Differenzielle Kryptanalyse von Symmetrischen Primitiven[1]

Maria Eichlseder[2]

Abstract: Symmetrische Kryptographie stellt hocheffiziente Verfahren zur Verfügung, die Vertraulichkeit und Integrität von Daten in diversen Anwendungen schützen. Die Sicherheit dieser Verfahren ruht auf deren Primitiven, wie Blockchiffren oder Permutationen. Die spezifischen Anforderungen an Funktionalität, Effizienz und Robustheit dieser Primitive sind im steten Wandel, was sich in einer regen Publikation neuer Designs und Designprinzipien niederschlägt.

In dieser Dissertation entwickeln wir Techniken zur differenziellen Kryptanalyse verschiedener Primitive. Unsere Ergebnisse zeigen dabei signifikante Schwachstellen in einigen neuen Designs auf. Zusätzlich entwickeln und evaluieren wir verbesserte Strategien in der automatisierten Kryptanalyse.

Keywords: Kryptographie Differenzielle Kryptanalyse Hashfunktionen Authenticated Encryption

1 Einleitung

IT-Systeme verarbeiten heute mehr sensible Informationen denn je, darunter private persönliche Daten und vertrauliche Geschäftsdaten. Um diese Daten zu schützen, werden kryptographische Algorithmen wie Verschlüsselungsverfahren und Hashfunktionen benötigt. Ein zentraler Faktor für die Sicherheit dieser kryptographischen Algorithmen ist die Widerstandsfähigkeit ihrer Kernbestandteile, der sogenannten Primitive wie beispielsweise Blockchiffren, gegen Angriffe wie differenzielle, lineare und algebraische Kryptanalyse. Das Ziel der Kryptanalyse ist es, unsichere Primitive zu identifizieren sowie den sogenannten „Security Margin“ (ein Maß für die Sicherheit ausgehend von den derzeit besten Angriffen) von sicheren Primitiven möglichst genau zu schätzen. Beides ist wichtig, um sichere Verfahren für die Zukunft zu gewährleisten.

Differenzielle Kryptanalyse ist dabei eine der bedeutendsten Angriffsmethoden und versucht, geheime Informationen zu extrahieren oder Nachrichten zu fälschen, indem das Verhalten der Primitive statistisch untersucht wird, wenn zwei ähnliche, aber leicht unterschiedliche Eingaben verarbeitet werden. Seit Einführung Anfang der 1990er [BS90] hat sich diese Methode als ausgesprochen effektiv und vielseitig bewährt, und entsprechende Gegenmaßnahmen gehören daher zu den Grundpfeilern beim Design von modernen Blockchiffren.

Während symmetrische Kryptographie jahrzehntelang quasi synonym zum Design und der Analyse von Blockchiffren war, sind in den letzten Jahren auch alternative Primitive ins akademische Rampenlicht gerückt: Insbesondere kryptographische Permutationen

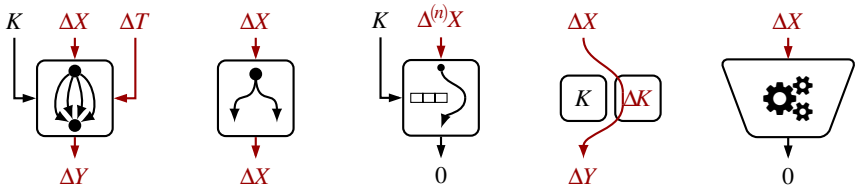
[1] Englischer Titel der Dissertation: „Differential Cryptanalysis of Symmetric Primitives“

[2] Technische Universität Graz, maria.eichlseder@iaik.tugraz.at

und tweakbare Blockchiffren (tweakable blockciphers, TBCs) machen Blockchiffren ihre Rolle als ideale Primitive für effiziente, sichere und elegante Verfahren streitig. Diese Primitive bieten dem Kryptanalysten allerdings eine veränderte Angriffsoberfläche, beispielsweise durch schlüssellose Rundenfunktionen oder durch zusätzliche kontrollierbare Tweak-Inputs in jeder Runde. Die Implikationen dieser Unterschiede sind bislang nur unzureichend untersucht und der entsprechende kryptanalytische Werkzeugkasten noch nicht ausgereift.

Als zentrale Ergebnisse der Dissertation [Ei18] zeigen wir, dass die von Blockchiffren übernommenen Design-Strategien nicht immer ausreichenden Schutz gegen differenzielle Angriffe bieten können. Wir zeigen neue Analysetechniken und potenzielle Schwachstellen auf, die bei neuen Designs berücksichtigt werden sollten. Mehrere in den letzten Jahren publizierte vielversprechende Primitive, beispielsweise die in Software besonders performante Permutation Simpira oder die leichtgewichtige TBC MANTIS, konnten auf diesem Wege geknackt werden. Abb. 1 gibt einen symbolischen Überblick über die vorgeschlagenen Analysetechniken, -szenarien, und -ziele. Zusätzlich entwickeln wir Techniken zur Verbesserung der computergestützten differenziellen Analyse von schlüssellosen Primitiven und erreichen damit die besten praktischen Kollisionsangriffe auf mehrere reduzierte Varianten der Hashfunktion SHA-2, was maßgeblich dazu beiträgt, den Security Margin dieses weltweit intensiv genutzten Standards einzuschätzen – SHA-2 kommt unter anderem im Großteil aller https-gesicherten Web-Verbindungen oder in Bitcoin zum Einsatz.

Weitere Beiträge und Ergebnisse von Kollaborationen im Rahmen des Doktorats, die nicht im Dissertationstext ausgeführt werden, betreffen die praktische Sicherheit von kryptographischen Implementierungen und Designs. Wir nutzen unter anderem Techniken aus der differenziellen Kryptanalyse, um zu zeigen, dass ein Angreifer mit speziellen physikalischen Fehlerangriffen (Statistical Ineffective Fault Attacks, SIFA: Abb. 3) durch Stören der Berechnungen geheime Informationen lernen kann – selbst wenn die Implementierung eigentlich mit den gebräuchlichen Gegenmaßnahmen gegen genau solche Angriffe ausgestattet ist. Ein bedeutendes Ergebnis ist die Mitentwicklung und Analyse des authentifizierten Verschlüsselungsverfahrens Ascon, das besonders effiziente und ressourcenschonende Implementierungen ermöglicht, die dabei robust gegen verschiedene Implementierungsangriffe sind. Ascon wurde 2019 als Gewinner der 2014 gestarteten „CAESAR Competition“ für kryptographische Designs in der Kategorie „Lightweight Applications“ ausgezeichnet.



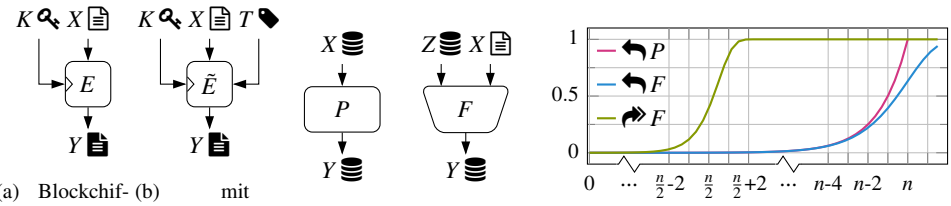
(a) MANTIS (b) Simpira (c) LowMC (d) Prøst (e) SHA-2

Abb. 1: Überblick über die entwickelten differenziellen Analysetechniken und analysierte Primitive.

2 Hintergrund

Kryptographische Primitive sind die kleinsten Bausteine in einem kryptographischen System, mit denen ein Sicherheitslevel assoziiert werden kann. Die darüberliegenden Schichten, wie Modes of Operation oder Protokolle, führen ihre Sicherheit jeweils – idealerweise in Form eines Reduktionsbeweises – auf diese Primitive zurück. In der asymmetrischen Kryptographie sind diese Primitive typischerweise (mehr oder weniger nahe) verwandt mit klassischen Problemen der Komplexitätstheorie, während die symmetrischen Kryptographie immer wieder neue, effiziente Circuits dazu entwickelt. Die meisten klassischen symmetrischen Primitive sind Blockchiffren, d.h. Familien von Permutationen mit einer fixen Inputgröße von beispielsweise 128 Bits, wobei ein geheimer Schlüssel K eine Permutation E_K aus dieser Familie auswählt, mit der dann die Klartextblöcke X in Ciphertextblöcke Y übersetzt werden. Der Angreifer versucht, aus beobachteten Daten (X,Y) entweder den Schlüssel K oder andere Informationen über die Permutation E_K abzuleiten, um damit die Sicherheit der darüberliegenden Ebenen zu untergraben, wie etwa die Vertraulichkeit der Nachricht in einem authentifizierten Verschlüsselungsverfahren.

Eine limitierende Eigenschaft des Blockchiffren-Modells ist die fehlende Abbildung des Kontexts der übersetzten Daten, etwa der Adresse des Blocks innerhalb der Nachricht. Das muss auf darüberliegenden Ebenen kompensiert werden, was diverse Probleme mit sich bringt. Als Lösungsansatz bieten tweakbare Blockchiffren eine explizite zusätzliche Inputmöglichkeit, den Tweak T, während Permutationen mit vergrößertem Input die Grenzen zwischen Daten, Schlüssel und Kontext für die Berechnung völlig verschwimmen lassen. Intern folgen die Primitive grundsätzlich einer ähnlichen Struktur, bei der eine einfache, durch K,T parametrisierte Rundenfunktion oft iteriert wird; durch die verschiedene Parametrisierung und typische Blockgrößen ergeben sich jedoch Unterschiede im konkreten Design. Abb. 2 illustriert die entstehenden Interfaces der Primitive sowie einige generische Schranken für deren Sicherheit, die sich aus diesen Interfaces ergeben.



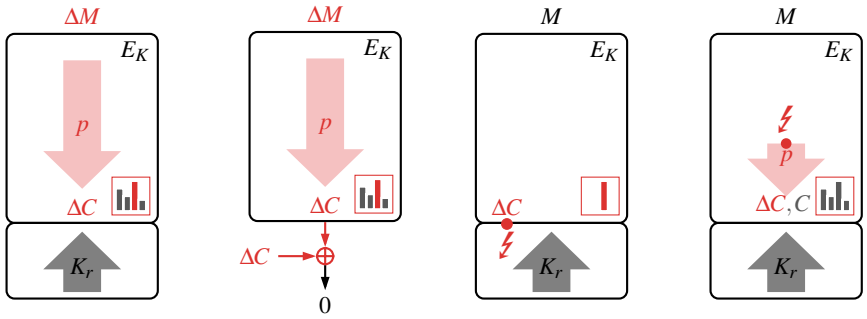
(a) Blockchiffre (b) mit Tweak (c) Permutation (d) Kompression (e) $\mathbb{P}$[Erfolg] nach 2^x Versuchen mit $n = |Y|$

Abb. 2: Verschiedene Typen symmetrischer Primitive sowie generische Erfolgswahrscheinlichkeit von Preimage- (↶) und Kollisionsangriffen (↷) auf Permutationen (P) und Funktionen (F).

Das Ziel differenzieller Kryptanalyse [BS90] ist, Schwachstellen in den Primitiven zu identifizieren, die effizientere Angriffe als diese generischen Schranken erlauben. Sei $f : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto y$ eine vektorielle Boolesche Funktion, etwa eine Blockchiffre mit einem fixen unbekannten Schlüssel. Wir betrachten Paare von Inputvariablen (x,x^*) mit einer Differenz $\Delta x = x^* \oplus x$ und interessieren uns für die Outputdifferenz $\Delta y = y^* \oplus y$, genauergesagt, für die von einer fixen Inputdifferenz $\alpha = \Delta x$ induzierte Ableitungsfunktion

$$\Delta_\alpha f(x) := f(x \oplus \alpha) \oplus f(x)\,.$$

Selbst wenn der Wert x bzw. der Schlüssel K mit $f = E_K$ unbekannt sind, lassen sich gegebenenfalls Aussagen über die statistische Verteilung $\mathsf{edp}(\alpha,\beta) := \mathbb{P}_{K,x}[\Delta_\alpha f_K(x) = \beta]$ von β treffen. Dazu werden mögliche Charakteristiken χ, die resultierende Differenzen nach jeder Runde in f beschreiben, sowie ihre erwartete Wahrscheinlichkeit $p = \mathsf{edp}(\chi)$ untersucht. Gibt es eine Charakteristik χ und damit ein Differential (α,β) mit $-\log_2(\mathsf{edp}(\alpha,\beta)) < \min(n,|K|)$ für (fast) die volle Rundenanzahl von f, so lässt sich f mit einer Komplexität in der Größenordnung $\mathsf{edp}(\alpha,\beta)^{-1}$ von einer zufälligen Funktion unterscheiden und damit beispielsweise der Schlüssel K ableiten oder eine Nachricht fälschen (Abb. 3). Eine notwendige Bedingung für ein sicheres Design ist also die Nicht-Existenz so einer Charakteristik mit hoher Wahrscheinlichkeit. Diese klassische Bedingung ist aber keineswegs hinreichend, wie mehrere Ergebnisse dieser Dissertation zeigen.



(a) DC: Schlüssel (b) DC: Fälschungen (c) DFA: Schlüssel (d) SIFA: Schlüssel

Abb. 3: Differenzen in Angriffen: Differenzielle Kryptanalyse (DC) und Fehlerangriffe (DFA, SIFA).

3 Differenzielle Kryptanalyse neuer symmetrischer Primitive

Im ersten Teil der Dissertation werden vier kürzlich vorgeschlagene neue Primitive und darauf basierende Modes analysiert. Die Analysetechniken bedienen sich dabei im weiteren Sinne der differenziellen Kryptanalyse. Da klassische differenzielle Analyse selbstverständlich bei allen untersuchten Primitiven im Designprozess berücksichtigt wurde und daher die Existenz geeigneter Charakteristiken durch die Designer ausgeschlossen wurde, schlagen wir verschiedene neue Techniken vor, die das Interface sowie konkrete Designentscheidungen ausnutzen. Die Ergebnisse beinhalten Full Breaks, also Widerlegung des Security Claims der Autoren in Form praktischer oder theoretischer Angriffe, aber auch Schwachstellen in reduzierten Primitiven mit verringerter Rundenzahl oder in einer Verwendungsweise, die nicht vom Security Claim abgedeckt wird. Mehrere unserer Angriffe konnten inzwischen weiterentwickelt und verbessert oder auf weitere Ziele angewendet werden. Zwei der Designs wurden in Reaktion auf die Angriffe aktualisiert, um die Schwachstellen zu beheben.

Unser erstes Analyseziel ist die leichtgewichtige tweakbare Blockchiffre MANTIS, publiziert auf der CRYPTO 2016 [Be16], der Top-Konferenz im Bereich Kryptographie. Durch den zusätzlichen Tweak-Input T, der der Kontrolle des Angreifers unterliegt, können unabhängig vom Inputblock X weitere Differenzen in die Ausführung eingebracht werden. Die Designer berücksichtigen dies grundsätzlich und beweisen, dass trotzdem keine einzelne Charakteristik der Variante MANTIS-5 eine Wahrscheinlichkeit über 2^{-68} bei einer Blockgröße von $n = 64$ Bits aufweist. Zusätzlich schränken sie den Angreifer sicherheitshalber auf ein Datenlimit von 2^{30} Chosen-Plaintext Queries ein.

Eine erste Beobachtung zu dem Design ist, dass sich aufgrund spezieller differenzieller Eigenschaften der leichtgewichtigen Hauptbausteine von MANTIS, nämlich der involutiven S-box und der Near-MDS-Matrix im linearen Layer, vergleichsweise leicht verschiedene passende Charakteristiken χ zum selben Differential (α, β) finden lassen. In Folge entwickeln wir ein Framework zum Finden und Bewerten von großen, strukturierten Clustern aus Charakteristiken, die wir als Semi-Truncated Differential Characteristics bezeichnen. Diese kombinieren Vorteile von Truncated Characteristics (die etwa mit Mixed-Integer Linear Programming oder SMT-Solvern gesucht werden und einfach approximativ zu bewerten sind) mit der präziseren Auswertung und höheren Wahrscheinlichkeit von einzelnen Charakteristiken (per Hand oder mit dem in section 4 beschriebenen Tool gesucht) und sind besonders bei der Analyse von leichtgewichtigen Blockchiffren mit Tweak nützlich. Zusätzlich beschreiben wir, wie damit besonders effizient der geheime Schlüssel abgeleitet werden kann. Auf diese Weise finden wir einen Cluster mit einer hohen Wahrscheinlichkeit von 2^{-39}, dessen spezielle Struktur es außerdem erlaubt, passende Inputs mit noch geringerer Datenkomplexität von etwa 2^{25} und damit unter dem von den Designern gesetzten Limit zu finden. In einer detaillierten Analyse identifizieren wir noch weitere Eigenschaften von MANTIS, die die Komplexität in die eine oder andere Richtung beeinflussen. Eine praktische, nicht parallelisierte Implementierung der Attacke findet schlussendlich den Schlüssel in unter einer Stunde, während die Designer von einer Mindestlaufzeit von astronomisch hohen 2^{96} Verschlüsselungsäquivalenten ausgingen. Die Publikation [Do17] wurde als eine der drei besten auf der Konferenz FSE 2017 ausgezeichnet.

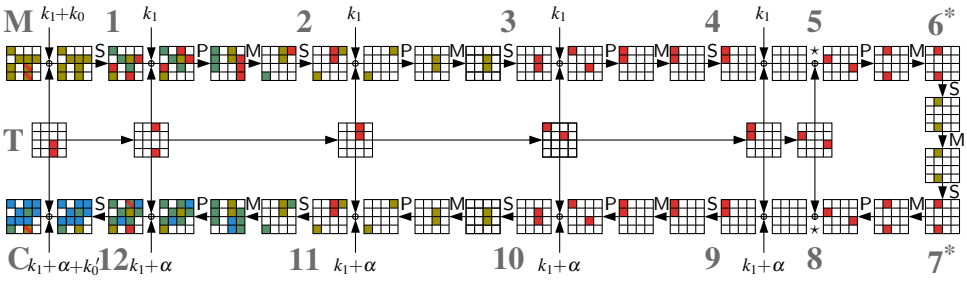


Abb. 4: Semi-Truncated Differential Characteristic für MANTIS-5 mit verschieden großen Mengen an erlaubten Differenzen pro Zelle ($|\chi_i| \in \{1$ ■, 4 ■, 13 ■, 15, 16 ■$\}$)

Unser zweites Analyseziel ist die Permutation Simpira [GM16], deren Designer (Intel, NIST) besonders auf hohe Performance auf modernen Desktop-CPUs abzielen. Dazu schlagen sie ein generalisiertes Feistel-Netzwerk (GFN) aus rundenreduzierten AES-Instanzen vor, das mit Intels AES-NI und vergleichbaren Instruktionserweiterungen anderer Plattformen äußerst effizient in Software implementierbar ist. Gleichzeitig soll die Verwendung der bewährten und gut analysierten AES-Rundenfunktion sowie des beweisbar sicheren Feistelnetzwerks einen hohen Security Margin bieten.

Wir können zeigen [DEM16], dass die computergestützte Sicherheitsanalyse der Designer (ebenso wie der Sicherheitsbeweis des GFNs) mehrere Abhängingkeiten zwischen Zwischenergebnissen der Permutation außer Betracht lässt. Dadurch sind die hergeleiteten Schranken für die maximale differenzielle Wahrscheinlichkeit einzelner Charakteristiken von 2^{-450} ungültig. Tatsächlich können mit einer theoretischen Komplexität von „nur“ 2^{110}, also weniger als dem Security Claim von 2^{128}, differenzielle Fixpunkte für die volle 512-bit-Permutation Simpira-4 gefunden werden (Abb. 5). In der von den Designern vorgeschlagenen Verwendung mit Feed-Forward als Hashfunktion entspricht das einer Kollision. Die Ergebnisse zeigen, wie unvorhersehbar der Security Margin bei schlüssellosen Primitiven wegen interner Abhängigkeiten sowie der Möglichkeit für den Angreifer, Zwischenergebnisse zu kontrollieren und deterministische Startstrukturen zu konstruieren, sein kann. Die Designer haben mittlerweile eine aktualisierte Variante Simpira v2, die den Fehler durch eine Neukonstruktion des GFNs behebt, publiziert.

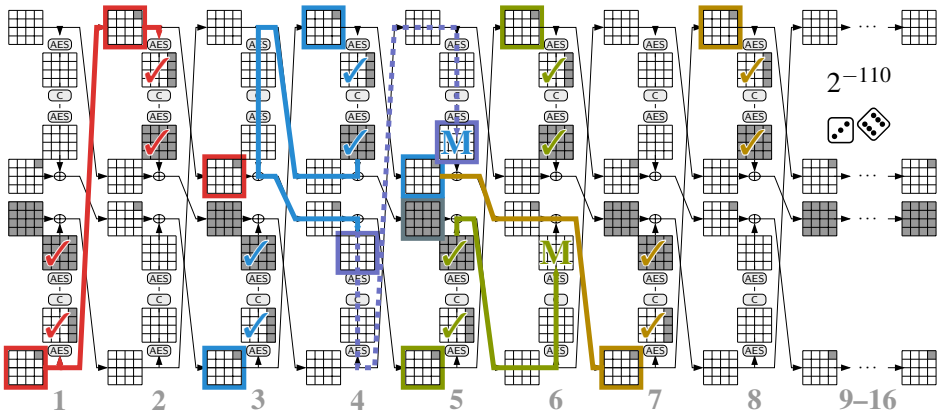


Abb. 5: Differenzieller Fixpunkt für Simpira-4 mit 16 von 15 Runden: 40 statt 80 aktive S-boxen, davon 20 deterministisch erfüllbar (markiert) und 20 probabilistisch mit Wahrscheinlichkeit 2^{-110}

Weitere Analyseziele, die in der Dissertation diskutiert werden, sind die Blockchiffre LowMC (EUROCRYPT 2015) sowie das permutationsbasierte authentifizierte Verschlüsselungsverfahren Prøst (ein Kandidat in Runde 1 der CAESAR Competition). LowMC ist durch sein Designziel – die Minimierung der multiplikativen Komplexität – besonders anfällig gegen höherdimensionale differenzielle Angriffe, die nicht nur die erste Ableitung $\Delta_\alpha f(x)$, sondern höhere Ableitungen $\Delta^{(d)}_{\alpha_1,\ldots,\alpha_d} f(x) := \Delta_{\alpha_d} \cdots \Delta_{\alpha_1} f(x) = \bigoplus_{\alpha \in \langle \alpha_1 \ldots \alpha_d \rangle} f(x \oplus \alpha)$ betrachten und so den bereits niedrigen algebraischen Grad der Funktion weiter reduzieren. Wir erweitern dabei den von den Designern bereits analysierten einfachen Distin-

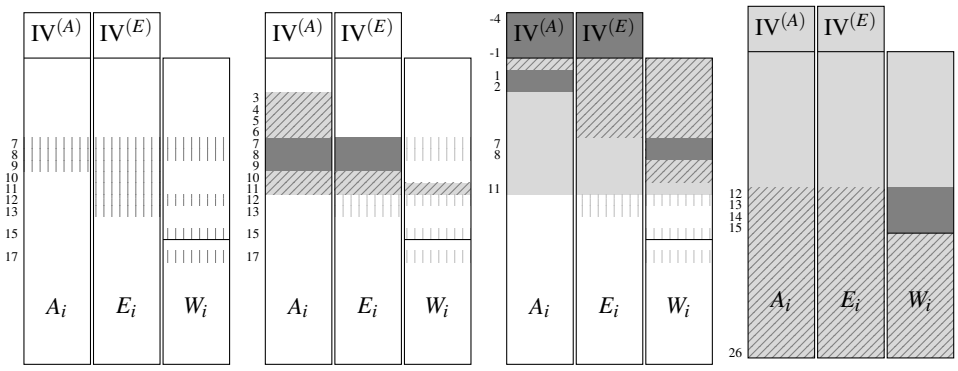
guisher um bis zu 4 Runden (bei einem Security Margin von nur 5 Runden), indem wir mehrere differenziell invariante Unterräume konstruieren und verketten. Die Designer haben mittlerweile eine aktualisierte Version LowMC v2 mit einem größeren Security Margin vorgeschlagen. Bei Prøst analysieren wir ausnahmsweise nicht das Primitiv, sondern den Mode of Operation, und zeigen, wie ein Angreifer, der Nachrichten unter zwei verwandten Schlüsseln beobachten kann, sehr einfach Fälschungen konstruieren kann. Diese Beobachtung ist zwar unerwartet, ist aber keine Bedrohung für die Sicherheit von Prøst.

Zusammenfassend zeigen unsere Ergebnisse, dass Design und Sicherheitsanalyse von schlüssellosen, tweakbaren, oder anderweitig atypischen Primitiven für aktuelle Anwendungs-Bedürfnisse nach wie vor eine Herausforderung sind. Insbesondere strikte Performance-Anforderungen können zu Designs führen, deren hochoptimierte Bausteine unerwünschte Eigenschaften mit sich bringen, die in klassischen Analysemethoden schwer einkalkulierbar sind. Während jeder unserer Angriffe spezifische Schwachstellen der jeweiligen Primitive identifiziert und ausnutzt, sind mehrere der Techniken, beispielsweise Semi-Truncated Differential Characteristics oder die Linearisierungstechniken für algebraische Analysen, von allgemeinerem Interesse für die Anwendung auf neue Primitive.

4 Automatische Tools für differenzielle Kryptanalyse

Der zweite Teil der Dissertation widmet sich der Verbesserung und Anwendung von automatischen Tools zur differenziellen Kryptanalyse von Hashfunktionen, insbesondere SHA-2. Während im ersten Teil hauptsächlich externe Solver für Mixed-Integer Linear Programming oder Boolean Satisfiability zum Einsatz kamen, wenden wir uns hier einem spezialisierten Such-Tool zu, das von Mendel, Nad und Schläffer [MNS11]für die Kollisionssuche in SHA-2 entwickelt wurde und intern eine spezialisierte Guess-and-Determine-Suche verwendet, die Parallelen zu SAT-Solvern aufweist. Die SHA-2-Familie von Hashfunktionen wird als aktueller US- und internationaler Standard allgegenwärtig eingesetzt, ob für die Integrität in TLS-Handshakes, Zertifikaten, SSH, oder Bitcoin. Die Familie besteht aus zwei Hauptzweigen: SHA-256 (bevorzugt für 32-bit-Plattformen) und SHA-512 (64-bit), wobei der Großteil der bisherigen Analyse sich auf SHA-256 bezieht, SHA-512 auf aktuellen Plattformen aber effizienter ist und gleichzeitig ein höheres Sicherheitsniveau bietet. Unser Fokus sind dabei die Herausforderungen bei der Anwendung vorher für SHA-256 entwickelter Analysestrategien auf SHA-512, die sich aus der doppelten Größe der Kompressionsfunktion von SHA-512 ergeben.

Wir erweitern das bestehende Such-Tool um Techniken zum schnelleren Propagieren von Informationen besonders in linearen Operationen sowie für eine zielgerichtetere Suche durch eine Look-Ahead-Heuristik, die Widersprüche früher identifizieren soll und somit die Zeit minimiert, die in „toten“ Abschnitten des Suchbaums verbracht wird. Mit dem verbesserten Tool können signifikant mehr Runden analysiert werden und so die besten praktische Kollisionsangriffe auf die Varianten von SHA-512 gefunden werden, insbesondere Kollisionen für 27 von 80 Runden (Abb. 6), Semi-Free-Start Collisions für 39 Runden, und Free-Start Collisions für bis zu 44 Runden je nach Variante (vorher bei SHA-512 alle nur für bis zu 24 Runden, bei SHA-256 auch Semi-Free-Start Collisions für 38 Runden).



(a) Charakteristik (b) Dichter Abschnitt (c) IV matchen (d) Sparser Abschnitt

Abb. 6: Phasen der Kollisionssuche für 27-Step SHA-512 mit Message W_i und State-Wörtern A_i, E_i in Step i: Geratene Werte ■ und Differenzen □, abgeleitete Werte ▨, fixe Werte ■ und Differenzen □

Zusätzlich verwenden wir das Tool, um aufzuzeigen, wie ein bösartiger Designer einige Rundenkonstanten im Vorgänger SHA-1 so wählen könnte, dass er ein Kollisions-Backdoor einbaut. Der Wert dieser Rundenkonstanten spielt normalerweise für die Sicherheit keine Rolle, doch wenn der Designer die Konstanten während der Durchführung eines Angriffsversuchs wählt (und diese Konstanten für das Design fixiert), kann er zukünftig ohne weiteren Aufwand Kollisionen mit einem bestimmten Präfix generieren. Wir konstruieren in einer Kollaboration [A114] Konstanten und passende Präfixe, mit denen nachher gültige, kollidierende Dateien in mehreren Formaten (z.B. `.sh`, `.rar`, `.mbr`, `.jpg`) erzeugt werden können (Abb. 7).

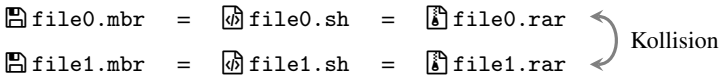


Abb. 7: Malicious SHA-1 mit Polyglot-Kollisionen.

5 Design und Implementierungssicherheit

Neben den obigen Kernthemen, die in der Dissertation ausgeführt werden, lieferte die Forschung im Rahmen des Doktorats auch Beiträge zu etwas breiter gestreuten Themen, insbesondere im Kontext von Implementierungssicherheit und neuen Designs.

Wie in Abb. 3 angedeutet ist ein Angreifer in der Praxis nicht darauf angewiesen, für eine Erlangung des Schlüssels mit differenziellen Methoden die notwendigen Differenzen wie bisher diskutiert über die Inputdaten einzuführen und dann mühsam, mit immer geringerer Wahrscheinlichkeit Runde um Runde, durch die Berechnungen zu verfolgen: Stattdessen kann er auch „schummeln“ und die Differenzen mit physikalischen Mitteln, etwa einem Laser oder durch kurzfristiges Manipulieren der Stromversorgung, direkt kurz vor Ende der Berechnung einfügen und die Effekte wesentlich günstiger auswerten [BS97] (Differential Fault Attack, DFA). Um solche Angriffe zu verhindern, werden in der Praxis diverse Implementierungsgegenmaßnahmen eingesetzt, die fehlerhafte Berechnungen

erkennen (Fault Detection) sowie das Lernen einzelner Zwischenergebnisse durch Seitenkanäle für den Angreifer nutzlos machen (Masking). Gemeinsam mit Kollegen und unter Verwendung der statistischen Analysemethoden der differenziellen Kryptanalyse konnten wir zeigen, dass ein Angreifer trotz dieser üblichen Gegenmaßnahmen ans Ziel kommen und den Schlüssel erlangen kann [Do18b, Do18a], indem er eine Differenz einführt, die abhängig von mehreren Datenpunkten in der weiteren Berechnung vor der Detection wieder verschwinden kann, und dann nur die fehlerfreien Fälle analysiert (Statistical Ineffective Fault Attack, SIFA).

Last but definitely not least ist die Mitentwicklung von Ascon zu erwähnen, einem authentifizierten Verschlüsselungsverfahren, das sich besonders durch ein leichtgewichtiges Design bei hoher Robustheit gegenüber diversen Implementierungsangriffen und -fehlern auszeichnet [Do19]. Ascon wurde 2014 als Kandidat zur CAESAR Competition, einem internationalen Wettbewerb für kryptographische Designs, eingereicht, und 2019 nach jahrelanger Analyse von der Jury als primäre Empfehlung für ressourcenbeschränkte Anwendungen ausgezeichnet. Aktuell ist Ascon Kandidat im „Lightweight Cryptography Standardization Process“ der US-Standardisierungsbehörde NIST.

Literaturverzeichnis

[Al14] Albertini, Ange; Aumasson, Jean-Philippe; Eichlseder, Maria; Mendel, Florian; Schläffer, Martin: Malicious Hashing: Eve's Variant of SHA-1. In (Joux, Antoine; Youssef, Amr M., Hrsg.): Selected Areas in Cryptography – SAC 2014. Jgg. 8781 in LNCS. Springer, S. 1–19, 2014.

[Be16] Beierle, Christof; Jean, Jérémy; Kölbl, Stefan; Leander, Gregor; Moradi, Amir; Peyrin, Thomas; Sasaki, Yu; Sasdrich, Pascal; Sim, Siang Meng: The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In (Robshaw, Matthew; Katz, Jonathan, Hrsg.): Advances in Cryptology – CRYPTO 2016. Jgg. 9815 in LNCS. Springer, S. 123–153, 2016.

[BS90] Biham, Eli; Shamir, Adi: Differential Cryptanalysis of DES-like Cryptosystems. In (Menezes, Alfred; Vanstone, Scott A., Hrsg.): Advances in Cryptology – CRYPTO 1990. Jgg. 537 in LNCS. Springer, S. 2–21, 1990.

[BS97] Biham, Eli; Shamir, Adi: Differential Fault Analysis of Secret Key Cryptosystems. In (Kaliski Jr., Burton S., Hrsg.): Advances in Cryptology – CRYPTO '97. Jgg. 1294 in LNCS. Springer, S. 513–525, 1997.

[DEM16] Dobraunig, Christoph; Eichlseder, Maria; Mendel, Florian: Cryptanalysis of Simpira v1. In (Avanzi, Roberto; Heys, Howard M., Hrsg.): Selected Areas in Cryptography – SAC 2016. Jgg. 10532 in LNCS. Springer, S. 284–298, 2016.

[Do17] Dobraunig, Christoph; Eichlseder, Maria; Kales, Daniel; Mendel, Florian: Practical Key-Recovery Attack on MANTIS5. IACR Transactions on Symmetric Cryptology, 2016(2):248–260, 2017.

[Do18a] Dobraunig, Christoph; Eichlseder, Maria; Groß, Hannes; Mangard, Stefan; Mendel, Florian; Primas, Robert: Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures. In (Peyrin, Thomas; Galbraith, Steven, Hrsg.): Advances in Cryptology – ASIACRYPT 2018. Jgg. 11273 in LNCS. Springer, S. 315–342, 2018.

[Do18b] Dobraunig, Christoph; Eichlseder, Maria; Korak, Thomas; Mangard, Stefan; Mendel, Florian; Primas, Robert: SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3):547–572, 2018.

[Do19] Dobraunig, Christoph; Eichlseder, Maria; Mendel, Florian; Schläffer, Martin: , Ascon v1.2. Submission to NIST's Lightweight Cryptography Standardization Process, 2019. `https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/ascon-spec.pdf`.

[Ei18] Eichlseder, Maria: Differential Cryptanalysis of Symmetric Primitives. Dissertation, Technische Universität Graz, 2018.

[GM16] Gueron, Shay; Mouha, Nicky: , Simpira: A Family of Efficient Permutations Using the AES Round Function. IACR Cryptology ePrint Archive, Report 2016/122, 2016.

[MNS11] Mendel, Florian; Nad, Tomislav; Schläffer, Martin: Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions. In (Lee, Dong Hoon; Wang, Xiaoyun, Hrsg.): Advances in Cryptology – ASIACRYPT 2011. Jgg. 7073 in LNCS. Springer, S. 288–307, 2011.

Maria Eichlseder, geboren 1988, studierte an der Technischen Universität Graz Informatik (B.Sc., M.Sc.) und Technische Mathematik (B.Sc.). Im Anschluss begann sie 2013 ihr Doktoratsstudium unter der Betreuung von Florian Mendel und Christian Rechberger. Sie promovierte 2018 sub auspiciis praesidentis und wurde für ihre Arbeit mit dem Staatspreis für die besten Dissertationen 2018 (Award of Excellence des Bundesministeriums) ausgezeichnet. Das authentifizierte Verschlüsselungsverfahren Ascon, das sie im Rahmen ihres Doktorats mit entwickelte, wurde 2019 zum Gewinner der CAESAR Competition for Authenticated Encryption in der Kategorie „Lightweight Applications“ gekürt. Sie ist derzeit als Postdoc an der TU Graz und forscht im Bereich symmetrische Kryptographie an Kryptanalyse und Design von effizienten Hashfunktionen, authentifizierten Verschlüsselungsverfahren, und deren Primitiven. Schwerpunkte sind dabei mathematische Aspekte der Kryptanalyse, Zusammenhänge zwischen kryptanalytischen und physikalischen Angriffen, sowie automatisierte Werkzeuge und Heuristiken für Kryptanalyse.