zur Unterstützung des “Secure-by-Design”-Konzepts. Bestandteil der Arbeiten von NXP in diesem Arbeitspaket ist die Erforschung und Konzipierung von Verifikationsroutinen zur Bewertung der Resistenz gegen Seitenkanal-, Fehlerinjektions- sowie kombinierte Angriffe auf Hardwareschaltungen.

Eine zentrale Voraussetzung für die automatisierte formale Verifikation sind Modelle, die sowohl für Menschen als auch Maschinen lesbar sind und eine große Breite an praxisrelevantem Verhalten präzise darstellen können. Die geplanten Modellierungsarbeiten konnten planmäßig abgeschlossen werden. Als Ergebnis wurde eine industrietaugliche Modellierungssprache zur Repräsentation von Seitenkanal- und Fehlerinjektionsverhalten in Hardwareschaltungen erarbeitet. Diese Sprache ergänzt das weit verbreitete “Liberty”-Format von Synopsys. Testweise konnten die Ergebnisse einer Charakterisierung der physikalischen Prozesse von EMFI aus einer Veröffentlichung in ein für Verifikation geeignetes Modell in diesem Format transformiert werden. Ein Auszug des Modells für ein logisches UND-Gatter mit Seitenkanal- und Fehlerinjektionsverhalten in der entwickelten Sprache ist in Abbildung 3 dargestellt.

Des Weiteren wurden formale Sicherheitseigenschaften und Angreifermodelle unter Berücksichtigung der praktischen Angriffsmodelle aus **AP1** definiert und dokumentiert. Während dieser Tätigkeiten wurden mögliche Modellerweiterungen identifiziert, die eine dedizierte physikalische Charakterisierung erforderten, wofür die in **AP4.3** zu erstellende Evaluationsplattform von LFI auf EMFI umgestellt wurde.

In Zusammenarbeit mit der TU Graz konnte NXP eine grundlegend neue Methode entwickeln, um beweisbar vollständige Abstraktionen des Seitenkanalverhaltens von Hardwareschaltungen mit Microcodes zu erstellen und zu beweisen. Diese Modelle sind von erheblicher Bedeutung aufgrund ihrer verlässlichen Vollständigkeit und beschleunigen das Absichern von Software erheblich, ermöglichen jedoch auch systematische Änderungen an Prozessorimplementierungen mit dem Ziel, das Seitenkanalverhalten zu verbessern. Diese Arbeiten wurden auf der renommierten Fachkon-

Abbildung 3: Auszug eines Modells mit Seitenkanal- und Fehlerinjektionsverhalten.

```
1 library(jupiter) {
2   cell(AND2) {
3     pin(A1) { direction : input ; }
4     pin(A2) { direction : input ; }
5     pin(X) {
6       direction : output ;
7       function : "(A2&A1)" ;
8       faults() {
9         EMFI_LFI_set: "_ => 1";
10        EMFI_LFI_reset: "_ => 0";
11        EMFI_LFI_set_A1: "_ => A2"; /* reflected by faults on the output of the parent cell */
12        EMFI_LFI_set_A2: "_ => A1";
13        LFI_add: "_ => X^f"; /* f is controlled by an adversary, only interesting for pins carrying multiple bits */
14        EMFI_area_sub: "F11_in_tile_1234 => f"; /* representation of faults which affect multiple cells in some area (
15           ↪ computed from physical placement) */
16        EMFI_area_toggle: "F12_in_tile_1234 => ~X";
17      } /* these faults also affect the unstables (i.e., they are effective during the whole cycle) */
18    }
19    leakages() {
20      stable: "[final(X)]";
21      transition: "[final(X), initial(X)]";
22      glitch: "[unstables(X)]; /* requires accurate computation of unstables */
23    }
24  }
25 }
```

ferenz ACM SIGSAC Conference on Computer and Communications Security (CCS) 2022 veröffentlicht [2] und auch auf Fachseminaren präsentiert sowie für den “Tag der Vertrauenswürdigen Elektronik” 2023 und 2024 eingereicht.

In Zusammenarbeit mit ITS wurde an verbesserten Konstruktionen auf Basis des polynomiellen Maskings zur kombinierten Seitenkanal- und Fehlerinjektionsresistenz geforscht. Dabei konnte die Effizienz des Stands der Technik durch neuartige Konstruktionen wesentlich gesteigert und ein “Secure by Design“-Compiler entwickelt werden. Diese Arbeit wurde auf der renommierten Fachkonferenz CRYPTO der International Association for Cryptologic Research (IACR) veröffentlicht [1]. Darüber hinaus konnten mehrere Sicherheitsreduktionen und Verifikationsansätze abgeleitet werden. Eine erste Sicherheitsreduktion betrifft Angriffe auf Masken (gleichverteilte Zufallswerte), die in der Masking-Gegenmaßnahme verwendet werden. Diese Reduktion erlaubt es, den Rechenaufwand der Verifikation signifikant zu verringern, da die Resistenz gegen Seitenkanal- und Fehlerinjektionsangriffe separat betrachtet werden kann. Eine ähnliche Reduktion konnte für das additive Fehlerinjektionsmodell identifiziert werden.

Das vom amerikanischen National Institute of Standards and Technology (NIST) standardisierte Post-Quanten-Kryptographie-Schlüsselaustauschschemata “ML-KEM” Kyber wurde von NXP vollständig gegen Seitenkanalangriffe gehärtet, indem effiziente Algorithmen mit höherwertiger Maskierung konzipiert und testweise implementiert

wurden. Die gehärteten Implementierungen wurden nicht nur physikalischen Messungen unterzogen, sondern auch mit Verifikationswerkzeugen analysiert. Dazu wurde eine neue Verifikationsmethodik für maskierte Lookup-Tables konzipiert. Die Ergebnisse wurden auf der renommierten Fachkonferenz CHES der IACR veröffentlicht [3]. Es wurden zwei Patente beantragt und gewährt; "Masked Decoding of Polynomials" NXP Semiconductors Patent US11595195B2, sowie "Masked IND-CCA2 Comparison Circumventing Compression in Post-Quantum Schemes" NXP Semiconductors Patent US11528124B2.

Ein zentraler Bestandteil von **AP6** ist die Entwicklung eines neuen Verifikationskernels für die automatische Prüfung der Seitenkanal- und Fehlerinjektionsresistenz, die in Zusammenarbeit mit ITS sowie teilweise der TU Darmstadt CAC als externem Partner erfolgte. Insbesondere kombinierte Resistenz unterliegt einem kombinatorischen Problem, das besonders rechenaufwändig ist und sehr effiziente Algorithmen erfordert.

In einer gemeinsam mit ITS betreuten Masterarbeit konnte gezeigt werden, dass der zu Projektbeginn gewählte syntaxbasierte Verifikationsansatz aufgrund des "Phase-Ordering"-Problems eine inhärente Limitation entweder in Skalierbarkeit oder Korrektheit aufweist. NXP konnte gemeinsam mit ITS einen neuen Verifikationskernel entwickeln, der auf Equivalence Graphs und Equivalence Saturation basiert. Dadurch kann das "Phase-Ordering"-Problem nicht nur umgangen werden, sondern es wird auch die Falsch-Negativ-Rate von sprach- bzw. syntaxbasierten Verifikationsansätzen erheblich reduziert. Gleichzeitig erhält der neue Ansatz die wesentlich bessere Skalierbarkeit gegenüber SAT-basierten Ansätzen, da er weiterhin syntaxbasiert ist. Darüber hinaus ist der Ansatz flexibel erweiterbar und kann spezifisch auf Probleme wie komplexe Transformationen zwischen booleschem und arithmetischem Masking angewendet werden. Diese strategische Neuausrichtung steigert die Verwertbarkeit der EDA-Verifikation und somit die Bedeutung der VE-Jupiter-Projektergebnisse erheblich.

Der neue Verifikationskernel bietet erhebliche Vorteile, führt jedoch auch zu zusätzlichem Implementierungs- und Evaluierungsaufwand sowie Nachbesserungen an den in **AP6** bereits umgesetzten Arbeiten. Dieser Kernel wurde im weiteren Projektverlauf zu Evaluationszwecken implementiert. Dabei wurde festgestellt, dass der initiale Ansatz bei höheren Sicherheitsordnungen fehlerbehaftet war und weitere Nachbesserungen erforderte. In mehreren Iterationen wurden Adaptionen des Ansatzes

evaluiert und testweise implementiert. Umfangreiche Known-Answer-Tests und tiefgehende mathematische Analysen haben schrittweise zu Verbesserungen geführt. Zur Sicherstellung der Korrektheit und Transparenz hat NXP wesentliche Beiträge zur mathematischen Theorie und Beweisbarkeit des finalen Ansatzes geleistet. Während dieser Arbeiten wurden spezielle Verifikationsregeln konzipiert, die die Verifikation von polynomiellen Maskierungen und Algorithmen zur Transformation zwischen booleschem und arithmetischem Masking ermöglichen.

Zur Reduzierung der Risiken wurde die Evaluation des neuen Verifikationskerns auf die beweisbare Resistenz gegen Seitenkanalangriffe fokussiert. Die Benchmarks der experimentellen Prototypen sind in der ersten Spalte (JUPITER) von Tabelle 1 dargestellt. Zu beachten ist, dass die Geschwindigkeit des experimentellen Technologieträgers dabei bis auf eine Ausnahme auch bei sehr hohen Sicherheitsordnungen den Stand der Technik übertrifft aber gleichzeitig eine wesentlich breitere Anwendbarkeit, insb. auf Algorithmen zur Transformation zwischen booleschem und arithmetischem Masking (B2A). Der testweise entwickelte Technologieträger wird von ITS als Open-Source-Werkzeug veröffentlicht. NXP konnte bereits nachweisen, dass eine interne Implementierung, bei der das im Vorgängerprojekt entwickelte Verifikationswerkzeug "scVerif" ein falsch-negatives Ergebnis ausgab, mit dem neuem Ansatz korrekt verifiziert werden konnte. Somit löst der in VE-Jupiter entwickelte Verifikationsansatz auch Probleme, die eine breitere Anwendung von Verifikationsmethoden in industriellen Kontexten bisher blockiert haben.

Die Algorithmen und das zugrundeliegende formale Beweissystem werden als dediziertes Ergebnis in Form eines Fachartikels veröffentlicht und wurden dem Projektträger zugänglich gemacht.

1.1.7 Arbeitspaket AP7: Demonstrator & Evaluation

Die in **AP1** für den Demonstrator gewählte FPGA Plattform wurde erfolgreich aufgesetzt und ist in Abbildung 4 dargestellt. Die RISC-V Plattform PULPissimo wurde um ein iTrustlet erweitert und die sichere Kommunikation zwischen einem NXP SE050 als Root-iTrustlet und iTrustlet konnte erfolgreich validiert werden. Zur weiteren Evaluation wurde ein Raspberry Pi zwischen Root-iTrustlet und iTrustlet geschaltet um Man-in-the-Middle Angriffe in der Kommunikation einfacher zu simulieren. Anschließend wurde das Zusammenspiel zwischen Root-iTrustlet, iTrustlet, Lebenszyklus-IP

Tabelle 1: In unseren Benchmarks benötigten Instanzen, die mit “-” gekennzeichnet sind, mehr als eine Stunde zur Verifikation. Experimente, die mit ✓ markiert sind, wurden korrekt verifiziert, solche, die mit ✗ markiert sind, konnten von den EDA-Werkzeugen nicht verifiziert werden, und für ✗ waren keine Gadgets vorhanden.

Gadget	t	Tool					
		JUPITER	SILVER	IRONMASK	MASKVERIF	CHECKMASKS	
ISW Add	3	<1s	2s	<1s	<1s	✗	
	4	<1s	4m 16s	<1s	<1s	✗	
	5	<1s	-	<1s	<1s	✗	
	6	<1s	-	2s	<1s	✗	
	7	<1s	-	1m 7s	10s	✗	
	8	1s	-	-	1m 20s	✗	
	9	4s	-	-	-	✗	
	ISW Ref	4	<1s	4s	<1s	<1s	<1s
		5	<1s	3m 31s	<1s	<1s	24s
6		<1s	-	2s	<1s	26m 46s	
7		<1s	-	4s	<1s	-	
8		<1s	-	2m 14s	4s	-	
9		<1s	-	-	22s	-	
ISW Mul	3	<1s	13s	<1s	<1s	<1s	
	4	2s	-	<1s	<1s	1m 28s	
	5	10m 30s	-	<1s	18s	-	
	6	-	-	7s	3m 2s	-	
B2A [4]	1	<1s ✓	(✓)	✗	✗	<1s ✓	
	2	<1s ✓	(✓)	✗	✗	<1s ✓	

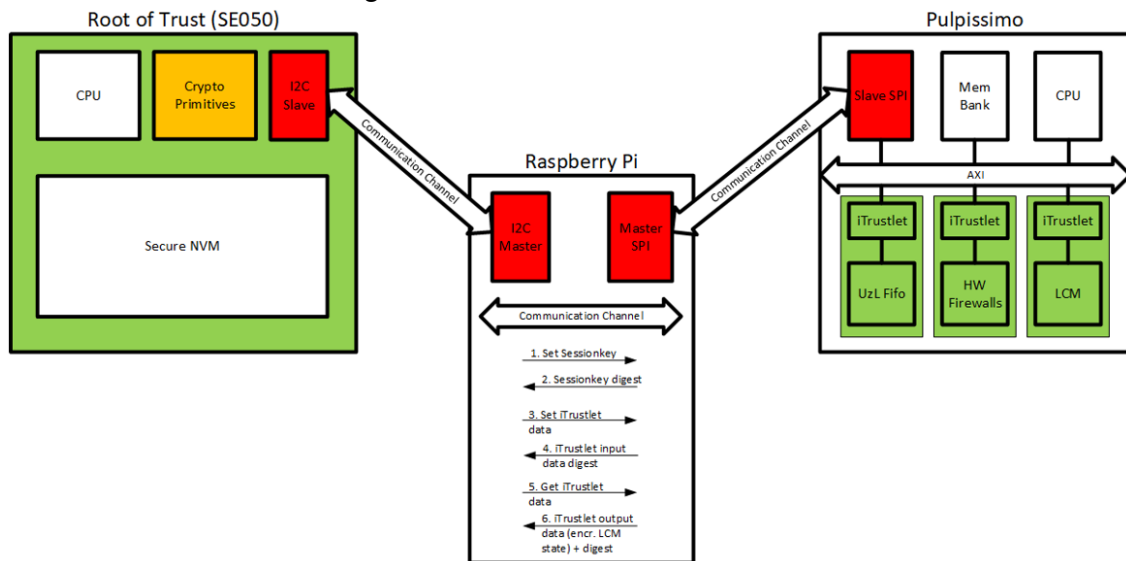
sowie der Hardware Firewalls im weiteren Verlauf des Projekts erfolgreich validiert und in einem Anwendungsszenario gegenüber ausgewählten Angriffen aus **AP1** evaluiert.

Die Anwendbarkeit des Verifikationstools wurde in einem separaten Demonstrator evaluiert und zum Projektabschluss gezeigt.

1.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die Fördermittel wurden im Wesentlichen zur Finanzierung des Personalaufwandes verwendet. Es wurde eine Mittelumwidmung aus dem Reisebudget auf das Material-

Abbildung 4: Aufbau des FPGA-Demonstrators



budget vorgenommen um den zusätzlichen Materialaufwand von 5 T€ für die Evaluationsplattform bei konstantem Gesamtbudget zu kompensieren.

1.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die in VE-Jupiter durchgeführten Arbeiten sind zum einen sehr kompliziert und forschungsintensiv gewesen und haben daher einen erheblichen Personalaufwand verursacht. Auf der anderen Seite entsprechen die Ergebnisse der Zielsetzung und die entstandenen Aufwände sind somit lohnend gewesen.

Gerade im Sicherheitsbereich sind Ebenen-übergreifende, holistische Lösungen erforderlich, die sowohl wegen des enormen Forschungs- und Innovationsbedarfs als auch wegen der erforderlichen spezialisierten technologischen Kompetenzen kaum von einer Einzelpartei gestemmt werden können. Für das stattdessen erforderliche konzertierte Vorgehen sind erhebliche Personalaufwände und Sachkosten zu bestreiten, die die vorwettbewerbliche FuE-Intensität von NXP überschreiten und angesichts der großen technischen Herausforderungen hohe wirtschaftliche Risiken als Einzelunternehmen bergen. In Anbetracht des potenziell hohen Zugewinns an Sicherheit über die gesamte Lebenszeit und Lieferkette von Elektronik-Produkten (**AP3, AP4, AP6**) eignen sich die Herausforderungen allerdings optimal für ein "high risk-high gain" Verbundforschungsprojekt zwischen Industrie und Universitäten.

Die Notwendigkeit der Zuwendung ergibt sich auch durch die unumgängliche Entwicklung eines neuen Verifikationsansatzes im bereits fortgeschrittenen Projekt die erst durch die umfangreiche Analyse des initialen Verifikationsansatzes bekannt geworden ist. Eine derart ergebnisoffene und gleichzeitig aufwändige Analyse ist in unternehmerischen Kontexten ohne entsprechend geförderter Kooperation unwirtschaftlich. Daher wäre ohne Zuwendung ein derartiger Durchbruch wie durch den neuen Ansatz auf Basis von Equivalence Graphs und Equivalence Saturation nicht zu erwarten gewesen.

1.4 Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse bzw. Erfahrungen

Die in VE-Jupiter entwickelten Ergebnisse die Entwicklung sicherer und vertrauenswürdiger Produkte wesentlich verbessert.

Die patentierten Algorithmen für maskierte Post-Quanten Kryptographie übertreffen bekannte Konkurrenzlösungen und werden durch interne Transferprojekte bereits in 1-2 Jahren Vorteile für kommerzielle Produkte darstellen.

NXP wird die gesammelten Erkenntnisse zu iTrustlets, den sicheren Bindungsprotokollen und dem Lebenszyklusmanager in der Weiterentwicklung der eigenen Hardware-Plattformen für vertrauenswürdige Sensoren, Prozessoren und Hardware Root-of-Trusts, z.B. Secure Elements und Edge-Lock, nutzen und so verschiedene Anwendergruppen in Deutschland und Europa stärken.

Das Verifikationstool "scVerif" aus dem Vorgängerprojekt "VeriSec" befindet sich bereits in einem internen Transferprojekt. Dies ermöglicht die in VE-Jupiter entwickelten neuartigen EDA-Verifikationsroutinen zeitnah zu verwerten, indem die bisherigen Verifikationsroutinen in "scVerif" ersetzt werden. Die verbesserten Eigenschaften und die Anwendbarkeit auf Designs mit Fehlerinjektionsresistenz wird NXP in die Entwicklung von sicherem IP einbringen und so u.a. durch Kostenreduktionen bzw. Effizienzsteigerungen den Standort mit seinen hochqualifizierten Arbeitsplätzen stärken. Darüber hinaus wird NXP die Erkenntnisse zu iTrustlets und sicheren Bindungsprotokollen in die Produktentwicklung in Industrie 4.0, Automotive, Edge-Computing und Industrial Internet of Things einbringen.

Die erforschten innovativen Polynomielle Maskierungstechniken mit verbesserter Effizienz sind bereits Bestandteil weiterer Forschungen über das Projekt und die Partner hinaus. Dies stärkt das Forschungsnetzwerk von NXP durch weitere Kooperationen mit anderen Forschungsstellen. Das entwickelte Verifikationstool soll zeitnah auf andere Konstruktionen angewendet werden, insbesondere Post-Quanten Kryptographie und polynomielle Maskierung. Daraus resultieren erwartungsgemäß

- neue bzw. verbesserte Techniken zum Schutz gegen kombinierte Seitenkanal- und Fehlerinjektionsangriffe,
- Verbesserungen im Laufzeitverhalten des Verifikationstools und den prüfbaren Sicherheitsdefinitionen, sowie
- eine verbesserte Anwendbarkeit auf Hard- und Softwareimplementierung z.B. durch Unterstützung maskierter Table-Lookups.

Die iTrustlets und die sicheren Bindungsprotokolle können im Bezug auf verbesserte Sicherheitsparameter, Skalierbarkeit und Adaptionfähigkeit aber auch ihrer automatisierten Integration und Anwendung in anderen, z.B. dynamischen, Umgebungen weiter erforscht werden.

Die Wissenschaftliche Anschlussfähigkeit ist ausgezeichnet, weil das Verifikationswerkzeug durch den Partner ITS der Uni Lübeck als Open Source verfügbar gemacht wird und so die zuvor genannten konkreten Forschungsthemen aber auch weitere Themen mit anderen Partnern und Universitäten vorgenommen werden können. Ein Folgeprojekt u.a. zum Transfer der Forschungsergebnisse im Bereich der iTrustlets und dem Verifikationswerkzeug befindet sich bereits mit weiteren Partnern in Abstimmung.

1.5 Während der Durchführung des Vorhabens bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Die Publikationen von anderen Forschungseinrichtungen bestätigen weiterhin die signifikante Bedeutung von holistischen Sicherheitslösungen und EDA-Verifikation. Es sind keine Publikationen bekannt geworden die die Fortschritte des Vorhabens in ihrer Bedeutung schmälern.

1.6 Erfolgte und geplante Veröffentlichungen der Ergebnisse

Bisher sind folgende wissenschaftliche Veröffentlichungen entstanden:

IACR CRYPTO Combined Fault and Leakage Resilience: Composability, Constructions and Compiler Sebastian Berndt, Thomas Eisenbarth, Sebastian Faust, Marc Gourjon, Maximilian Orlt, and Okan Seker CRYPTO 2023, Lecture Notes in Computer Science, vol 14083. Springer, Chambridge

ACM CCS Power Contracts: Provably Complete Power Leakage Models for Processors Roderick Bloem, Barbara Gigerl, Marc Gourjon, Vedad Hadzic, Stefan Mangard, and Robert Primas Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022, ACM 2022, pp. 381–395

IACR CHES Masking Kyber: First- and Higher-Order Implementations Joppe W. Bos, Marc Gourjon, Joost Renes, Tobias Schneider, and Christine van Vredendaal IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.4 (2021), pp. 173–214

Eine weitere Publikation zu den iTrustlets in Verbindung mit den HW-Firewalls, sowie weitere Publikationen zum Verifikationswerkzeug befinden sich in Begutachtungsprozessen bzw. Erstellung.

Darüber hinaus wurden Teil- sowie Zwischenergebnisse auf folgenden Konferenzen und Workshops präsentiert:

Tage der vertrauenswürdigen Elektronik Poster Alexander Treff, Pajam Pauls, Maximilian Orlt, Marc Gourjon Juni 2024, München, Deutschland

Tage der vertrauenswürdigen Elektronik Poster Christian Ewert, Andrija Neskovic, Felix Muss, Saleh Muhlem, Mladen Berekovic, Rainer Buchty, Alexander Treff, Thomas Eisenbarth, Carsten Heinz, Andreas Koch, Marc Gourjon Juni 2024, München, Deutschland

EGRAPHS superVer: Verifying Probabilistic Independence of Systems of Expressions using Equality Saturation Alexander Treff, Pajam Pauls, Maximilian Orlt, Marc Gourjon EGRAPHS 2024, June 2024, Copenhagen, Denmark

Tage der vertrauenswürdigen Elektronik Poster Christian Ewert, Andrija Neskovic, Felix Muss, Saleh Muhlem, Mladen Berekovic, Rainer Buchty, Alexander

Treff, Thomas Eisenbarth, Carsten Heinz, Andreas Koch, Marc Gourjon 2023, Deutschland

VeriSiCC Fine-Grained Power Leakage Models and Verification of Software Masking
Marc Gourjon Verification and Generation of Side-Channel Countermeasures
(VeriSiCC Seminar 2022), September 22nd 2022, Paris, France

TASER Power Contracts: Provably Complete Power Leakage Models for Secure Execution of Masked Software on Processors Marc Gourjon Topics in hArdware SEcurity and RISC-V (TASER), September 18th 2022, Leuven, Belgium

Tage der vertrauenswürdigen Elektronik Vortrag Nils Müsegaes 2022, virtuell

TASER Panel Discussion Markku-Juhani O. Saarinen, Patrick Karl, Shoei Nashimoto, Marc Gourjon, and Andy Dellow Topics in hArdware SEcurity and RISC-V (TASER), September 18th 2022, Leuven, Belgium

Literatur

- [1] S. Berndt, T. Eisenbarth, S. Faust, M. Gourjon, M. Orlt, and O. Seker. Combined fault and leakage resilience: Composability, constructions and compiler. In H. Handschuh and A. Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 377–409. Springer, 2023.
- [2] R. Bloem, B. Gigerl, M. Gourjon, V. Hadzic, S. Mangard, and R. Primas. Power contracts: Provably complete power leakage models for processors. In H. Yin, A. Stavrou, C. Cremers, and E. Shi, editors, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, pages 381–395. ACM, 2022.
- [3] J. W. Bos, M. Gourjon, J. Renes, T. Schneider, and C. van Vredendaal. Masking kyber: First- and higher-order implementations. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(4):173–214, 2021.
- [4] J. Coron. High-order conversion from boolean to arithmetic masking. In W. Fischer and N. Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 93–114. Springer, 2017.

Kurzbericht zu VE-Jupiter: Eindeutige Identifizierbarkeit für vertrauenswürdige Mikroelektronik mit Chiplets

Dieser Kurzbericht beschreibt die von NXP Semiconductors Germany GmbH (NXP) erzielten Ergebnisse in dem vom BMBF geförderten Verbundforschungsprojekt "VE-Jupiter" mit Förderkennzeichen 16ME0231.

Aufgabenstellung Das Verbundforschungsprojekt VE-Jupiter befasste sich mit der Sicherheit von Elektronikprodukten über deren gesamten Lebenszyklus. Durch eine innovative Kombination von Methoden, die über alle Phasen der Produktentstehung, der Produktfertigung und dem Einsatz im Feld ineinandergreifen, wird ermöglicht die Authentizität und Unversehrtheit (A&U) von allen elektronischen Komponenten über die komplette Lieferkette sicherzustellen und jederzeit zu prüfen.

Das Teilvorhaben von NXP adressiert den Entwurf vertrauenswürdiger Elektronik. Fokus liegt dabei im Schutz des Hersteller-IP, der Absicherung von Entwürfen, und dem Erzeugen von Vertrauen gegenüber komplexen und unsicheren Fertigungsketten.

Zum einen wurden "iTrustlets" erforscht, dabei handelt es sich um kostengünstige Hardware-Vertrauensanker die in die verschiedenen Komponenten eines Elektronikprodukts integriert werden können und erlauben die A&U durch Hersteller, Systemintegratoren und Endkunden jederzeit zu prüfen. Zum anderen wurden Mechanismen erforscht um iTrustlets sicher zu verbinden und somit die A&U eines Gesamtsystems prüfbar zu machen und Manipulationen zu detektieren. Ein weiterer Bestandteil von VE-Jupiter sind Techniken zur EDA-Verifikation, die erlauben die Entwicklung von Hardware-IP mit Resistenz gegen weitverbreitete physikalische Seitenkanal- und Fehlerinjektions-angriffe zu beschleunigen und gleichzeitig die Sicherheit und Vertrauenswürdigkeit europäischer Designs zu verbessern.

Die entwickelten Technologien steigern die Vertrauenswürdigkeit der Elektronik und tragen zur Vermeidung von Manipulationen & zur technologischen Souveränität bei.

Ablauf des Vorhabens Die Arbeiten von NXP konzentrierten sich auf Arbeitspakete **AP1**, **AP3**, **AP4**, **AP6** und **AP7**. In einer anfänglichen Bestandsaufnahme in **AP1** wurden die grundlegenden Sicherheitsdefinitionen, Gegenmaßnahmen, die Zielplattform und Zielkriterien festgelegt. Anschließend fand in **AP3** die Konzeption und Entwicklung der iTrustlets statt. Darauf aufbauend wurde in **AP4** die Absicherung eines Gesamtsystems anhand eines Life-cycle-managers erarbeitet. Zum anderen ermöglicht

die verlässliche Absicherung von Intellectual Property (IP) und iTrustlet-Hardware (HW) mittels automatisierter Verifikation (**AP6**) die Prüfung flexibler Sicherheitslevel, sodass die Entwicklungsprozesse agiler gestaltet werden können. Die Arbeitspakete **AP2**, **AP3**, **AP4** und **AP6** beinhalten Wechselwirkungen. Mit Erreichen der Zielkriterien wurden in **AP7** basierend auf den iTrustlets und dem EDA-Werkzeug zwei Demonstratoren entwickelt. Das Projekt lief vom 01.03.2021 bis zum 31.08.2024.

Wesentliche Ergebnisse und Zusammenarbeit mit anderen Einrichtungen

Die iTrustlet Technologie und der Lebenszyklusmanager konnten anhand eines Demonstrators in einem konkreten Anwendungsfall erfolgreich evaluiert werden und stellen nachweislich eine breit nutzbare Technologie mit Anschlussfähigkeit an vorhandene und etablierte Standards und Normen wie z.B. "Common Criteria", "SESIP" und IEC 62443 dar.

Die entwickelten Routinen zur formalen EDA-Verifikation übertreffen nachweislich die Projektanforderungen und den Stand der Technik in Bezug zur Anwendbarkeit (z.B. Post-Quanten Kryptographie), Skalierbarkeit (hohe Sicherheitsparameter, größere Implementierungen), Genauigkeit (keine Falsch-Negativ Ergebnisse) und Erweiterbarkeit. Auch die entwickelten Sprachen und Verfahren zur Modellierung von physischem Seitenkanal- und Fehlerinjektionsverhalten erfüllen die Praxisanforderungen von NXP und übertreffen den Stand der Technik deutlich.

Der konzipierte "Secure by Design" Compiler für kombinierte Resistenz übertrifft den Stand der Technik. Erkenntnisse in diesen Arbeiten haben zu mehreren Komplexitätsreduzierungen und neuen Beweismethoden in der formalen Verifikation geführt.

Während der Laufzeit von VE-Jupiter stand NXP im engen Austausch mit den Projektpartnern aber auch mit weiteren Institutionen. Gemeinsam mit der **TU Graz** wurde eine industrietaugliche Modellierungssprache zur Repräsentation von praxisnahem Seitenkanalverhalten von Prozessoren konzipiert und ein Verifikationswerkzeug entwickelt, welches es erstmalig erlaubt die Genauigkeit und Vollständigkeit solcher Modelle gegenüber der Implementierung eines Prozessors zu prüfen. Gemeinsam mit der **Chair of Applied Cryptography** der **TU Darmstadt** und dem Partner ITS der Uni Lübeck wurden verbesserte Schemata auf Basis von polynomiellen Maskierungen für kombiniert Fehler- und Seitenkanal-resistente Kryptographie entwickelt, sowie an dazugehörigen Verifikationstechniken erforscht. Beide Zusammenarbeiten haben zu Veröffentlichungen auf renommierten Konferenzen geführt.