INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Bachelorarbeit

Implementierung und Evaluation von WalnutDSA als Modul für den Linux Kernel

Stefan Seil

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 18.12.2017

. . . . . .

(Unterschrift des Kandidaten)

Abstract

Der Trend des *Internet of Things* stellt durch die komplexe Vernetzung vieler leistungsschwacher Geräte neue Herausforderungen an kryptographische Systeme. Zudem werden durch die laufende Forschung an Quantencomputern neue Verfahren benötigt, die vor quantenbasierte Angriffe geschützt sind. WalnutDSA ist ein digitales Signaturverfahren, welches zur Authentisierung von Geräten im Netz eingesetzt werden kann. Der Algorithmus basiert auf der Zopftheorie und verspricht damit geringen Ressourcenverbrauch sowie eine Resistenz gegen Angriffe eines Quantenrechners. Im Rahmen dieser Arbeit wurde WalnutDSA auf einem Rapberry Pi als Modul für den Linux Kernel implementiert. Die Umsetzung wurde gegen zwei andere Implementierungen getestet und bezüglich Rechenzeit und benötigem Speicherplatzverbrauch evauliert. Während die Leistung der Implementierung der Autoren von WalnutDSA nicht erreicht wurde, so kann das Kernelmodul als mögliche Referenzimplementierung des Verfahrens für Linux gesehen werden. Die theoretischen Untersuchungen zeigen, dass WalnutDSA viel Potential für ein zukunftträchtiges digitales Signaturverfahren innehält.

Inhaltsverzeichnis

1 Einleitung

Durch die Fortschritte der Rechnerarchitektur und zugehöriger Herstellungsprozesse können Computer heute in sehr kleinen Formfaktoren hergestellt werden. Die dadurch entstandene Branche des *Internet of Things (IoT)* hat einen rasanten Trend für die Verwendung von stark vernetzten eingebetteten Geräten in bisher analogen Umfeldern gestartet. Aktuelle Schätzungen prognostizieren einen wirtschaftlichen Einfluss der Branche von bis zu 6,2 Billionen US-Dollarn bis 2025 [1]. Für Endkonsumenten sind z.B. bereits rechnergesteuerte Produkte für Türschlösser, Thermostate oder Glühbirnen verfügbar. Aber auch im professionellen Kontext werden immer mehr Bereiche zur Automatisierung von Arbeitsschritten mit Computern ausgestattet, wie z.B. industrielle Kontrollanlagen oder intelligente Stromnetze. Aufgrund der komplexen Vernetzung vieler unterschiedlicher Geräte ergeben sich neue Herausforderungen zur Gewährleistung der Sicherheit und Privatsphäre von Benutzern [2]. Leider verfügen viele IoT-Geräte nicht über ausreichende Sicherheitsmaßnahmen; selbst bekannte Produkte großer Hersteller weisen Sicherheitslücken auf [3].

Um die Kommunikation dieser vernetzten Geräte abzusichern, können die üblichen Sicherheitsprotokolle der IT-Sicherheit verwendet werden. Allerding sind viele Verfahren in der Kryptographie aufgrund zu hohen Rechenaufwands nicht für kleine eingebettete Systeme geeignet. Daher ergibt sich die Suche nach sog. *Lightweight Cryptography* [4], also Verfahren welche auch im Umfeld von leistungsschwachen Computern eingesetzt werden können. Ein Teil der Sicherung von IoT-Geräten besteht in der Verwendung von Authentisierungs- und Authentifizierungsmaßnahmen. Bei der Kommunikation mehrerer Geräte möchte der Empfänger die Identität des Senders bestätigen und sicherstellen, dass sie nicht von einer dritten Partei gefälscht wurde. Es handelt sich also um eine digitale Unterschrift, mit der sich die Rechner im Netz untereinander ausweisen können. Gerade im IoT-Szenario findet kontinuierlich ein Datenaustausch zwischen den zahlreichen Geräten statt, was hohe Anforderungen an die verwendeten Verfahren stellt. Üblicherweise wird zur Authentisierung asymmetrische Kryptographie eingesetzt. Zu den traditionellen Public-Key-Verfahren zählen RSA und DSA, welche häufig in normalen Desktop-Computern oder Serversystemen verwendet werden. Diese Algorithmen basieren jedoch auf sehr rechenintensiven mathematischen Problemen, die sie aus mangelnder Leistung vieler eingebetteter Systeme für den IoT-Sektor weitestgehend ungeeignet machen. So steigt z.B. der Speicherplatzverbrauch der Verfahren zu schnell an, um den laufend wachsenden Erfordernissen an Sicherheitsmaßnahmen gerecht zu werden. Zudem ist seit geraumer Zeit ein Angriff auf Basis eines Quantencomputers bekannt, der die beiden Kryptosysteme bei Verfügbarkeit eines solchen Rechners auf einen Schlag unsicher machen würde.

Eine potentielle Lösung bietet das US-amerikanische Unternehmen SecureRF mit dem digitalen Signaturverfahren *WalnutDSA* [5]. Der Algorithmus verwendet im Gegensatz zu traditionellen asymmetrischen Kryptosystemen Berechnungsprobleme aus drei unterschiedlichen Teilbereiche der Mathematik, allen voran der Zopftheorie. Die Autoren versprechen dadurch ein Verfahren mit kleinem Speicherplatzverbrauch und geringen Leistungsanfor-

derungen für effiziente Signaturen in eingebetteten Systemen, welches zudem auch gegen Angriffe eines Quantencomputers resistent sein soll [6].

Im Rahmen dieser Arbeit soll WalnutDSA als Modul für den Linux Kernel auf einem Raspberry Pi implementiert werden und diese Implementierung folglich in Bezug auf Rechendauer und Speicherplatzverbrauch gegenüber anderen vorhandenen Verfahren untersucht werden. Während das gewählte Gerät wohl leistungsstärker als viele andere häufig verwendete eingebettete Systeme ist, so dient die Implementierung auch zur Anwendung in einem performanteren Kontrollsystem im IoT-Szenario. Zudem kann die Software durch die Verwendung der Programmiersprache C und die weitestgehend plattformunabhängige Entwicklung als Kernelmodul als quelloffene Referenzimplementierung verwendet werden.

Die vorliegende Arbeit ist wiefolgt strukturiert: Zu Beginn wird der Hintergrund zu digitalen Signaturen, der Gefahr von Quantencomputern in der Kryptographie und dem Trend des Internet of Things dargestellt. Anschließend folgt eine Übersicht über den derzeitigen Forschungsstand kryptographischer Verfahren für leistungsschwache eingebettete Geräte bzw. Verfahren mit Resistenz gegen quantenbasierte Angriffe. Es wird eine kurze Einführung in die Zopftheorie und die modulare Arithmetik in endlichen Körpern gegeben sowie die Einwegfunktion des Signaturverfahrens erläutert, um die nötigen mathematischen Grundlagen zu etablieren. Es folgt eine Übersicht über die Bestandteile von WalnutDSA, wobei sowohl auf die grundlegende Funktionsweise als auch auf interessante Aspekte bei der generischen Implementierung eingegangen wird. Im Anschluss soll die Implementierung des Verfahrens unter Linux auf dem Raspberry Pi dargestellt und evaluiert werden, wobei auch auf Probleme bei der Umsetzung sowie auf das Laufzeitverhalten und den Speicherplatzverbrauch des Programms eingegangen wird. In einer Diskussion wird schließlich die Sicherheit des Verfahrens sowie die Umsetzbarkeit und das Potenzial von WalnutDSA untersucht. Zudem werden Vergleiche sowohl zur bisherigen Implementierung von SecureRF als auch zu anderen potentiellen digitalen Signaturverfahren gezogen.

2 Background

——— Der folgende Text ist ein direktes Zitat von [7] ———

Hier geht es um die grundlegende Probleme, an der der Walnut-DSA arbeiten.

2.1 Ziel von Cryptography

Neben der Vertrauchlichkeit, dass nur erlaubte Nutzer Daten lesen können, kann die Kryptographie für andere Ziele verwendet werden.
Integrität: Der Empfänger von Nachricht muss in der Lage sein, die empfange Daten zu überprüfen, ob es während Übertragung modifiziert wurde.
Authenzität: Der Empfänger kann verifizieren, dass Nachricht vom Sender kommt.
Nichtabstreitbarkeit: Der Sender von einer Nachricht kann nicht später verneinen, dass die Nachricht von ihm stammen.[8, S. 2-3]

2.2 Arten von Verschlüsselungsverfahren

Es gibt zwei Arten von Verschlüsselungsverfahren. Die beide Arten unterscheiden sich wegen ihre Schlüsseln. *Symmetrische Verschlüsselungsverfahren*: In dieser Art von Verfahren wird eine Nachricht mit Schlüssl k verschlüsselt und auch entschlüsselt. Dabei erfordet es, dass die beide Partei in der Kommunikation den Schlüssel bereits über einen sicheren Weg austauscht haben[9]. Die Nichtabstreitbarkeit kann es nur mithilfe ein dritte vertrauchte Partei geben[10]. *Asymmetrische Verschlüsselungsverfahren*: Bei dem asymmetrischen Verschlüsselungsverfahren werden unterschiedliche Schlüsseln, wobei ein Teil geheim bleiben und ein anderer Teil öffentlich wird. Bei Verschlüsselung von einer Nachricht, die nur vom Empfänger gelesen werden darf, wird der öffentlichen Schlüssel vom Empfänger verwendet. Da diese Nachricht nur mit dem privaten Schlüssel vom Empfänger entschlüsselbar ist, kann inklusiv der Sender niemand die Nachricht lesen. Dabei wird kein geheimer Schlüsselaustausch nötig.[9]

2.3 Digitale Signatur

Eine digitale Signatur ist eine kryptographische Transformation von Daten über asymmetrische Verschlüsselung. Im Gegensatz zum Fall, wo der Sender seine Nachricht mit dem öffentlichen Schlüssel vom Empfänger verschlüsselt, nutzt der Sender seine eigene private Schlüssel zu Verschlüsselung. Dabei kann man versichern, dass der Sender von der Signatur wirklich die Information anerkannt hat. Als Zusatzeffekt könnte man die digitale Signatur, dafür nutzen, um zu überprüfen, ob gesendete Daten nach Signierung modifiziert wurde. Mit der digitalen Signatur kann man also den orginalen Sender authentifizieren, die Integrität von Daten überprüfen und die Nichtabstreitbarkeit gewinnen.[11, S. 2, 9]

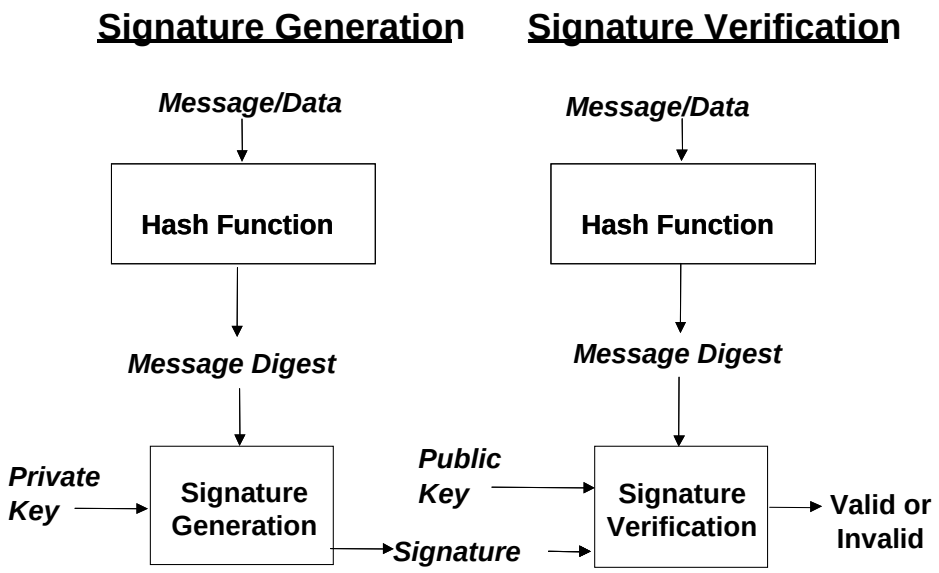


Abbildung 2.1: Digitalen Signatur Prozesse[11, S. 9]

Die Abbildung 2.1 zeigt die Prozesse von digitalen Signaturen. Ein digitale Signatur Algorithmus enthält ein Signaturgenerierungsverfahren und ein Signaturverifikationsverfahren. Bei Generierung von Signatur wird ein privaten Schlüssel vom Sender benötigt. Bei Verifizierung von Signatur wird ein öffentlichen Schlüssel verwendet. Der öffentlichen Schlüssel müssen nicht geheim bleiben, aber die Integrität soll beibehalten werden. Der Empfänger verifiziert die orginale Nachricht und die zugehörige Signatur mithilfe der Signatur. Zudem braucht der Empfänger eine Garantie z.B. über ein Certificate Authority, dass der Sender seine vermeintliche Rechte tatsächlich besitzt. Sonst kann jeder, der irgendein mathematisch korrekte Schlüssel besitzt, kann sich für beliebige Identität signieren, aber der Empfänger hat keine Möglichkeit, diese zu überprüfen. [11, S. 9-10]

2.4 Post-Quanten-Kryptographie

Die klassische öffentlichen Schlüsselverfahren, wie z.B. RSA, basiert sich auf Schwierigkeiten von bestimmten zahlentheoretischen Problemen. Nun wurde es herausgefunden, dass die Quantencomputer mehere zahlentheoretische Probleme exponentiell schneller als den klassischen Computern berechnen können. Dazu fallen Faktorisierung, diskreter Logarithmus, pellsche Gleichung und Berechnung von Einheitengruppe und Idealklassengruppe eines algebraischen Zahlenkörpers[12, S. 17].
Die Abbildung 2.2 zeigt welche Kryptosysteme über einem Quantumalgorithmus gebrochen sind. Die Probleme, die mit Quantencomputer effizient lösbar sind, lassen sich mit dem HSP(Hidden Subgroup Problem) erklären, die eine Generalisierung von Shors Faktoriserung und diskrete Logarithmenalgorithmus ist. Als das HSP muss man für eine gegebene Gruppe und eine Funktion, die konstant und distinkt zu Nebenklassen von einer unbekannten Subgruppe ist, eine Menge von Generatoren für die Subgruppe finden. Es ist dabei entscheidend, um welche Gruppe ein Problem handelt. Ein wichtiger Faktor ist, ob die gegebene Gruppe abelsch ist.

Cryptosystem	Broken by Quantum Algorithms?
RSA public key encryption	Broken
Diffie-Hellman key-exchange	Broken
Elliptic curve cryptography	Broken
Buchmann-Williams key-exchange	Broken
Algebraically Homomorphic	Broken
McEliece public key encryption	Not broken yet
NTRU public key encryption	Not broken yet
Lattice-based public key encryption	Not broken yet

Abbildung 2.2: Aktuelle Sicherheit von klassische Kryptosystem im Bezug zu Quantencomputern[12, S. 16]

Abelian Group G	Associated Problem	Quantum Algorithm?
$\mathbb{Z}_2^n$		Yes
The integers $\mathbb{Z}$	Factoring	Yes
Finite groups	Discrete Log	Yes
The reals $\mathbb{R}$	Pell's equation	Yes
The reals $\mathbb{R}^c$, c a constant	Unit group of number field	Yes
The reals $\mathbb{R}^n$, n arbitrary	Unit group, general case	Open

Abbildung 2.3: Abelsche Gruppen und HSP[12, S. 25]

In der Abbildung 2.3 und 2.4 sieht man verschiedene Gruppen und deren Bezug zu Quantenalgorithmen. Bis auf R^n Gruppe gibt es bereits Quantenalgorithmus, wobei der Algorithmus ab R sehr komplex wird, da die Gruppen nicht mehr abzählbar sind. Für die nichtabelschen Gruppe stehen noch viele offene Fragen, ob sie mithilfe eines Quantenalgorithmus lösbar ist[12, S. 25-29].

2.5 Internet der Dinge

Der Term Internet der Dinge(Kurzgeschrieben *IoT* aus englischen *Internet of Things*) ist die Generalisierung von Geräte, die mit dem Internet verbindbar sind. Typischerweise bezieht man mit IoT Sensoren in Automobile, im Bereich Medizin oder auch z.B. alle Geräte, die mit dem Begriff Smarthome einbezogen werden, die klein und wenig Rechleistung und Speicher zur Verfügung haben[13, S. 113]. In der Regel sind die IoT Geräte nicht nur in der Lage, sich mit dem Netzwerk zu verbinden, sonderen auch sensorische Daten zu sammeln und/oder ihr Umgebung zu modifizieren. Im Gegensatz zu der Kommunikation zwischen RFID Leser und Objekt können IoT Geräte sowohl aktive als auch passive Rolle in der Kommunikation übernehmen[13].
Die grundlegende Sicherheitsprobleme bei den normalen System gelten auch bei IoT. In IoT kommt dazu noch Problem mit beschränkte Rechenleistung und Speicher. Und falls ein Gerät mit einer Batterie getrieben wird, muss man auch auf die Energieeffizienz achten. Außerdem muss man sicherstellen können, wie zuverlässig Geräte, die auch oft verteilt sind, physisch verbunden sind. Im Extremfall kann es passieren, dass ein Komponent plötzlich ausgeht, da der Nutzer woanders den Netzkabel braucht hat und den Kabel deshalb ohne große Achtung rauszieht[14]. Neben den physische Probleme, gibt es Probleme, wie man ein

Nonabelian Group G	**Associated Problem**	**Quantum Algorithm?**
Heisenberg group		Yes
$\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, r constant		Yes
$\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$, p a fixed prime		Yes
Extraspecial groups		Yes
$\downarrow$?		
Dihedral group $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$	Unique shortest lattice vector	Subexponential-time
Symmetric group S_n	Graph isomorphism	Evidence of hardness

Abbildung 2.4: nichtabelsche Gruppen und HSP[12, S. 26]

zuverlässig ein IoT Gerät identifiziert und wie man eine sichere Verbindung baut. Einer von Lösungsvorschläge ist, dass man die MAC Addresse von jeweilige Geräte nutzt. Diese kann aber von einem bösartigen Sender verfälscht werdem und IoT System hat keinen Weg, dabei zu überprüfen, ob die Nachricht von den legitime Nutzer(in diesem Fall auch ein Gerät) kommt. Eine andere Variante ist Einsatz von asymmetrische Verschlüsselungsverfahren. Das Problem dabei ist, dass derartige Verfahren oft große Menge von Ressourcen verbraucht, die bei den IoT Geräten eher wenig vorhanden ist. [13].

——— Ende des Zitats. ———

3 Braids

Die Zopftheorie geht auf den österreichischen Mathematiker Emil Artin zurück, welcher sie mit seiner 1925 erschienenen Arbeit *Theorie der Zöpfe* [15] ins Leben rief. Die Theorie lässt sich in den mathematischen Teilbereich der Topologie einordnen und beschäftigt sich sowohl mit dem geometrischen Aufbau von Zöpfen, als auch mit ihren zugrundeliegenden algebraischen Eigenschaften.

In der Kryptographie hat die Zopftheorie erst recht spät Anklang gefunden; die ersten Arbeiten erschienen 1999 [16] und 2000 [17]. Daher handelt es sich bei der Braid-basierten Kryptographie um ein noch recht neues Konzept, welches jedoch durch die Abweichung von den traditionellen mathematischen Problemen kryptographischer Verfahren als auch durch die intuitive Verständlichkeit der Zopftheorie einen interessanten Kandidaten für moderne und zukunftsträchtige Kryptosysteme darstellt.

Im Folgenden soll eine kleine Einführung in die Zopftheorie gegeben werden, um die mathematischen Grundlagen für WalnutDSA zu etablieren. Für eine detailliertere Ausarbeitung siehe bspw. *An Introduction to Braid Theory* [18], woran sich folgendes Kapitel anlehnt. Aufgrund der überwiegend englischsprachigen Literatur in der Braid-basierten Kryptographie wird im Rahmen dieser Arbeit neben dem deutschen Begriff ,,Zopf" auch der englische Begriff ,,Braid" verwendet werden. Beide Terminologien haben jedoch dieselbe Bedeutung.

3.1 Grundlagen der Braid-Theorie

Ein Zopf bzw. Braid ist eine Verflechtung aus mehreren Strähnen im dreidimensionalen Raum. Sei der Raum ein Würfel und nehme man n Strähnen Schnur, so müssen vier Eigenschaften erfüllt sein, sodass es sich dabei um einen sog. *n-Braid* mit n Strähnen handelt [18, 5]:

1. Keine Strähne liegt ganz oder teilweise außerhalb des Würfels.
2. Jede Strähne beginnt an der Oberseite des Würfels und endet an dessen Unterseite.
3. Zwei verschiedene Strähnen können sich nicht überschneiden, sonder nur nebeneinander bzw. vor- oder hintereinander vorbei laufen.
4. Die Strähnen bewegen sich kontinuierlich nach unten, sodass kein Teil horizontal oder nach oben verläuft.

Abbildung 3.1 zeigt links einen 3-Braid; die rechte Konstruktion ist kein Braid, da die vierte Eigenschaft nicht erfüllt wird.

Es existiert eine mögliche Äquivalenz zwischen mehreren solchen n-Braids mit n Strähnen. Ein n-strähniger Braid b ist äquivalent zu einem weiteren b', wenn die einzelnen Strähnen

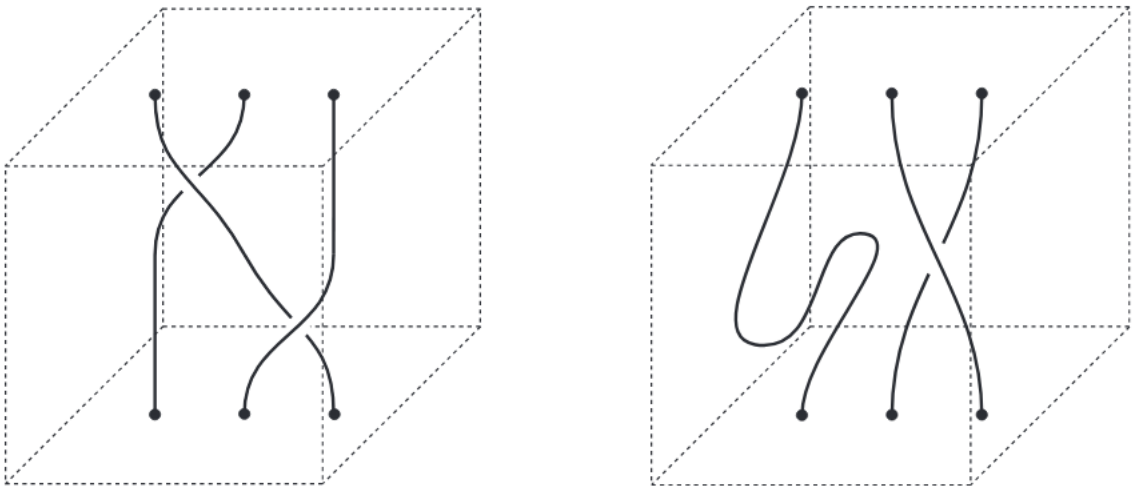


Abbildung 3.1: Links ein 3-Braid, rechts kein Braid. Quelle: [18].

von b so ,,verschoben" werden können, dass der Braid b' entsteht. Dabei müssen jedoch stets die vier besagten Eigenschaften erfüllt sein, und es darf keine Strähne durchgeschnitten und wieder zusammengeklebt oder ihr Anfangs- oder Endpunkt im Würfel verschoben werden. Abbildung 3.2 zeigt zwei äquivalente 2-Braids.

Zur einfacheren Veranschaulichung kann die dreidimensionale Projektion sowie der Würfel selbst weggelassen werden und ein Braid auf einer Ebene dargestellt werden. Hierbei sollen vermeintliche Überschneidungen so gesehen werden, dass eine durchlaufende Strähne über einer durchtrennten verläuft. Abbildung 3.3 zeigt die zweidimensionale Darstellung des 3-Braids aus Abbildung 3.1.

Die essentielle Operation in den Zopfgruppen ist die Multiplikation. Zwei n-Braids b und b' können multipliziert werden, indem man b' an das untere Ende von b anhängt und dabei die Enden der Strähnen verschmelzt. Abbildung 3.4 zeigt das Produkt aus zwei 3-Braids.

Die Äquivalenzklassen aller Braids mit n Strähnen, die obige Eigenschaften erfüllen, bilden die Zopfgruppe B_n. Die Verknüpfung ist hierbei die Multiplikation. Das Einselement ist der n-Braid mit ausschließlich geraden Strähnen ohne Überkreuzungen. Die Inverse eines n-Braids ist dessen Spiegelung am horizontalen unteren Ende. Abbildung 3.5 zeigt wieder den bekannten 3-Braid mit seiner Inversen.

3.2 Artingeneratoren und Braid-Permutation

Eine mögliche Repräsentierung von Braids besteht in Form von *Artingeneratoren*. Dies sind die einfachsten n-Braids in der Zopfgruppe B_n, abgesehen vom trivialen Braid. Geometrisch ausgedrückt ist ein Artingenerator b_i mit $1 < i < n$ für die Zopfgruppe B_n der Braid, bei dem sich nur die i-te und $i+1$-te Strähne überkreuzen, wobei die i-te Strähne unter der $i+1$-ten verläuft. Bei der Inversen dieses Generators, b_i^{-1}, verläuft die i-te Strähne über der $i+1$-ten Strähne. Abbildung 3.6 zeigt die Darstellung der Artingeneratoren einer Zopfgruppe

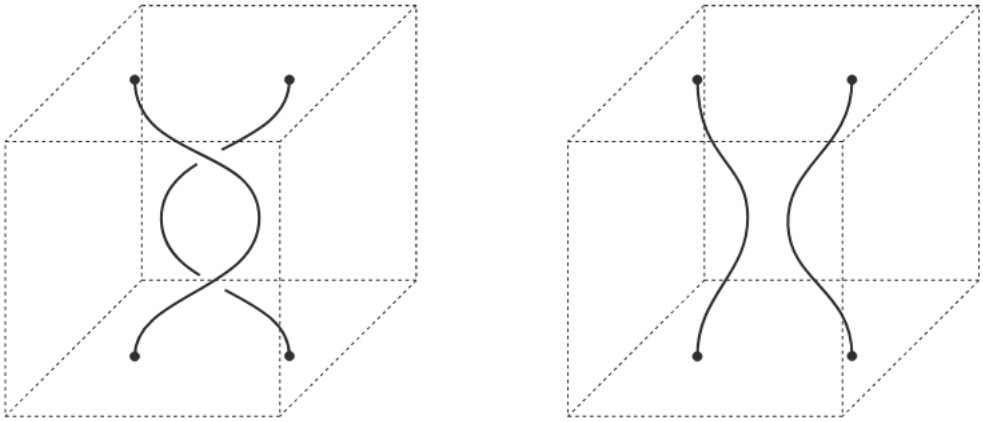


Abbildung 3.2: Zwei äquivalente 2-Braids. Quelle: [18].

Abbildung 3.3: Zweidimensionale Darstellung eines 3-Braids.

Abbildung 3.4: Rechts das Produkt aus dem linken und mittleren 3-Braid. Quelle: [18].

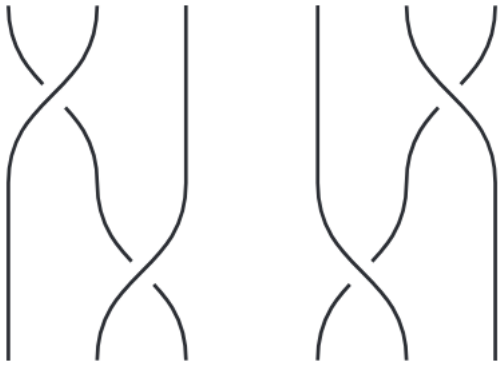


Abbildung 3.5: Rechts die Inverse des linken 3-Braids.

Abbildung 3.6: Verallgemeinerte Darstellung eines Artingenerators (links) und seiner Inversen (rechts). Quelle: [18].

B_n. Jeder Braid kann in diese Artingeneratoren der entsprechenden Zopfgruppe aufgeteilt und somit auch aus ihr Erschaffen werden. Abbildung 3.4 zeigt die Zusammensetzung des 3-Braids $b_1 b_2$ aus den zwei Artingeneratoren b_1 und b_2.

Es existieren zwei fundamentale Relationen in dieser Repräsentierung von Braids. Für die Menge an Artingeneratoren $b_1, b_2, ..., b_{n-1}$ gilt:

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1} \quad \text{für } i = 1, ..., n-2, \tag{3.1}$$

$$b_i b_j = b_j b_i \quad \text{für } |i-j| >= 2. \tag{3.2}$$

Mithilfe dieser lassen sich jegliche zwei äquivalente Braids einer Zopfgruppe ineinander ,,umwandeln" (s. wiederum Abbildung 3.2). Abbildung 3.7 zeigt die erste, Abbildung 3.8 die zweite der beiden Operationen.

Artingeneratoren sind die entscheidende Repräsentierung von Braids bei WalnutDSA. Für die Implementierung des Verfahrens lassen sie sich offensichtlich sehr einfach als ganze Zahlen speichern, sodass sich ein Braid als Liste aus Artingeneratoren darstellen lässt, aus denen er aufgebaut wird. Ein 4-Braid bestehend aus den Artingeneratoren $b_1 b_3 b_2^{-1} b_3 b_1^{-1}$ ließe sich bspw. einfach als Zahlenfolge 1 3 −2 3 −1 kodieren.

Eine weitere für WalnutDSA wichtige Abbildung in der Zopfgruppe ist die der Braid-Permutation σ. Je nach Überkreuzungen enden verschiedenen Strähnen an unterschiedlichen Enden eines Braids. Dies kann als Permutation dargestellt werden, welche die An-

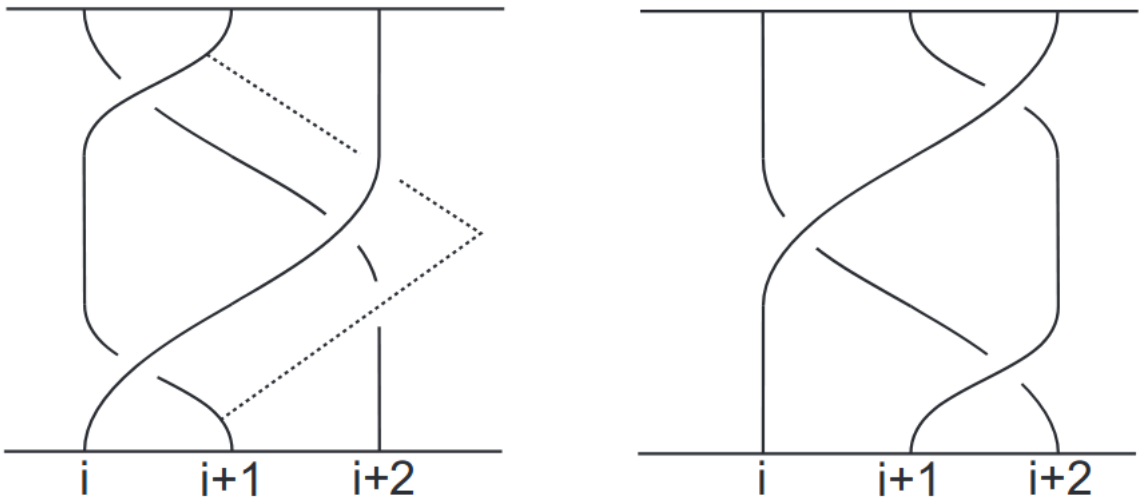


Abbildung 3.7: Darstellung der Relation 3.1. Quelle: [18].

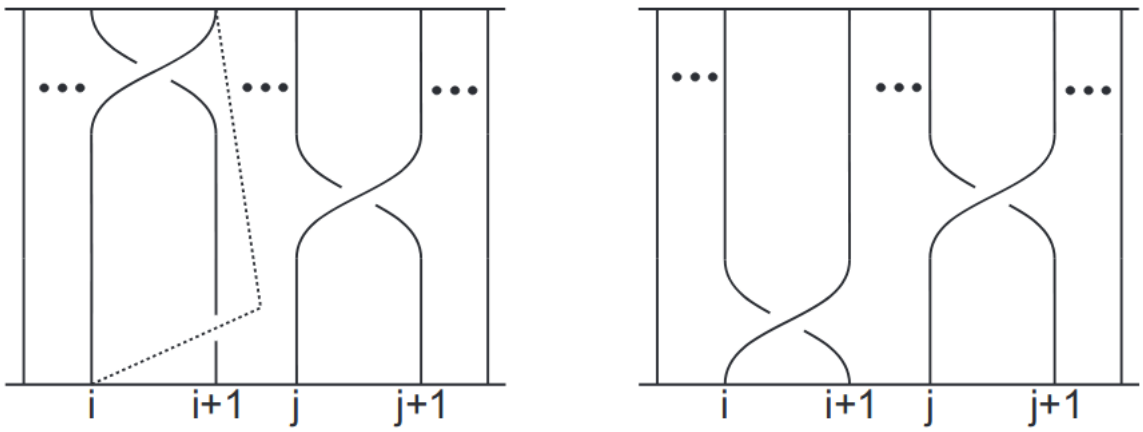


Abbildung 3.8: Darstellung der Relation 3.2. Quelle: [18].

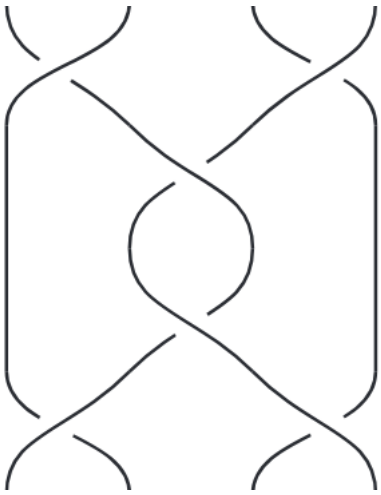


Abbildung 3.9: Darstellung eines reinen 4-Braids. Quelle: [18].

fangsposition einer Strähne auf ihre Endposition im Braid, jeweils gegeben als Index i mit $1 \leq i \leq n$, abbildet. Somit existiert für jeden Braid eine zugrundeliegende, jedoch nicht eindeutige Braid-Permutation.

Es besteht ein einfacher Zusammenhang zwischen der Permutation eines Braids und den Artingeneratoren, aus denen er zusammengesetzt ist. Sowohl für einen Artingenerator b_i als auch dessen Inverse b_i^{-1} werden die Strähnen mit den Indizes i und $i+1$ vertauscht; somit werden auch bei der Braid-Permutation diese beiden Elemente ausgetauscht. Beginnend bei der trivialen Permutation kann so die Braid-Permutation berechnet werden, indem man fortlaufend die Vertauschungen der entsprechenden Artingeneratoren auf die Permutation anwendet. Die Permutation des 3-Braids aus Abbildung 3.3 bzw. $b_1^{-1}b_2$ lautet bspw. wiefolgt:

$$\sigma(b_1^{-1}b_2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Auch die Braid-Permutation lässt sich einfach durch ein normales Array aus natürlichen Zahlen repräsentieren, wobei der Wert an der Stelle i mit $0 \leq i < n$ mit der Permutation der $i+1$-ten Strähne korrespondiert.

3.3 Untergruppe der reinen Braids

Ein Braid ist ein *reiner* Braid, wenn seine zugrundeliegende Permutation trivial ist, wenn also die Anfangs- und Endposition jeder Strähne gleich ist. Diese Braids bilden die Untergruppe der reinen Braids P_n, welche offensichtlich in der normalen Zopfgruppe enthalten ist. Abbildung 3.9 zeigt einen reinen 4-Braid.

Für diese Untergruppe existieren eigene Generatoren, welche selbst wiederum aus Artingeneratoren bestehen. Sie werden in mehreren Teilprozeduren von WalnutDSA benutzt und können zur einfachen Generierung von reinen Braids verwendet werden. Ein Generator $p_{i,j}$ ist nach folgendem Schema aufgebaut:

$$p_{i,j} = b_{j-1}b_{j-2}\dots b_{i+1}b_i^2b_{i+1}^{-1}\dots b_{j-2}^{-1}b_{j-1}^{-1} \quad \text{für } 1 \leq i < j \leq n \tag{3.3}$$

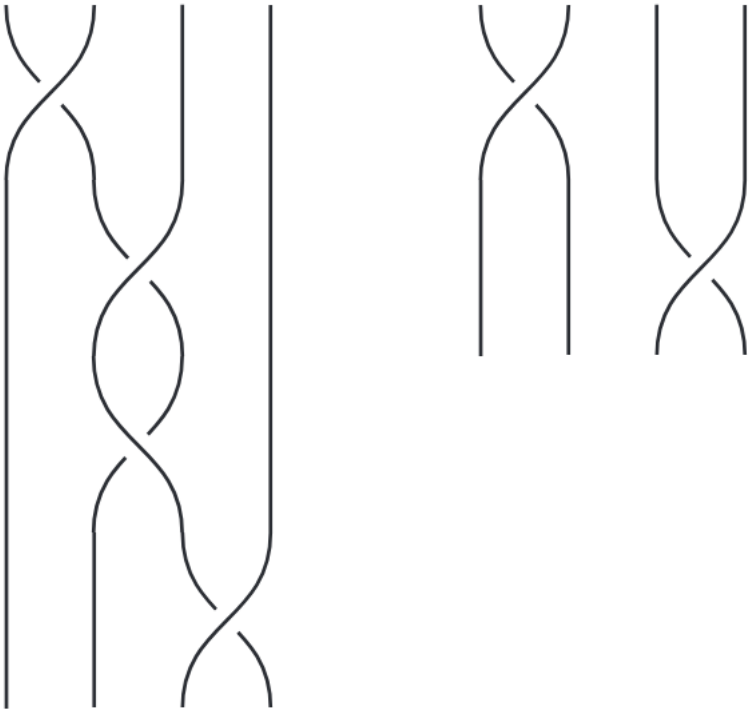


Abbildung 3.10: Rechts die frei-reduzierte Version des linken 4-Braids.

3.4 Freie Reduktion

Das Produkt eines Artingenerators und seiner Inversen ist das Einselement, sprich der triviale Braid, welcher bei der Repräsentierung durch Artingeneratoren der Nicht-Existenz eines Generators gleich kommt. Daher werden bei einer solchen Operation die beiden entsprechenden Generatoren ,,ausgelöscht". Man beachte, dass dies auch nur dem Anwenden der beiden fundamentalen Operationen 3.1 und 3.2 gleichkommt. Besteht ein Braid aus noch weiteren Artingeneratoren als den beiden Operanden der Multiplikation, so wird er dadurch verkürzt. Da der resultierende Braid immer noch äquivalent zum alten ist und die zugrundeliegende Permutation gleich bleibt, handelt es sich hierbei gewissermaßen um eine Reduktion. Diese Form der Reduktion wird *freie Reduktion* genannt. Ein Braid gilt als *frei-reduziert*, wenn in seiner Repräsentierung durch Artingeneratoren keine Vorkommnisse der Form $b_i b_i^{-1}$ bzw. $b_i^{-1} b_i$ enthalten sind. Abbildung 3.10 zeigt die freie Reduktion eines 4-Braids.

4 E-Multiplikation

——— Der folgende Text ist ein direktes Zitat von [19] ———

Die E-Multiplikation ist eine der Kernoperationen des WalnutDSAs, mit deren Hilfe der öffentliche Schlüssel berechnet und die Verifizierung der Signatur durchgeführt wird. Bevor ihre Funktionsweise näher behandelt werden kann, wird neben der Braidtheorie auch Wissen aus anderen mathematischen Bereichen benötigt.

4.1 Braids als Colored-Burau-Matrizen

Bei einer *Colored-Burau-Matrix* handelt es sich um die beste bekannte Möglichkeit, Braids linear darzustellen.[20, p. 49] Sei $GL_n\left(\mathbb{Z}\left[t^{\pm t}\right]\right)$ die Gruppe invertierbarer $n \times n$ Matrizen über Polynome eines Laurent-Rings $\mathbb{Z}\left[t^{\pm t}\right]$ $\{f(t_1), ..., f(t_N)\}$, dann beschreibt die *reduzierte Colored-Burau-Repräsentation* einen Homomorphismus $B_N \to GL_N\left(\mathbb{Z}\left[t^{\pm t}\right]\right)$, der Braids der Ordnung N auf Matrizen abbildet. Ein Artin-Generator b_i lässt sich wie folgt darstellen [20, p. 50]:

$$CB(b_i^{+1}) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & t_i & -t_i & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \qquad CB(b_i^{-1}) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & 1 & -t_{i+1}^{-1} & t_{i+1}^{-1} & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \tag{4.1}$$

Die t-Einträge befinden sich in der i-ten Zeile. Bei $i = 1$ fällt dabei der linke Eintrag weg. Der Artin-Generator b_i hat die Eigenschaft, den i-ten Strang des Braids mit den $i+1$-ten zu vertauschen. Assoziiert man mit jedem Generator eine Permutation aus der symmetrischen Gruppe mit N Elementen $\sigma_i \in S_N$ auf die N Variablen $\{t_1, ..., t_N\}$, lassen sich Braids mit mehreren Generatoren durch die Multiplikation der Tupel $(CB\left(b_i\right), \sigma_i)$ berechnen.[21, p.4]

$$\left(\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & t_i & -t_i & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \sigma_i\right) \quad \circ \quad \left(\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & t_j & -t_j & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \sigma_j\right)$$

$$= \left(\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & t_i & -t_i & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} * \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & t_{\sigma_i(j)} & -t_{\sigma_i(j)} & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \sigma_i \sigma_j \right) \tag{4.2}$$

4.2 Arithmetik in Binärkörpern

Mit wachsender Länge des Braids wachsen auch die Laurent-Polynome der CB-Matrizen. Die Matrixeinträge und die Rechenoperationen werden schnell sehr komplex. Für den Einsatz auf ressourcenarmen Systemen, wird daher eine algebraische Struktur benötigt, die die CB-Einträge für effiziente Rechenoperationen möglichst klein hält.

Endliche Körper, oder auch *Galois-Körper* genannt, beinhalten endlich viele, positive ganze Zahlen und erfüllen die Anforderungen an mathematische Körper bzgl. Addition und Multiplikation. Die Anzahl der Elemente q (Ordnung) ist hierbei eine ganzzahlige Potenz einer Primzahl p. In der Informatik sind vor allem *Galois-Körper* der Charakteristik $p = 2$ interessant, da ein *Galois-Körper* $GF(2^m)$ alle Binärzahlen mit m Bits beinhaltet. Diese werden auch Binärkörper genannt. Die Elemente eines Binärkörpers lassen sich als Polynome mit den Koeffizienten 0 und 1 und einem Grad $g < m$ darstellen.[22, pp. 25-26]

4.2.1 Addition im Binärkörper

Die Addition im Binärkörper ist die Addition der Polynome mit anschließenden *modulo* 2 auf die Koeffizienten und gleicht damit einer bitweisen Addition ohne Übertrag bzw. einer XOR-Operation.

Beispiel im $GF(2^4) : 7 + 9 = 0111 \oplus 1001 = 1110 = 14$

Jedes $a \in GF(2^m)$ besitzt ein Inverses bzgl. der Addition $(-a)$, sodass $a + (-a) = 0$. Da es sich bei der Addition um die XOR-Operation handelt, ist das Inverse von a gleich a selbst. [22, 26-27]

4.2.2 Multiplikation im Binärkörper

Die Multiplikation im Binärkörper ist definiert durch $a * b \, modulo \, x$ mit dem irreduziblen Polynom x, das sich nicht aus einem Produkt aus Polynomen eines geringeren Grades als m faktorisieren lässt. [22, p. 28]

Beispiel im $GF(2^8) : 50{*}40 = (z^5{+}z^4{+}z){*}(z^5{+}z^3) \, mod \, (z^8{+}z^4{+}z^3{+}z{+}1) = z^7{+}z^4{+}1 = 145$

Analog zur Addition besitzt auch jedes Element $a \in GF(2^m)$ ein Inverses bzgl. der Multiplikation a^{-1}, sodass $a * a^{-1} = 1$.

Die Subtraktion erfolgt über eine Addition mit dem Inversen bzgl. der Addition und die Division über die Multiplikation mit dem Inversen bzgl. der Multiplikation:[22, pp. 25-26]

$$a/b = a * b^{-1} \qquad a - b = a + (-b)$$

4.3 E-Multiplikationsschritt

Die E-Multiplikation nimmt als Eingabe ein Tupel (M, σ) mit $M = CB(\beta)$ und $\beta \in B_N$. Die Operation erfolgt schrittweise für jeden Generator in β. Das Ergebnis ist wieder ein Tupel (M, σ)[21, p. 6].

$$(M, \sigma_0) \star (\beta, \sigma_\beta) = \left(\left((M, \sigma_0) \star \left(b_{i_1}^{\in_1}, \sigma_{\beta_1}\right)\right) \star \left(b_{i_2}^{\in_2}, \sigma_{\beta_2}\right)\right) \star \cdots \star \left(b_{i_k}^{\in_k}, \sigma_{\beta_k}\right) \tag{4.3}$$

Um das Bilden komplexer Einträge zu vermeiden werden die Variablen $t_1 ... t_N$ durch positive Elemente eines Binärfelds der Ordnung q ersetzt, die sogenannten „$T - Werte$“ . Da die Arithmetik nun im Binärkörper stattfindet, ist das negative Vorzeichen der Colored-Burau-Darstellung der Artin-Generatoren vernachlässigbar. Bei negativen Generatoren ist es notwendig, das Inverse bezüglich der Multiplikation des dazugehörigen T-Value zu bestimmen.

$$CB(b_i^{+1}) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & t_i & t_i & 1 & & \\ & & & \ddots & & \\ & & & & & 1 \end{pmatrix} \qquad CB(b_i^{-1}) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & 1 & t_{i+1}^{-1} & t_{i+1}^{-1} & & \\ & & & \ddots & & \\ & & & & & 1 \end{pmatrix} \tag{4.4}$$

Die iterative Multiplikation entspricht der CB-Multiplikation 4.2, bis auf den Unterschied dass die Addition und die Multiplikation durch ihre Pendants aus der Galois-Arithmetik ersetzt werden. D.h. der Eintrag z in Zeile i, Spalte j wird mit dem irreduzibles Polynom zu $GF(2^m)$ x berechnet durch:

```
for i ← 1 to N do
    for j ← 0 to N do
        result ← 0; for i ← 0 to N do
            result ← result ⊕ (a[i][k] * b[k][j] modulo x);
        end
    end
end
```

Der Ressourcenaufwand der E-Multiplikation wächst aufgrund der iterativen Abarbeitung aller Artin-Generatoren linear mit der Braidlänge. Der benötigte Speicherplatz der Matrix ist lediglich abhängig von N und q. Als zentraler Bestandteil der Verifizierung ist

die E-Multiplikation daher ein geeignetes Mittel für die Kryptographie auf ressourcenarmen Systemen.

4.4 Beispiel einer E-Multiplikation

gegeben: $N = 4$; $\beta_1 = \epsilon$; $\beta_2 = \{3, -1\}$; T-Werte = $\{14,\ 1,\ 8,\ 1\}$

$$\left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, (1,2,3,4)\right)\right) \star \left(\{3,-1\}, \sigma_{\{3,-1\}}\right)$$

$$= \left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, (1,2,3,4)\right)\right) \star (\{3\}, \sigma_3) \star (\{-1\}, \sigma_{-1})$$

$$= \left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} *^{(1,2,3,4)} \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&t_3&t_3&1\\0&0&0&1\end{pmatrix}, \sigma_3\right)\right) \star (\{-1\}, \sigma_{-1})$$

$$= \left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} * \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&t_3&-t_3&1\\0&0&0&1\end{pmatrix}, \sigma_3\right)\right) \star (\{-1\}, \sigma_{-1})$$

$$= \left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&t_3&t_3&1\\0&0&0&1\end{pmatrix}, (1,2,4,3)\right)\right) \star (\{-1\}, \sigma_{-1})$$

$$= \left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&t_3&t_3&1\\0&0&0&1\end{pmatrix} *^{(1,2,4,3)} \begin{pmatrix}t_2^{-1}&t_2^{-1}&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \sigma_3 * \sigma_{-1}\right)\right)$$

$$= \left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&t_3&t_3&1\\0&0&0&1\end{pmatrix} * \begin{pmatrix}t_2^{-1}&t_2^{-1}&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, (2,1,4,3)\right)\right)$$

$$= \left(\left(\begin{pmatrix}t_2^{-1}&t_2^{-1}&0&0\\0&1&0&0\\0&t_3&t_3&0\\0&0&0&1\end{pmatrix}, (2,1,4,3)\right)\right) = \left(\left(\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&8&8&0\\0&0&0&1\end{pmatrix}, (2,1,4,3)\right)\right)$$

——— Ende des Zitats. ———

5 Stand der Forschung

Die beschränkte Rechenleistung und Speicherkapazität eingebetteter Systeme stellt neue Herausforderungen an digitale Signaturverfahren. Zudem ist durch die fortschreitende Forschung an Quantencomputern die Resistenz gegen quantenbasierte Angriffe ein neues Ziel in der Kryptographie. Es existieren neben WalnutDSA weitere Verfahren, die diese Aspekte abdecken wollen. Auf einige dieser Kryptosysteme soll nun eingegangen werden.

5.1 Elliptische-Kurven-Kryptographie

Auf elliptischen Kurven beruhende Kryptosysteme wie ECDSA übertragen das schwere Problem des diskreten Logarithmus auf die Gruppe der Punkte einer elliptischen Kurve. Dadurch kommen sie mit weitaus kleineren Schlüsseln zurecht, benötigen jedoch bei der Verifizierung von Signaturen mehr Rechenzeit. So korrespondiert z.B. ein 224-Bit ECDSA-Schlüssel bzgl. der Sicherheit mit einem 2048-Bit RSA-Schlüssel [23, 25]. Die tatsächliche Leistung des Algorithmus hängt von der gewählten elliptischen Kurve ab. Bei der Signaturgenerierung ist das Verfahren mit traditionellem RSA weitestgehend gleichauf, wobei die Verifizierung von RSA unabhängig von der Schlüssellänge um mehrere Größenordnungen schneller ist [24].

Verfahren auf elliptischen Kurven sind genau wie RSA auch anfällig für Angriffe durch Quantencomputer. Der *Shor-Algorithmus* [25] bietet eine Möglichkeit, die üblicherweise schweren Probleme der Primfaktorzerlegung und des diskreten Logarithmus effizient mit einem Quantencomputer zu lösen. Daher sind besagte kryptographische Systeme nicht quantenresistent.

5.2 Gitter-basierte und RLWE-Kryptographie

Gitter-basierte Kryptosysteme ziehen ihre Sicherheit aus schweren Berechnungsproblemen in mathematischen Gittern. Bei Gittern handelt es sich um regelmäßigen Mengen aus Vektoren des euklidischen Vektorraums. Eine typische Einwegfunktion dieser Kryptosysteme ist das *Shortest Vector Problem*, welches den kürzesten Vektor in einem Gitter sucht. Diese Verfahren sind vielversprechende Lösungen zur Post-Quanten-Kryptographie, da sie nicht auf den Problemen der Primfaktorzerlegung und des diskreten Logarithmus beruhen, sondern einen davon unabhängigen, neuen Ansatz verfolgen. Effiziente Lösungen, die die Sicherheit dieser Verfahren schwächen würden, wurden bisher noch nicht gefunden. Zudem bietet die Familie der Gitter-basierten Verschlüsselungssysteme theoretisch sowohl kleine Schlüssellängen als auch eine effiziente Verarbeitung [26].

Die *Ring learning with errors signature (RLWE-SIG)* ist ein Gitter-basiertes digitales Signaturverfahren. Es existiert eine Implementierung für FPGAs, die effizienter als RSA arbeitet, jedoch weitaus größere Schlüssellängen benötigt. In der Arbeit der Autoren werden ca. 12000 Bits für den öffentlichen und 2000 Bits für den privaten Schlüssel verwendet, um vergleichbare Sicherheit zu einem 1024-Bit RSA-Schlüssel zu erzeugen. Wie stark die

Schlüssellängen mit steigendem Sicherheitslevel wachsen, wurde nicht untersucht. Das Verfahren arbeitet jedoch um den Faktor $1,5$ schneller als eine vergleichbare Implementierung von RSA [27].

5.3 Weitere Braid-basierte Kryptosysteme

Neben WalnutDSA gibt es weitere digitale Signaturverfahren, die auf Zopfgruppen basieren. Die gängige Einwegfunktion dieser Kryptosysteme ist das Konjugationsproblem in einer Zopfgruppe. Hierfür ist bislang keine effiziente Lösung – weder für Quantencomputer noch für das klassische Rechenmodell – gefunden worden. Zudem werden durch die Repräsentierung der Signaturen durch Braids gängige mathematische Angriffsvektoren ausgeschalten [28].

Das *Braid Signature Scheme (BSS)* ist ein anderes digitales Signaturverfahren auf Basis der Zopfgruppen. Es existiert eine Implementierung der Autoren, bei der Schlüssellängen von 370–591 Bit verwedet wurden, um angemessene Sicherheit zu erreichen. Die Längenangaben sind jedoch grobe Schätzungen und es sind keine ausreichenden Daten vorhanden, um ein klares Bild über die Leistungsanforderungen des Algorithmus zu erhalten [29].

6 WalnutDSA - Bestandteile

Es sollen nun die einzelnen Teilprozeduren von WalnutDSA dargestellt und auf relevante Aspekte bei der generischen Implementierung eingegangen werden. Zum Zeitpunkt der Veröffentlichung der vorliegenden Arbeit sind aufbauend auf die ursprüngliche Fassung zwei aktualisierte Versionen der wissenschaftlichen Arbeit von WalnutDSA erschienen. Die im Folgenden behandelten Definitionen des Verfahren richten sich nach der ersten Aktualisierung vom 18. September 2017. Es soll hierbei zunächst auf die öffentlichen Informationen und Sicherheitsparameter sowie die Schlüsselgenerierung eingegangen werden. Anschließend wird die Kodierungsfunktion für den Nachrichtenhashwert erläutert und die Generierung der sog. Cloaking-Elemente dargestellt. Abschließend soll die Bildung und Verifizierung von Signaturen erklärt und auf zwei unterschiedliche Umformungsfunktionen eingegangen werden.

6.1 Öffentliche Informationen und Sicherheitslevel

Bei der Verwendung eines digitalen Signaturverfahrens besitzt jeder Kommunikationspartner ein Schlüsselpaar aus einem privatem und einem öffentlichen Schlüssel. Der private Schlüssel eines Teilnehmers ist nur ihm selbst bekannt und dient zur Generierung von Signaturen. Der öffentliche Schlüssel wird an andere Teilnehmer weitergegeben und kann folglich dazu verwendet werden, die erstellten Signaturen zu verifizieren.

Die Autoren von WalnutDSA definieren eine Reihe an ,,öffentlichen systemweiten Parametern" [5, 6]. Es ist nicht ganz klar, welchen Zweck die Gruppierung dieser Parameter genau erfüllen sollen. An selber Stelle wird definiert, dass diese von einer ,,zentralen Autorität" generiert werden [5, 6]. Dadurch kann angenommen werden, dass es sich hierbei um diejenigen Informationen handelt, die zwischen den Kommunikationspartnern ausgetauscht werden müssen, damit die Implementierungen miteinander kompatibel sind und folglich die Verifizierung von fremden Signaturen möglich ist. Es bleibt jedoch fraglich, inwiefern diese Parameter ,,systemweit" definiert sein sollen. Man kann sich vorstellen, verschiedene Parameter für unterschiedliche Schlüsselpaare auf einem System zu verwenden (s. Implementierung auf Raspberry Pi). Möglicherweise ist als ,,System" das Kryptosystem selbst gemeint. Im Rahmen dieser Arbeit wurde angenommen, dass die Parameter dem gerade beschriebenen Zweck dienen, zwei kommunizierende Implementierungen miteinander zu synchronisieren. Auf die Parameter soll nun eingegangen werden.

Die öffentlichen Informationen bestehen aus folgenden Bestandteilen:

n Die Anzahl an Strähnen in der verwendeten Zopfgruppe B_n.

q Eine Zweierpotenz für die Ordnung des bei der E-Multiplikation verwendeten endlichen Körpers $GF(q)$.

T-Werte n umkehrbare, geordnete Elemente aus dem endlichen Körper $GF(q)$, wobei zumindest zwei verschiedene Elemente a und b mit $1 < a < b < n$ den Wert 1 haben

müssen.

Kodierungsgeneratoren Vier verschiedene Generatoren $p_{i,j}$ der Gruppe der reinen Braids (als Untergruppe zur Zopfgruppe B_n).

Die Autoren von WalnutDSA erwähnen die zur Nachrichtenkodierung (s. Kapitel 6.3) verwendeten vier reinen Braidgeneratoren nicht. Sie müssen jedoch unbedingt bei den Kommunikationspartnern übereinstimmen, um die Signaturverifizierung möglich zu machen.

Zudem enthalten die öffentlichen Informationen nach der ursprünglichen Definition noch zwei weitere Parameter. Zum einen sind dies die Werte a und b, die die Indizes der beiden T-Werte mit dem Wert 1 darstellen sollen. In dieser Arbeit wurde auf diese beiden Werte verzichtet, da man sie für die Signaturverifizierung nicht benötigt und für die Signaturgenerierung einfach aus den T-Werten selbst auslesen kann (s. Kapitel 6.4). Zum anderen ist es eine Umschreibungsfunktion, die am Ende der Generierung auf die Signatur angewendet wird. Dies scheint auch hinfällig zu sein, da diese Funktion die Signatur zwar in ihrer Gestalt abwandelt, jedoch den zugrundeliegenden Braid nicht verändert und folglich bei der Verifizierung nicht benötigt wird. Somit wurde der Parameter in dieser Arbeit auch aus den öffentlichen Informationen ausgelassen.

Um die ausreichende Sicherheit von WalnutDSA gegen Bruteforce-Angriffe sicherzustellen, benötigen sowohl der private Schlüssel als auch die sog. Cloaking-Elemente (welche auch als Braids repräsentiert werden, s. Kapitel 6.4) eine Mindestlänge in Artingeneratoren. Wie bei gängigen Verschlüsselungsverfahren kann die Sicherheit eines Schlüsselpaars oder einer Signatur durch ein *Sicherheitslevel* SL in Bits angegeben werden. Für einen endlichen Körper GF ist dieses über die kleinste Anzahl an Operationen definiert, die zum Finden eines Geheimnisses im Körper benötigt werden [5, 13]. Ein Sicherheitslevel von 128 Bit korrespondiert also z.B. mit der Sicherheit eines symmetrischen AES-128 Verfahrens. Konkret dient es zur Bestimmung von besagten Mindestlängen des privaten Schlüssels und der Cloaking-Elemente.

Für die Cloaking-Elemente wird mithilfe des Sicherheitslevels speziell die Mindestlänge L des beinhalteten Produkts an Generatoren der Untergruppe der reinen Braids (s. Kapitel 6.4) bestimmt. Sie kann nach folgender Formel berechnet werden [5, 15]:

$$L \;=\; \lceil SL \div \big(3 \log_2 \big(n\,(n-1)\,\big)\big) \rceil \tag{6.1}$$

Für die Mindestlänge l des privaten Schlüssels existiert eine nicht-lineare Gleichung, welche mittels des Newton-Verfahrens gelöst werden kann [5, 14]:

$$l + (n-2) log_2(l) \;=\; SL + log_2\big((n-1)!\big) \tag{6.2}$$

Es sei gesagt, dass die Cloaking-Elemente nur bei der Signaturgenerierung verwendet werden. Es ist also prinzipiell möglich, unterschiedliche Sicherheitslevel für die Erstellung eines Schlüsselpaars und die Generierung einer dazu passenden Signatur zu verwenden. Ob dies sinnvoll ist oder lieber vermieden werden sollte, geht nicht aus der Arbeit über WalnutDSA hervor. Zudem fehlen Informationen der Autoren darüber, welches Sicherheitslevel ein Minimum für ausreichende Sicherheit des digitalen Signaturverfahrens darstellt.

6.2 Schlüsselgenerierung

Zur Generierung eines Schlüsselpaars benötigt man die Parameter n, q und die T-Werte.

Der private Schlüssel ist ein zufälliger, frei-reduzierter Braid aus der Zopfgruppe B_n mit der entsprechenden Mindestlänge l [5, 6]. Es bietet sich offensichtlich an, schon während der Schlüsselgenerierung sicherzustellen, dass keine frei reduzierbaren Vorkommnisse bb^{-1} bzw. $b^{-1}b$ im Braid enthalten sind.

Ein öffentlicher Schlüssel ist ein Paar aus einer $n \times n$ Matrix sowie einer n-stelligen Permutation, welche der zugrundeliegenden Permutation des privaten Schlüssels entspricht. Um den zugehörigen öffentlichen zu einem privaten Schlüssel zu generieren, wendet man die E-Multiplikation an [5, 6]:

$$PubKey = (Id_n, Id_{S_n}) \star PrivKey \tag{6.3}$$

Hierbei stellt Id_n die $n \times n$ Identitäsmatrix und Id_{S_n} die n-stellige Identitäspermutation dar.

Wie in Kapitel 6.1 angedeutet, müssen bei der Signaturverifizierung die besagten drei Parameter n, q und die T-Werte desjenigen privaten Schlüssels angewendet werden, der zur Signierung verwendet wurde. Daher sollten die Parameter an das Schlüsselpaar gekoppelt und bei dessen Speicherung miteinbezogen werden, um die korrekten Werte wiederherstellen zu können.

6.3 Kodierung des Nachrichtenhashwerts

Bei der Verwendung von digitalen Signaturalgorithmen muss der Hashwert einer Nachricht signiert werden, um neben der Authentizität des Senders auch die Integrität der Nachricht sicherzustellen. Bei WalnutDSA ist die Signatur selbst ein zusammengesetzter Braid, in den der Nachrichtenhash eingebettet wird. Daher muss der Hashwert in einen Braid konvertiert werden, wozu eine eigene Kodierungsfunktion verwendet wird. Um die Verifizierung der Signatur nicht zu vereiteln, muss der aus dem Hashwert kodierte Braid eine triviale zugehörige Permutation besitzen. Hierfür verwendet man die Untergruppe der reinen Braids. Zusätzlich muss der Braid frei reduziert sein, damit eine einzigartige Zuordnung von einem Hashwert zu seinem kodierten Braid gewährleistet ist [5, 7].

Zur Kodierung wählt man vier beliebige, verschiedene Generatoren der Untergruppe der reinen Braids (s. Kapitel 3.3). Diese benötigen eine feste Reihenfolge untereinander, sodass jeder Generator eindeutig über einen Index angesprochen werden kann. Man betrachtet den Hashwert dann als Bitfolge und iteriert über diese in 4-Bit-Inkrementen. Die zwei niedrigigwertigen Bits bestimmen, welcher der vier Braidgeneratoren für diesen Teil des Hashwerts verwendet wird. Die zwei höherwertigen Bits legen einen Exponenten im Intervall 1–4 fest, zu dem der Generator potenziert wird [5, 7]. Bei der Potenzierung handelt es sich um die übliche Multiplikation in der Braidgruppe, also einer Hintereinanderreihung des entsprechenden Generators.

Bei Verwendung der reinen Braidgeneratoren $p_{1,4}, p_{3,8}, p_{5,6}$ und $p_{7,8}$ in der Zopfgruppe B_8 würde die 4-Bitfolge 1001 also den zweiten Generator zur dritten Potenz bestimmen und somit wiefolgt kodiert werden:

7, 6, 5, 4, 3, 3, -4, -5, -6, -7, 7, 6, 5, 4, 3, 3, -4, -5, -6, -7, 7, 6, 5, 4, 3, 3, -4, -5, -6, -7

Diesen Schritt wiederholt man in 4-Bit-Schritten für den gesamten Hashwert und reiht dabei die einzelnen Teile aneinander. Die theoretische maximale Länge des resultierenden Braids lässt sich also — ohne dabei auf Einschränkungen oder Muster im Aufbau des Hashwerts einzugehen — einfach nach folgender Formel bestimmen:

$$length_{max} \;=\; 2 \cdot bytes_{hash} \cdot 4 \cdot (j_{max} - i_{min}) \cdot 2 \tag{6.4}$$

Hierbei steht $bytes_{hash}$ für die Größe des Hashwerts in Bytes sowie i_{min} und j_{max} für die Werte i und j des längsten verwendeten reinen Braidgenerators $p_{i,j}$ (mit der größten Differenz $j - i$).

Wie angesprochen, muss der engültige Braid jedoch frei-reduziert sein. Die frei-reduzierte Version des beispielhaften Braids lautet wiefolgt:

7, 6, 5, 4, 3, 3, 3, 3, 3, 3, -4, -5, -6, -7

Als einfache Möglichkeit zur Reduzierung ergibt sich, nach der Kodierung des Hashwerts den Braid zu durchlaufen und sämtliche frei-reduzierbare Vorkommnisse an Artingeneratoren zu entfernen, bis der Braid im gewünschten Zustand ist. Dies benötigt jedoch eine zusätzliche Iteration über den gesamten Braid. Zudem müssen die resultierenden Lücken des Braids wieder beseitigt werden, oder der gesamte Braid als frei-reduzierte Version neu gespeichert werden. Daher bietet es sich an, die freie Reduktion während der Kodierung selbst durchzuführen. Bei der Potenzierung kann einfach der quadratische Mittelteil des reinen Braidgenerators je nach Exponent entsprechend häufig wiederholt werden.

Die theoretische maximale Länge des Braids verringert sich hierbei, da die freie Reduktion zumindest die Länge der potenzierten Generatoren verkleinert. Sie lässt sich nun wiefolgt bestimmen:

$$length_{max} \;=\; 2 \cdot bytes_{hash} \cdot \big((j_{max} - i_{min} - 1) \cdot 2 + 8 \big) \tag{6.5}$$

Um den Braid noch weiter zu verkleinern, kann man sich bei der Wahl von j einschränken. Wählt man einen festen Wert j für alle vier reinen Braidgeneratoren $p_{i,j}$, so ergeben sich weitere frei-reduzierbare Sektionen an den Anfängen und Enden der kodierten 4-Bit-Inkremente. Man kann vor dem Aufbau der hinteren Hälfte eines Inkrements im Hashwert vorausschauen und dabei nur die Artingeneratoren anhängen, welche nicht durch den kommenden reinen Braidgenerator frei reduziert werden würden.

Folgendes Beispiel zeigt diese Situation bei Aufeinanderfolgen der beiden reinen Braidgeneratoren $p_{3,8}$ und $p_{5,8}$, wobei die frei-reduzierbaren Artingeneratoren unterstrichen wurden:

7 6 5 4 3 3 -4 <u>-5 -6 -7 7 6 5</u> 5 -6 -7

Dies verkleinert wiederum die theoretische maximale Länge des kodierten Braids. Im ungünstigsten Fall folgen jeweils vier reine Braidgeneratoren $p_{i_{min},j}$ und $p_{j-1,j}$ aufeinander. Dadurch wird durch die freie Reduktion jedes zweite Inkrement auf 6 Artingeneratoren reduziert. Die Formel für die Maximallänge verändert sich so zum Folgenden:

$$length_{max} \;=\; bytes_{hash} \cdot \big((j - i_{min} - 1) \cdot 2 + 8 + 6 \big) \tag{6.6}$$

Für $j = n$ entspricht dies genau dem Vorgehen der Autoren von WalnutDSA. Das Kriterium für die Wahl der reinen Braidgeneratoren ist, dass sie eine freie Untergruppe zur Zopfgruppe B_n bilden, in der ein frei-reduzierter Braid niemals das neutrale Element ist [5, 7]. Es darf also offensichtlich kein Generator das leere Braidwort sein. Dies lässt jedoch noch die Möglichkeit offen, für die reinen Braidgeneratoren $p_{i,j}$ nur solche zu wählen, bei denen $i = j - 1$ gilt. Dadurch würde der kodierte Braid auf eine maximale Länge von $16 \cdot bytes_{hash}$ reduziert werden.

Bei den Implementierungen dieser Arbeit wurde auf diese Möglichkeit verzichtet. Zum einen soll die Kompatibilität mit potentiellen anderen Implementierungen gewährleistet werden, die sich streng an die Ausarbeitung der Autoren halten. Zum anderen ist ohne genauere Analyse nicht offensichtlich, ob diese Optimierung nicht die Sicherheitseigenschaften der Kodierung gefähren würde.

Die Sicherheit des Kodierungsverfahrens an sich ist gegeben, solange als Eingabe nur kryptographische Hashwerte verwendet werden. Die Kodierungsfunktion E ist homormorph; sie erhält also die Zusammensetzung der einzelnen Inkremente, sodass auch für zwei Nachrichten m_1 und m_2 gilt $E(m_1 m_2) = E(m_1)E(m_2)$. Würde man die Nachricht selbst in einen Braid kodieren, so könnte man durch besagte Eigenschaft einfach Rückschlüsse auf die Nachricht ziehen [5, 7].

Die Autoren von WalnutDSA spezifizieren kein Verfahren zur generischen asymmetrischen Ver- und Entschlüsselung von Daten. Würde man ein solches definieren wollen, so müsste man zumindest sicherstellen, dass der verschlüsselte Braid einer Umschreibungsfunktion (s. Kapitel 8.9) unterzogen wird. Ob die dadurch erreichte Verschleierung der Struktur des Braids ausreichen würde, um die Sicherheit des Verfahrens zu garantieren, ist uns nicht bekannt und bedarf wohl weiterer Diskussion.

6.4 Cloaking-Elemente

——— Der folgende Text ist ein direktes Zitat von [19] ———

Um die finale Signatur zu erstellen, werden mehrere Teilbraids zu einem ganzen konkateniert. Mit der Generierung des privaten Schlüssels und der Kodierung des Nachrichten-Hashs verfügt der Algorithmus bisher über zwei Braids, die richtig zusammengesetzt die Verifizierung mit dem öffentlichen Schlüssel bestehen würden. Durch die Anwendung einer Umformungsfunktion bliebe das Ergebnis der Verifizierung identisch und der private Schlüssel wäre trotz der vorherigen einfachen Konkatenation nicht direkt ersichtlich. Da jedoch sowohl der Hash, als auch die Kodierungsgeneratoren und damit auch die Länge des kodierten Hashs öffentlich bekannt sind, wäre es möglich, durch einen Algorithmus zur Lösung des *Conjugacy Search Problems* den privaten Schlüssel von einem auf diese Art und Weise erzeugten Braid effizient zu extrahieren.[20] Um die Positionen der Bestandteile der Signatur zu verschleiern

werden sogenannte Cloaking-Elemente generiert. Dabei handelt es sich um Braids zufälliger Länge, die das Ergebnis der E-Multiplikation nicht beeinflussen und dennoch bei der freien Reduktion nicht verschwinden.

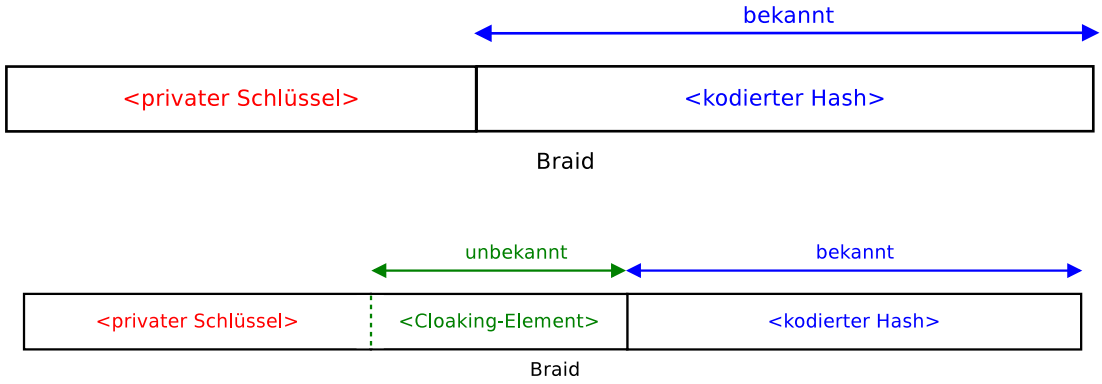


Abbildung 6.1: Konkatenation der Teilbraids mit und ohne Cloaking-Element

Für die Generierung der Cloaking-Elemente wird die Permutation σ des Schlüssels, bzw. des zu „verhüllenden“ Braids, und die Variablen a und b benötigt. Man wählt ein zufälliges $i \in \{1, \ldots, N\}$ und erzeugt einen Braid, der $\sigma^{-1}(a)$ an die Stelle i und $\sigma^{-1}(b)$ an die Stelle $i+1$ verschiebt. [30, p. 5]

Den nächsten Teilbraid bilden zufällig generierte reine Braids, die mithilfe folgender Generatoren für reine Braids und zufällig gewählten l und r erzeugt werden:[30, p. 7]

$$g_{l,r} = b_{r-1}b_{r-2}\ldots b_{l+1} \cdot b_l^2 \cdot b_{l+1}^{-1}\ldots b_{r-2}^{-1}b_{r-1}^{-1}, \qquad 1 \leq l < r \leq N. \tag{6.7}$$

Es werden solange reine Braids aneinander gehängt, bis die vordefinierte Mindestlänge L erreicht wurde.

Sei ω der bisherige Braid.
Das fertige Cloaking-Element ist definiert durch: $v = \omega b_i^2 \omega^{-1}$, wobei es sich bei b_i^2 um ein doppeltes Vorkommen des Artingenerators i und bei ω^{-1} um das Braid-Inverse von ω handelt.[30, p. 5]

Beispiel der Generierung eines Cloaking-Elements:

gegeben: $a = 4$; $b = 5$; $i = 5$; T-Werte = {22, 56, 76, 1, 1, 128, 15, 33}; $L = 10$
und Braid β: {-3 6 4 -1 2}

ω Teil 1:
Permutation von β: (2 4 1 5 3 7 6 8);
$\sigma^{-1}(a) = 2$;
$\sigma^{-1}(b) = 4$

→ Braid, der Position 2 nach 5 und 4 nach 6 verschiebt: 4 5 2 3 4

ω Teil 2:
Braid mind. der Länge $L = 10$, bestehend aus zufällig gewählten reinen Braids: $g_{3,5}\ g_{4,7}\ g_{3,7}$
= 4 3 3 -4 6 5 4 4 4 3 3 -4 -5 -6 (frei reduziert)

Cloaking-Element $v = \omega b_i^2 \omega^{-1}$
= 4 5 2 3 4 4 3 3 -4 6 5 4 4 4 3 3 -4 -5 -6 5 5 6 5 4 -3 -3 -4 -4 -4 -5 -6 4 -3 -3 -4 -4 -3 -2 -5 -4

E-Multiplikation von β und v:

Braid β in der Colored-Burau-Form: $(CB(\beta), \sigma_\beta) =$

$$\left(\begin{pmatrix} 81 & 163 & 242 & 0 & 0 & 0 & 0 & 0 \\ 22 & 22 & 1 & 0 & 0 & 0 & 0 & 0 \\ 22 & 22 & 76 & 76 & 1 & 0 & 0 & 0 \\ 0 & 0 & 76 & 76 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 128 & 128 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, (2,4,1,5,3,7,6,8) \right)$$

e-multipliziert mit dem Cloaking-Element v: $(CB(\beta), \sigma_\beta) \star (v, \sigma_v) =$

$$\left(\begin{pmatrix} 81 & 163 & 242 & 0 & 0 & 0 & 0 & 0 \\ 22 & 22 & 1 & 0 & 0 & 0 & 0 & 0 \\ 22 & 22 & 76 & 76 & 1 & 0 & 0 & 0 \\ 0 & 0 & 76 & 76 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 128 & 128 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, (2,4,1,5,3,7,6,8) \right) = (CB(\beta), \sigma_\beta)$$

Weder die Colored-Burau-Matrix noch die Permutation von β ändern sich durch die E-Multiplikation mit dem Cloaking-Element.

——— Ende des Zitats. ———

6.5 Signaturbildung

——— Der folgende Text ist ein direktes Zitat von [7] ———

Die Generierung von Signatur für einen Hashwert H(m) von der zu signierenden Nachricht m läuft in folgende Schritten:
1. Generiere Cloaking-Elemente v, v_1 und v_2, wobei v die Colored-Burau-Representation

von leeren Braid versteckt(D.h. $(Id_N, Id_{S_N}) \star v = (Id_N, Id_{S_N})$ mit der Identitätsmatrix Id_N und die triviale Permutation Id_{S_N}) und v_1, v_2 die Colored-Burau-Representation von den privaten Schlüssel versteckt.
2. Codiere den Hashwert H(m) in E(H(m)). 3. Konkateniere Elemente, sodass $(v_2 v_1^{-1} Priv(S)^{-1} vE(H(m)) Priv(S) v_1)$ gebildet wird. Das Ergebnis von diesem Schritt ist nicht sicher, da der privaten Schlüssel noch unverändert steht.
4. Forme das Ergebnis vom Schritt 3 um.
Hier wird die Signatur mit Hilfe einer oder mehre Umformungsalgorithmus verändert, um das beim dritten Schritt erwähnte Problem zu lösen. Ein Umformungsalgorithmus soll in der Lage sein, die konkatenierte Elemente z.B. durch Normalization von Braid zu mischen und dadurch genug Diffusion zu erzeugen. Als den Umformungsalgorithmen kann man BKL-Normalform verwendet.[5, S. 8]

6.6 Verifizierung

Die Verification von Signatur haben folgende Schritte:
1. Codiere die Nachricht in E(H(m)). 2. Definiere Colored-Burau-Representation von E(H(m)) als Pub(E(H(m)). 3. E-Muliplizieren den öffentlichen Schlüssel mit der Signatur(Pub(S) $\star$ Sig).
4. Überprüfe die Gleichheit von 2 Matrizen Matrix(Pub(S) $\star$ Sig) und (Matrix(Pub(E(H(m) * Matrix (Pub(S)). Die Verifizierung ist positiv, wenn die beide Matrizen gleich sind.[5, S. 8]

6.7 Umformungen

Für die Umformung von Signatur kann man den BKL-Normalform und den Algorithmus von Dehornoy verwenden. Die notwendige Diffusion wird überwiegend durch BKL-Normalform erzeugt. Der Henkelreduktionsalgorithmus von Dehornoy wird zusätzlich verwendet, um die Gesamtlänge von Signatur zu reduzieren, da die Signatur über BKL-Normalform oft viel länger wird.

6.7.1 BKL(Birman-Ko-Lee)-Normalform

Ein BKL-Normalform verwandelt beliebeiges Braid mit n Strähne zu diesem Form:

$$W = \begin{cases} \delta_n^u A_1 A_2 ... A_k \text{ (Linksnormalform)} \\ A_1 A_2 ... A_k \delta_n^u \text{ (Rechtsnormalform)} \end{cases} \text{, wobei } u \in Z \tag{6.8}$$

δ ist ein *Funtamental Braid* und A_i sind *Kanonische Factoren*, die aus Produkt von positiven Band-Generatoren entstehen. Dabei ist u möglichst groß und k möglichst kleine Zahl[31, S. 150]. D.h., man verschiebt alle verschiebbare Elemente nach Links(oder nach Rechts, wenn es um Rechtsnormalform geht), um möglichst viele Generatoren als dieses Fundamental Braid zusammenzufassen.

Band-Generator

Bis zu diesem Kapitel hat man Artin-Generatoren verwendet, die Transposition zwischen nebeneinanderliegende Strähne darstellen. Für die BKL-Normalform nutzt man andere Generatoren für Braid. Diese Generatoren vertauscht Position von zwei beliebige Strähne, ohne

dabei Position von andere Strähne zu ändern[32, S. 325]. Folgende Abbildung zeigt die Struktur von Band-Generatoren.

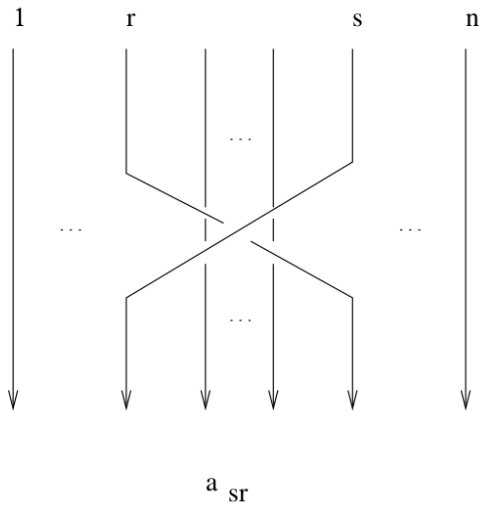


Abbildung 6.2: Band-Generator[33, S. 8]

s und r sind die Indizies von den Strähne und man schreibt die Strähne zuerst, die auf anderen Strähne laufen wird. Ein Band-Generator ist positiv, wenn $s \geq r$ gilt, und negativ, wenn $s<r$ gilt. Die Artin-Generator sind also spezielle Fälle von Band-Generatoren, in der s und r benachbart sind[32, S. 324-325]. Jeder Band-Generator hat auch eine äquivante Darstellung als Artin-Generatoren:

$$a_{sr} = \begin{cases} (\sigma_{s-1}\sigma_{s-2}...\sigma_{r+1})\sigma_r(\sigma_{r+1}^{-1}...\sigma_{s-2}^{-1}\sigma_{s-1}^{-1}) & \text{für } s \geq r \\ (\sigma_{r-1}\sigma_{r-2}...\sigma_{s+1})\sigma_s^{-1}(\sigma_{s+1}^{-1}...\sigma_{r-2}^{-1}\sigma_{r-1}^{-1}) & \text{für } s<r \end{cases} \tag{6.9}$$

Hier muss man aufpassen, dass alle positive Artin-Generatoren auch positive Band-Generatoren sind, aber nicht alle positive Band-Generatoren sind mit positiven Artin-Generatoren darstellbar.

Fundamental Braid

Das Fundamental Braid δ_n ist spezielles Braid mit mehre wichtigen Eigenschaften. Das Fundamental Braid sieht so aus:

$$\begin{aligned} \delta_n &= a_{n(n-1)}a_{(n-1)(n-2)}...a_{21} \\ &= \sigma_{n-1}\sigma_{n-2}...\sigma_1 \text{ (in Artin-Generator)} \end{aligned} \tag{6.10}$$

Eigenschaft (1): Für alle positive Band-Generator a gilt:

$$\delta_n = aA = Ba \text{ , für Braids A und B} \in B_n^+ \tag{6.11}$$

B_n^+ ist die Menge aus Produkt von positive Generatoren[31, S. 150].

Eigenschaft (2): Für alle positive Band-Generator a gilt:

$$\begin{aligned} a\delta_n &= \delta_n \tau(a) \\ \delta_n a &= \tau^{-1}(a)\delta_n \end{aligned} \tag{6.12}$$

wobei τ ist ein Automorphismus von B_n, der als $\tau(a_{rs}) = \delta_n^{-1} a \delta_n = a_{(r+1)(s+1)}$ definiert wird(Falls $r+1>n$, dann $\tau(a_{rs}) = a_{(s+1)((r+1)\%n)}$)[31, S. 150]. Diese Regel ist bei der Berechnung von Normalform ganz nützlich, um Fundamental Braids nach links oder nach rechts zu verschieben.

Kanonische Factor

Die kanonische Factoren sind die Produkt aus positiven Band-Generatoren, die noch folgende Bediengung erfüllen sollen:

$$e \leq A \leq \delta_n \text{ (e ist ein neutrales Braid)} \tag{6.13}$$

Für zwei Braids V und W in B_n gilt $V \leq W$, wenn es $PVQ = W$ ist, wobei P und Q aus B_n^+ sind. Es gibt $\frac{(2n)!}{n!(n+1)!}$ kanonische Factoren, die als A anpasst. Das ist ein großer Vorteil von BKL-Normalform im Vergleich zu andere Normalformen, die ihre Berechnung mit Atrin-Generatoren durchführen, da sie andere Fundamental Braid benötigen, wodurch die Anzahl von kanonischen Factoren viel größer mit $n!$ ist. Da es wengiere kanonische Factoren gibt, kann man einige Operation leichter berechnen[31, S. 150].
Nun muss man überlegen, wie man alle kanonische Factoren einzigartig darstellen kann. Diese Darstellung heißt *Descending Cycle Decomposition Table*. Dieses Table ist von der Permutation von Braid ableitbar und jedes Table ist äquivalent zu genau einem kanonischen Faktor und diese gelten auch umgekehrt. Wie sie heißen, kann dieses Table mehre absteigende Zyklen enthalten. Hier ist ein Beispiel von Descending Cycle Decomposition Table, das ein Braid A mit $a_{65}a_{52}a_{43}$ aus B_6 darstellt:

$$\begin{aligned} &\text{Permutation von A: } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 3 & 2 & 5 \end{pmatrix} \\ &\text{Descending Cycle Decomposition Table von A: } \begin{pmatrix} 1 & 6 & 4 & 4 & 6 & 6 \end{pmatrix} \end{aligned} \tag{6.14}$$

Man kann 2 Zyklen aus der Permutation von A herleiten. Diese sind (3 4) und (2 6 5). Da in einem Zyklus beliebige Verschiebung erlaubt ist, solange die Reihenfolge identisch ist, sind dann (4 3) und (6 5 2). (4 3) entsteht aus a_{43} und (6 5 2) aus $a_{65}a_{52}$. Sowie dieses Beispiel haben ein Descending Cycle immer den Form von $(s_i s_{i-1} ... s_1)$ mit $s_i > s_{i-1} > ... > s_1$. Die Zyklen werden in dem Descending Cycle Decomposition Table geschieben, in dem man die alle Zellen, die zu jeweiligem Zyklus gehören, mit höchtste Zahl von Zyklus auffüllt(z.B. bei (4 3) werden die dritte und vierte Zellen mit 4 geschrieben).
Der Zyklus (4 3) und (6 5 2) lassen sich nicht gegeneinander „separieren“, da die Anfangsindex und Endesindex von Zyklus (4 3) zwischen 5 und 2 sind. Die Zyklen wie diese sind *parallel* und erfüllen diese Bedingung:

$$\begin{aligned} &\text{Die Zyklen S und T sind parallel } \leftrightarrow (s_a - t_c)(s_a - t_d)(s_b - t_c)(s_b - t_d) > 0, \\ &ie\text{wobei } 1 \leq a<b \leq i, 1 \leq c<d \leq j \end{aligned} \tag{6.15}$$

Der Band-Generator a_{31} mit dem Zyklus (1 3) kann nicht zusätzlich mit $a_{65}a_{52}a_{43}$ in einem Table dargestellt werden, da es den Zyklus (4 3) zu (4 3 1) erweitert, was aber nicht mehr

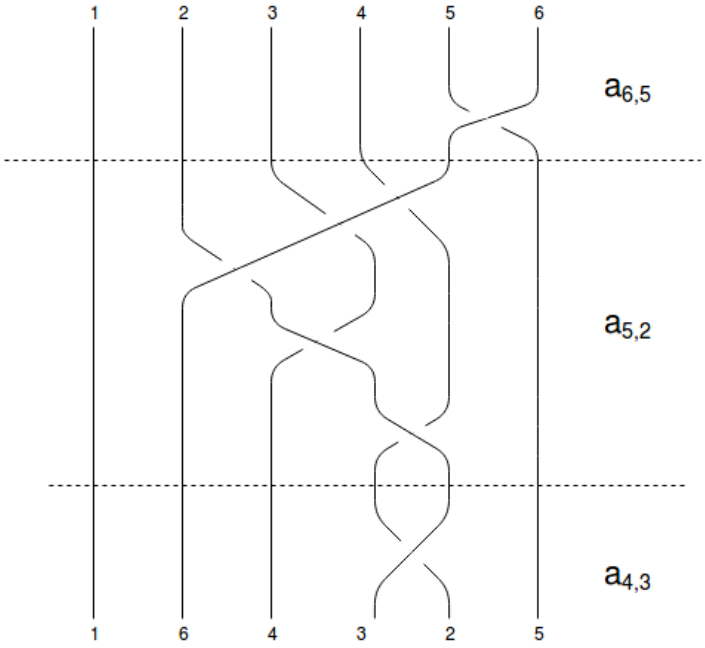


Abbildung 6.3: Graphische Darstellung von $a_{65}a_{52}a_{43}$

parallel zu (6 5 2) ist. In diesem Fall benötigt man zwei Tables, da sie sonst keine kanonische Factoren sind. Demgegenüber kann a_{21} hinzugefügt werden, da dann (6 5 2) zu (6 5 2 1) erweitern wird, der noch parallel zu (3 1) ist.
Hier sieht man nochmal, wieso das Fundamental Braid im Sinne von der partiellen Ordnung größer oder gleich zu alle andere kanonische Factoren ist.

$$\begin{aligned}
&\text{Permutation von } \delta_n\text{: } \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & 1 & 2 & \dots & n-2 & n-1 \end{pmatrix} \\
&\text{Zyklus von } \delta_n\text{: } \begin{pmatrix} 1 & n & n-1 & n-2 & \dots & 3 & 2 \end{pmatrix} = \begin{pmatrix} n & n-1 & n-2 & \dots & 3 & 2 & 1 \end{pmatrix} \\
&\text{Descending Cycle Decomposition Table von } \delta_n\text{: } \begin{pmatrix} n & n & n & \dots & n & n \end{pmatrix}
\end{aligned} \tag{6.16}$$

Da der Zyklus von n bis 1 füllt, kann er nicht mehr erweitert werden und es gibt auch kein „Zwischenbereich“, wo andere Zyklus reingelegt werden kann(Jeder Zyklus entsteht aus positive Generatoren).
Für die Berechnung von Normalform nutzt man sowohl Permutation Table(Permutation von Braid ohne die erste Zeile, da sie immer gleich ist) als auch Descending Cycle Decomposition Table, da manche Operation wie z.B. Multiplikation von Kanonischen Factoren als Permutation einfacher zu berechnen ist, während die Meet-Operation, die später noch genauer betrachten wird, aber als Descending Cycle Decomposition Table einfacher zu berechnen ist[31, 147]. Darum braucht man folgende Algorithmen1 und 2, so dass man von einem Darstellungsform auf anderen hin und her konvertieren kann.

Algorithm 1: Konvertierung von Permutation auf Descending Cycle Decomposition Table[31, 147]

Input: Permutation Table A in Länge von n
Output: Descending Cycle Decomposition Table X in Länge von n
for $i \leftarrow 1$ **to** n **do**
  $X[i] \leftarrow 0$;
end
for $i \leftarrow n$ **to** 1 **do**
  if $X[i] = 0$ **then**
    $X[i] \leftarrow i$;
  end
  if $A[i] < i$ **then**
    $X[A[i]] \leftarrow X[i]$;
  end
end

Algorithm 2: Konvertierung von Descending Cycle Decomposition Table auf Permutation[31, 148]

Input: Descending Cycle Decomposition Table X in Länge von n
Output: Permutation Table A in Länge von n
(We need an array Z of size n.)
for $i \leftarrow 1$ **to** n **do**
  $Z[i] \leftarrow 0$;
end
for $i \leftarrow 1$ **to** n **do**
  if $Z[X[i]] = 0$ **then**
    $A[i] \leftarrow X[i]$;
  else
    $A[i] \leftarrow Z[X[i]]$;
  end
  $X[A[i]] \leftarrow X[i]$;
end

Operationen

Um den Normalform zu berechnen, braucht man diverse Operationen, die nun auf kanonische Factoren einsetzbar sind. Diese sind der Vergleich, die Produkt, die Inverse, der Automorphismus und das *Meet*.

Vergleich Mit dem Vergleich überprüft man die Gleichheit von zwei kanonischen Factoren. Dabei sehen wir, ob das Permutation Table oder das Descending Cycle Decomposition Table identisch ist. Der Aufwand ist für die beide Darstellungen gleich mit O(n)[31, S. 148].

Produkt Diese Operation ist als das Permutaion Table leichter durchführbar. Die Komplexität vom folgenden Algorithmus3 ist O(n)[31, S. 148].

Algorithm 3: Multiplikation von Permutation Tables

Input: Permutation Table A, B in Länge von n
Output: Permutation Table C in Länge von n

for $i \leftarrow 1$ **to** n **do**
  $C[i] \leftarrow A[B[i]]$;
end

Inverse Diese Operation ist auch als das Permutaion Table leichter durchführbar mit der Komplexität von O(n)[31, S. 148]. Der ALgorithmus4 beschreibt genauere Ablauf.

Algorithm 4: Inverse von Permutation Table

Input: Permutation Table A in Länge von n
Output: Permutation Table B mit $B = A^{-1}$ in Länge von n

for $i \leftarrow 1$ **to** n **do**
  $B[A[i]] \leftarrow i$;
end

Automorphismus Der Automorphismus ist für einen kanonischen Factor A als $\tau(A) = \delta * A * (\delta^{-1}$ definiert. D.h., zwei Multiplikation soll durchgeführt werden.
Für die Berechnung von BKL-Normalform braucht man aber sehr häufig $\tau(A)^z$ mit $\delta^z * A * (\delta^{-z}$ statt einfacher Automorphismus. Dabei ist Permutation Table von δ^n noch mal zum Betrachten:

$$\begin{aligned}
\delta &= \begin{pmatrix} 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} \\
\delta^2 &= \begin{pmatrix} 7 & 8 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \\
\delta^3 &= \begin{pmatrix} 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \\
&\dots \\
\delta^8 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}
\end{aligned} \tag{6.17}$$

Nun sehen wir, dass für jede δ die Permutation Table nach rechts(links, wenn die Exponent negativ ist) rotiert. D.h., ein beliebiges δ^z kann man mit der $nmod8$ Verschiebungen nach rechts oder nach links gewinnen, ohne dabei tatsächliche die Produkt von Permutationen durchführen zu müssen.

Meet Die Meet-Operation ist einer von wichtige Stellen, wo das Descending Cycle Decomposition Table verwendet wird. Mit dieser Operation muss man alle gemeinsame Teilzyklen herausfinden können. Hier ist ein Beispielsein- und ausgabe.

$$\begin{aligned}
&\text{Eingaben:} \\
&\text{Descending Cycle Decomposition Table A} = \begin{pmatrix} 2 & 2 & 4 & 4 \end{pmatrix} \\
&\text{Descending Cycle Decomposition Table B} = \begin{pmatrix} 1 & 4 & 4 & 4 \end{pmatrix} \\
&\text{Ausgabe:} \\
&\text{Descending Cycle Decomposition Table C} = \begin{pmatrix} 1 & 2 & 4 & 4 \end{pmatrix}
\end{aligned} \tag{6.18}$$

A = (2 2 4 4) B = (1 4 4 4)

Bucket

	Array 1
1	
2	1, 2
3	
4	3, 4

Sortiere Bucket 2 von Array 1:

	Array 2
1	1
2	
3	
4	2

Kein Zyklus

Sortiere Bucket 4 von Array 1:

	Array 2
1	
2	
3	
4	3, 4

Ein Zyklus mit (4 3).
F"ulle Index 4 und 3 von
Table C mit 4

Ergebnis: Table C mit (1 2 4 4)

Abbildung 6.4: Ein Beispielsablauf von Berechung der Meet-Operation

A enthält den Zyklus (4 3), (2 1) und B (4 3 2). Also (4 3) ist dann der gemeinsame Teilzyklus.
Hier ist eine mögliche Variante, diese Operation zu berechnen. Dabei braucht man zwei zweidimensionale Arrays als Buckets. Die Indizies von Descending Cycle Decomposition Table A wird nach ihren Wert im ersten Array eingelegt. Als nächsten Schritt muss man Buckets einzeln betrachten. Falls es mehre Elemente haben, wird das in zweiten Array verteilt, wobei diesmal der Wert von Table B genommen wird. Wenn ein Bucket im zweiten Array mehre Elemente hat, enthält es gemeinsame Zyklen. Die Abbildung 6.4 stellt diese Schritte graphisch dar.

Umwandlung von Artin-Generatoren in kanonische Factoren

Hier fängt der erste Schritt vom Normalform. Dazu muss man alle Artin-Generatoren in Kanonische Factoren umwandlen. Da manche Operation als Permutation Table einfacher ist, wird die Daten zu erst nur in Permutation Table konvertieren. Für die positive Artin-Generatoren muss man deren Permutation gleich verwenden. Z.B. für σ_2 wäre es dann $\big(1 \quad 3 \quad 2 \quad 4 \quad 5 \quad 6 \quad ... \quad n\big)$. Für die negative Artin-Generatoren braucht man noch zusätzliche Schritte. Die negative Generatoren werden mit $\delta^{-1} * (\delta * \sigma_n^{-1})$ für Linksnormalform dargestellt(Mit $(\sigma_n^{-1} * \delta)\delta^{-1}$, falls es um Rechtsnormalform geht). $\delta * \sigma_n^{-1}$ wird als ein kanonischer Factor beschrieben. σ_2^{-1} ist also $\delta^{-1} * (\big(1 \quad 3 \quad 2 \quad 4 \quad 5 \quad 6 \quad ... \quad n\big) * \big(n \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad ... \quad n-1\big) = \delta^{-1} * \big(n \quad 1 \quad 3 \quad 2 \quad 4 \quad 5 \quad ... \quad n-1\big))$.
Nun muss man noch alle D^{-1} zu einer Seite verschieben. Dafür werden der Automorphismus verwendet. So wird der Schritt aussehen[31, S. 151]:

$$A * (D^{-n} * B_1 B_2 ... B_n) = D^{-n} * \tau^n(A) * B_1 B_2 ... B_n \tag{6.19}$$

Der Algorithmus 5 zeigt der Gesamtprozess. Dieser hat die Komplexität von $\emptyset(l^2 n$, wobei n die Breite von Braid und l die Anzahl von Permutation Table ist.

Algorithm 5: Konvertierung von Artin-Generatoren in kanonische Factoren für Linksnormalform

Input: Braid A mit i Artin-Generatoren
Output: (funds, P), mit $funds \in Z$ und P als Permutation Tables

$funds = 0$;
if $Linksnormalform$ **then**
  for $i \leftarrow n$ **to** 1 **do**
    $temp = to\_perm\_left(A[i])$;
    $P[i] = \tau^n(temp)$;
    if $A[i] < 0$ **then**
      $funds = funds + 1$;
    end
  end
else
  `// falls Rechtsnormalform`
  for $i \leftarrow 1$ **to** n **do**
    $temp = to\_perm\_right(A[i])$;
    $P[i] = \tau^{-n}(temp)$;
    if $A[i] < 0$ **then**
      $funds = funds + 1$;
    end
  end
end

Normalization von kanonische Factoren

Algorithm 6: Linksnormalizierung von kanonische Factoren[31, S. 152]

Input: (funds, P), mit $funds \in Z$ und P als kanonische Factoren
Output: (funds, Q), mit Q als normalisierte kanonische Factoren

$l = Length(P)$;
$i = 1$;
while $i < l$ **do**
  $t \leftarrow l$;
  for $j \leftarrow (l-1)$ **to** i **do**
    `// berechne gemeinsame Braids zwischen Rechtskomplement von P[j] und P[j+1]`
    $B = meet(P[j]^{-1} * \delta, P[j+1])$;
    if B *ist nicht trivial* **then**
      $t \leftarrow j$;
      `// verschiebe B nach links`
      $P[j] \leftarrow P[j] * B$;
      $P[j+1] \leftarrow B^{-1} * P[j+1]$;
    end
  end
  $i \leftarrow t + 1$;
end
`// fasse Fundamental Braids an der linken Seite in funds zusammen`
while $l > 0$**and**$P[1] = \delta$ **do**
  lösche P[1] von P; $l = l - 1$;
  $funds = funds + 1$;
end
`// lösche triviale Braids an der rechten Seite`
while $l > 0$**and**$P[i]$ *ist trivial* **do**
  lösche P[i] von P; $l = l - 1$;
end

Der Algorithmus 6 normalisiert eingegebene kanonische Factoren nach links. Dabei betracht der für jeden Schritt zwei kanonische Factoren. Da wird ein Meet zwischen der Rechtskompliment vom linken Element(Es ist $A_j^{-1} * D$) und dem rechten Element. Falls das Ergebnis von der Meet-Operation nicht trivial ist, wird es nach links verschoben.
Für den Rechtsnormalform muss man von rechts nach links iterieren. Trivialerweiser muss man Linkskompliment von rechten Element berechnen und das Ergebnis von Meet-Operation nach links verschieben. Und Zusammenfassung von Fundamental Braids und Löschen von triviale Braids soll nun an andere Seite passieren.
Die durschnittliche Länge von BKL-Links- und Rechtsnormalform von Walnut-DSA Signatur ist beim Linksnormalform kürzer. Genauere Konfiguration und Werte sind bei [7] befindlich.

Konvertierung von Normalform in Artin-Generatoren

Hier konvertiert man zu erst Permutation Tables in Descending Cycle Decomposition Table, da die Zyklen damit leichter lesbar sind. Dann schreibt man alle Zyklen mit Artin-

Generatoren. Dann bleibt noch die Fundamental Braids übrig. Bei dem Linksnormalform wird am Anfang des Braids alle Fundamental Braids hinzugefügt(Bei dem Rechtsnormalform am Ende des Braids). Der Algorithmus 7 zeigt den konkrete Ablauf.

Algorithm 7: Konvertierung von kanonischen Factoren auf Artin-Generatoren

Input: (funds, Q), mit l kanonische Factoren
Output: A mit x Artin-Generatoren
`// Braid hat n Strähne`

if *Leftnormalform* **then**
  Schreibe Fundamental Braids;
end
for $i \leftarrow 1$ **to** l **do**
  for $j \leftarrow n$ **to** 2 **do**
    `// suche Descending Cycle mit j als höchste Index`
    $last \leftarrow Q[i][j]$;
    for $k \leftarrow j-1$ **to** 1 **do**
      if *Q[i][j] = Q[i][k]* **then**
        Schreibe Band-Generator $a_{last\ k}$ in A;
      end
      $last \leftarrow Q[i][k]$;
    end
  end
end
if *Rechtsnormal* **then**
  Schreibe Fundamental Braids;
end

6.7.2 Algorithmus von Dehornoy

Dieser Algorithmus ist ein anderer Normierungsalgorithmus, der zum Vergleich mehre unterschiedliche Braids verwendet wird[34, S. 1]. Der interessante Punkt ist das, dass dieser Verfahren unsere über BKL-Normalform umgeformte Signatur in der Regel stark verkürzen.

Henkel

In dieser Algorithmus wird folgende spezielle Folge von Braids als Henkel definiert:

$$\begin{aligned} &\sigma_j^e * v_0 * v_1 * ... * v_{m-1}\sigma_j^{-e}, \\ &\text{mit } e \in \{1,-1\} \text{ und } v_0,...,v_{m-1} \notin \{\sigma_{j-1}^1, \sigma_{j-1}^{-1}, \sigma_j^1, \sigma_j^{-1}\} \end{aligned} \tag{6.20}$$

Da ein Henkel keine σ_{j-1}^1 Generatoren enthalten, wird ein Henkel wie in Abbildung 6.5 aussehen. Der Generator σ_{j-1}^1 und σ_{j-1}^{-1} bilden also ein Henkel mit der Strähne $j+1$.

6.7.3 Reduktion von Henkeln

Die Henkelreduktion hat den Effekt die Abbildung 6.6 zeigt.
Für ein Henkel σ_j^e muss man lediglich die σ_{j+1}^f in der Henkel mit $\sigma_{j+1}^{-e} * \sigma_j^f * \sigma_{j+1}^e$ ersetzen

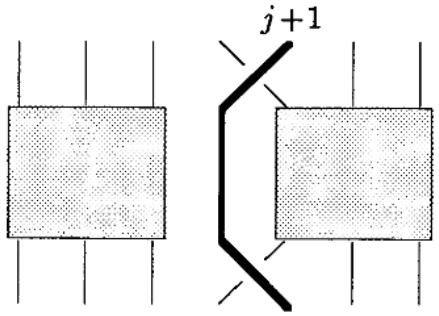


Abbildung 6.5: Ein σ_j Henkel[34, S. 205]

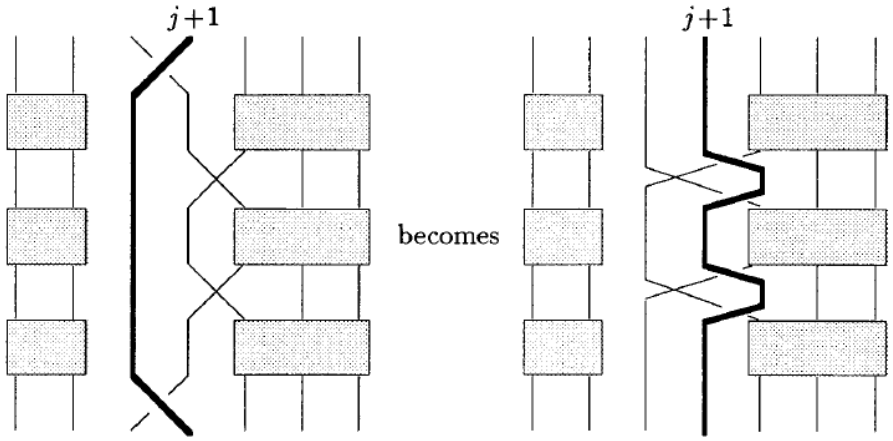


Abbildung 6.6: Henkelreduktion für σ_j[34, S. 206]

und σ_j^e, σ_j^{-e} am Anfang und am Ende der Henkel löschen.
Hier kommt doch eine Bedingung, wann ein Henkel reduzierbar ist. Ein Henkel σ_j^e ist reduzierbar, wenn er keinen anderen Henkel mit σ_{j+1}^f enthält, wobei $e, f \in -1, 1$. Sonst ist es möglich, dass die Reduktion das Braid unendlich verlängert, wie im folgenden Beispiel:

$$\begin{aligned} &\sigma_1\sigma_2\sigma_3\sigma_{-2}\sigma_{-1} \\ &\Leftrightarrow \sigma_{-2} * \sigma_1\sigma_2\sigma_3\sigma_{-2}\sigma_{-1} * \sigma_2 \\ &\Leftrightarrow \sigma_{-2}^n * \sigma_1\sigma_2\sigma_3\sigma_{-2}\sigma_{-1} * \sigma_2^n \text{ (nach n Reduktionen auf Henkel } \sigma_j) \end{aligned} \tag{6.21}$$

Gesamtablauf von Algorithmus

Es kann mehre Variante geben, in welcher Reihenfolge Henkeln reduzieren, weil man lediglich darauf achten muss, ob ein Henkel reduzierbar ist. Im Paper [34] wird dazu zwei Variante vorgeschlagen.

„greedy handle reduction“ Diese Variante erfüllt minimale Bedinung, zu Vergleich unterschiedliche Braids benötigt wird. Hier sieht man einen Artin-Generator mit den niedrigsten Absolut als ein *Main-Generator*. Man reduziert alle Henkeln, die gleiche Absolut wie der

Main-Generator haben. Dabei werden alle verschachtele Henkeln in betroffenen Henkeln zu erst reduziert.

„full handle reduction“ Diese Variante sucht einen reduzierbaren Henkel von links und reduziert es. Es wird beliebig oft wiederholt, während noch ein Henkel im Braid befindlich ist. Diese Variante könnte interessant sein, wenn es viel mehr darum geht, Anzahl von Artin-Generatoren zu verkleinern. Da diese aber auch alle Henkeln reduziert, braucht es mehr Berechnung

——— Ende des Zitats. ———

7 Implementierung unter Linux auf dem Raspberry Pi

Im Folgenden soll die Implementierung von WalnutDSA unter Linux auf dem Raspberry Pi dargestellt werden. Hierbei wird zunächst kurz das verwendete Gerät und Betriebssystem vorgestellt. Anschließend werden die wichtigsten Teile der generischen Implementierung des Signaturverfahrens aufgezeigt. Darauf folgt eine Darstellung der Einbettung des Quellcodes in ein Kernelmodul für Linux sowie die Einbindung in die kryptographische API des Betriebssystems. Zum Schluss soll die Implementierung bezüglich ihrer Korrektheit und der Fehlerfreiheit ihrer Speicherverwaltung sowie ihrem Speicherplatzverbrauch und Laufzeitverhalten evaluiert werden.

7.1 Raspberry Pi

Raspberry Pi bezeichnet eine Reihe sogenannter *Einplatinencomputer*, also Geräte die einen vollständigen Computer auf einer kleinen Leiterplatte beinhalten. Die Rechner werden von der Raspberry Pi Foundation im Vereinten Königreich entwickelt und erfreuen sich großer Beliebtheit; bis Juni 2017 wurden beinahe 15 Millionen Exemplare verkauft [35]. Der primär vorhergesehene Verwendungszweck besteht darin, Kindern und Jugendlichen mithilfe eines kostengünstigen Rechners Informatik und Programmierung beizubringen. Die Geräte wurden jedoch auch außerhalb von Bildungseinrichtungen in zahlreichen Projekten wie z.B. zur Automatisierung im Smarthome verwendet. [36]

Auf den Raspberry Pi's lassen sich eine Vielzahl an Betriebssysteme verwenden. Dazu zählen neben FreeBSD und Windows 10 IoT Core auch viele Linuxdistributionen. Hierzu gehört auch Raspbian, eine Abwandlung von Debian, die speziell auf die Rechner zugeschnitten ist.

Für die vorliegende Arbeit wurde ein Raspberry Pi Model B der ersten Generation benutzt. Dieses Modell verwendet die 32-Bit ARMv6Z-Architektur, speziell einen ARM1176JZF-S Einkernprozessor mit einer Taktfrequenz von 700 MHz. Auf dem Gerät sind 512 MB Arbeitsspeicher vorhanden, welche allerdings mit der GPU geteilt werden müssen. Zur Kommunikation mit anderen Geräten verfügt der Raspberry Pi über eine Ethernetbuchse für kabelgebundene Netzverbindungen. Für kabellose Datenübertragungen können USB-basierte WiFi-Adapter verwendet werden.

Bei dem Modell handelt es sich also um ein leistungsstärkeres Gerät als viele andere eingebettete Geräte. Da jedoch auf dem Raspberry Pi Linux unterstützt wird, kann so eine generische Implementierung von WalnutDSA für das Betriebssystem geschaffen werden, die auch auf vielen anderen Geräten mit unterschiedlichen Leistumgsumfängen verwendet werden kann.

7.2 Linux

Linux wurde 1991 von Linus Torvalds ins Leben gerufen und mittlerweile zum wohl weit verbreitesten Betriebssystem-Kernel aufgestiegen. Der Kernel wird in Geräten unterschiedlichster Größenordnungen wie Android-basierten Smartphones, Desktop-PCs, Serversystemen und Supercomputern benutzt, was nicht zuletzt der kostenlosen Verfügbarkeit und der verwendeten GPL2-Lizenz zuzuschreiben ist. Auch im Bereich der eingebetteten Systeme ist das Betriebssystem an oberster Stelle anzutreffen; im IoT-Bereich kommt bereits auf mehr als 80% aller Geräte Linux zu Einsatz. [37]

Bei Linux handelt es sich um einen monolithischen Kernel, für den jedoch separate Module dynamisch zur Laufzeit nachgeladen werden können, um neue Funktionalität bereitzustellen. Die Module verwenden dann nicht den normalen Userspace-Speicherbereich wie normale Anwendungsprogramme, sondern laufen im privilegierten Kontext des Kernels. Die Umsetzung von WalnutDSA geschieht in Form eines solchen Kernelmoduls. Zudem wurde das Verfahren in die sog. *Crypto-API* des Kernels — eine Programmierschnittstelle für kryptographische Verfahren — eingebunden. Für die Implementierung des Moduls wurde Linux 4.14.0 gewählt.

7.3 Implementierung von WalnutDSA

Zur Implementierung von WalnutDSA in C wurde das Verfahren in eine Kernel- und eine Userspacekomponente aufgeteilt. Das Kernelmodul ist für die Signaturgenerierung und -verifizierung verantwortlich und kann über besagte Crypto-API des Linux Kernels angesprochen werden. Das Userspaceprogramm dient zur Generierung von Schlüsselpaaren und kann zugleich dazu verwendet werden, die Funktionen des Kernelmoduls über Systemaufrufe anzusprechen. Das Kernelmodul enthält eine recht generische Implementierung von WalnutDSA in einer eigenen Quelldatei. Das eigentliche Kernelmodul bindet diese dann in die Crypto-API ein und kümmert sich um die Speicherverwaltung bei der Verwendung der Funktionen im Kernel.

Im Folgenden sollen einige Komponenten der Implementierung von WalnutDSA erläutert und dabei auf wichtige bzw. plattformspezifische Details eingegangen werden. Die Teile der Implementierung, welche hier nicht behandelt werden, sind einfache Umsetzungen der theoretischen Definitionen zu C-Quellcode und benötigen keine weitere Erklärung.

7.3.1 Datenstrukturen und Speicherverwaltung

Zur Repräsentierung der Daten, die beim Signaturverfahren verwendet werden, wurden passend große Datentypen verwendet, um nicht unnötig Speicherplatz zu verbrauchen.

Ein Artingenerator wird in einem Byte repräsentiert. Hierfür wird der Datentyp `int8_t` verwendet, welcher Platz für eine ganze Zahl im Intervall -128–127 bietet. Da in der Zopfgruppe B_n der geometrisch betrachtet am weitesten rechts liegende Artingenerator b_{n-1} ist, können hiermit alle Artingeneratoren sowie deren Inversen bis zur Zopfgruppe B_{128} dargestellt werden. Die zugrundeliegende Permutation eines Braids wird in einem normalen Integer-Array repräsentiert. Somit können hiermit auch alle zugehörigen Permutation für die Braids bis zur Zopfgruppe B_{128} dargestellt werden. Da die Permutationen nur zu Berechnungen verwendet werden und nicht in großer Anzahl dauerhaft gespeichert werden müssen, wurde auf die Verwendung von Datentypen kleinerer Größe abgesehen. Bei Verwendung der üblichen Arithmetik auf ganzzahligen Datentypen kleiner als `int` werden diese vor

der Berechnung ohnehin zu einem normalen Integer konvertiert [38, 6.2.1.1]. Für die Colored Burau-Matrizen wurde ein `uint8_t` pro Matrixeintrag verwendet. Das ganzzahlige Intervall 0–255 ermöglicht die Darstellung von allen Werten bis zum endlichen Körper $GF(256)$. Die T-Werte wurden wie auch die Braidpermutationen in einem normalen Integer-Array gespeichert. Die öffentlichen Informationen wurden in einer eigenen Struktur namens `pub_params` zusammengefasst. Diese ist wiefolgt aufgebaut:

```
struct pub_params {
  unsigned int braid_group;
  unsigned int galois_order;
  unsigned int *t_values;
  unsigned int *generators;
};
```

Für die reinen Braidgeneratoren $p_{i,j}$ in `generators` wird nur der Wert i gespeichert und für j stets der Maximalwert n aus B_n angenommen.

Die verwendeten Datentypen `int8_t` und `uint8_t` können im Userspace über die Headerdatei `stdint.h` eingebunden werden. Im Kernel sind diese unter denselben Namen in `linux/types.h` definiert, was zur einfachen Nutzung in beiden Kontexten beiträgt.

In allen Prozeduren der generischen WalnutDSA-Implementierung wurde in den entsprechenden Funktionen für die generierten Datenstrukturen selbst Speicher alloziiert, welcher anschließend vom Funktionsaufrufenden wieder freigegeben werden muss. Die einzige Ausnahme hierzu stellt die E-Multiplikation dar, welche den Speicherbereich der Operanden der Operation auch für die Speicherung des Ergebnisses benutzt.

7.3.2 Generierung von reinen Braids

In einigen Teileprozeduren von WalnutDSA werden reine Braids benötigt. Daher wurde eine eigene Funktion zu Generierung von frei-reduzierten, zufälligen Produkten aus reinen Braidgeneratoren definiert:

```
static void gen_pure_braids(int8_t **dest, unsigned int *dest_size,
    unsigned int min_len, unsigned int n)
{
  int8_t *braid = kcalloc(min_len + PURE_BRAID_SIZE(1, n), sizeof(int8_t), 0);
  unsigned int gen1, gen2; // Random generators being used.
  int reduced_middle = 0; // Flag: Remove one reduced middle generator?
  unsigned int rand = 0;  // Variable to store RNG values.
  unsigned int mark = 0;  // Marker for braid index.
  int i;

  // Start with gen2 for better loop management.
  get_random_bytes(&rand, sizeof(unsigned int));
  gen2 = abs(rand) % (n - 1) + 1;
  for (i = n - 1; i > gen2; i--, mark++)
    braid[mark] = i;

  while (true) {
    // Update generators.
    gen1 = gen2;
    get_random_bytes(&rand, sizeof(unsigned int));
    gen2 = abs(rand) % (n - 1) + 1;

    // Build first generator middle part.
```

```
    for (i = 0 + reduced_middle; i < 2; i++, mark++)
      braid[mark] = gen1;

    if (mark >= min_len)
      break;

    // Build freely reduced start and end connecting the two generators.
    if (gen1 >= gen2) {
      for (i = gen1; i > gen2; i--, mark++)
        braid[mark] = i;
      reduced_middle = 0;
    } else if (gen1 < gen2) {
      for (i = gen1 + 1; i < gen2; i++, mark++)
        braid[mark] = i * -1;
      reduced_middle = 1;
    }
  }

  // Build last generator ending.
  for (i = gen1 + 1; i <= n - 1; i++, mark++)
    braid[mark] = i * -1;

  *dest = braid;
  *dest_size = mark;
}
```

Eine leicht abgewandelte Version dieser Funktion wird auch bei der Kodierungsfunktion verwendet. Die Werte `gen1` und `gen2` definieren wiederum nur die unteren Grenze i für einen reinen Braidgenerator $p_{i,j}$ mit $j = n$ aus B_n. Der generierte Braid wird auch bereits während dem Aufbau frei-reduziert. Durch die Angabe des Funktionsparameters `min_len` kann die Mindestlänge des Braids festgelegt werden. Da mehrere zufällige reine Braidgeneratoren aneinandergehängt werden, kann der Braid jedoch auch größer sein. Daher müssen für den Zweifelsfall immer $length_{min} + 2 \cdot (j_{max} - i_{max})$ Bytes für eine Mindestlänge $length_{min}$ reserviert werden.

7.3.3 Galois-Arithmetik

Für die Arithmetik im endlichen Körper $GF(q)$ existiert eine fremde Softwarebibliothek in C [39]. Diese enthält jedoch Abhängigkeiten zur C-Standardbibliothek, welche nicht im Kernel verwendet werden kann. Da für die Implementierung von WalnutDSA zudem nur zwei Funktionen (Multiplikation und Inverse) benötigt werden, wurde auf die Umschreibung und Einbindung der Bibliothek verzichtet und einfache Versionen der besagten Operationen selbst implementiert.

Die Multiplikation im endlichen Körper wurde mithilfe der *Russischen Bauernmultiplikation* implementiert:

```
uint8_t galois_mult(uint8_t a, uint8_t b, int q) {
  uint8_t result = 0;
  int poly = irr_polys[(int) log2(q) - 5];
  bool overflow;
  while (a != 0) {
    if ((a & 1) != 0)
      result ^= b;
    overflow = (b & (q / 2)) != 0;
    b <<= 1;
    if (overflow)
      b ^= poly;
    a >>= 1;
```

```
    }
    return result;
}
```

Das irreduzible Polynom ist für jeden unterstützten endlichen Körper $GF(q)$ unterschiedlich. Daher wurden die Polynome in einem statischen Array gespeichert, sodass in der Funktion je nach Angabe der Ordnung q des endlichen Körpers das korrekte Polynom verwendet werden kann. Die verwendeten Polynome wurden für optimale Rechenzeit ausgewählt [40].

Die Inverse eines Elements im endlichen Körper wird durch eine Bruteforce-Suche erreicht. Für ein Element a findet man die Inverse, indem man alle möglichen Produkte $a \cdot b$ ausprobiert. Der Wert b, für den das Ergebnis 1 lautet, ist die Inverse des Elements a.

Die Summe und Differenz im endlichen Körper kann durch ein bitweises exklusives Oder realisiert werden, welches schon als Operator `^` in der Programmiersprache C enthalten ist.

7.3.4 E-Multiplikation

Die Funktion `emult(...)` stellt die Implementierung des einfachen Multiplikationsschritts für einen Artingenerator und seine zugehörige Permutation dar. Um die E-Multiplikation auf einem zusammengesetzten Braid zu berechnen, muss man wiederholt diese Funktion anwenden.

Die Umsetzung richtet sich ganz nach der formalen Definition. Zunächst werden die T-Werte permutiert und ggf. die Inverse des T-Werts berechnet. Anschließend konstruiert man die Colored Burau-Matrix und multipliziert sie mit der Matrix aus dem Funktionsparameter `matrix`. Die Permutation des Artingenerators wird mit der aus dem Funktionsparameter `perm` verkettet. Zum Schluss werden die Matrix und Permutation in die Speicherbereiche der Argumente `matrix` und `perm` kopiert und damit die alten Werte überschrieben. Dies ermöglicht eine einfachere Abarbeitung der E-Multiplikation bei zusammengesetzten Braids.

Die Funktion ist sowohl im Kernelmodul als auch im Userspaceprogramm definiert, da man sie auch für die Generierung des öffentlichen Schlüssels benötigt.

7.3.5 Cloaking-Elemente

Auch die Funktion zur Erzeugung von Cloaking-Elementen funktioniert genau gemäß der Beschreibung in Kapitel 6.4. Das erste Stück des Cloaking-Elements muss die Permutation des Braids verändern, damit in dieser die Abbildungen $i \mapsto \sigma^{-1}(a)$ und $i+1 \mapsto \sigma^{-1}(b)$ erfüllt sind. Dies geschieht durch folgendes Quellcodefragment:

```
if (mid <= perm_a && mid < perm_b) {
  for (i = 0; i < perm_a - mid; i++, mark++)
    braid[mark] = perm_a - i - 1;
  if (perm_b < perm_a)
    braid[mark++] = perm_b;
  for (i = 0; i < perm_b - (mid + 1); i++, mark++)
    braid[mark] = perm_b - i - 1;
} else if (mid < perm_b && mid >= perm_a) {
  for (i = 0; i < perm_b - (mid + 1); i++, mark++)
    braid[mark] = perm_b - i - 1;
  for (i = 0; i < mid - perm_a; i++, mark++)
    braid[mark] = perm_a + i;
} else if (mid < perm_a && mid >= perm_b) {
  for (i = 0; i < (mid + 1) - perm_b; i++, mark++)
    braid[mark] = perm_b + i;
  if (perm_a != mid + 1) {
```

```
      for (i = 0; i < perm_a - mid; i++, mark++)
        braid[mark] = perm_a - i - 1;
      braid[mark++] = mid + 1;
    }
  } else {
    for (i = 0; i < (mid + 1) - perm_b; i++, mark++)
      braid[mark] = perm_b + i;
    if (perm_b < perm_a)
      braid[mark++] = perm_a - 1;
    for (i = 0; i < mid - perm_a; i++, mark++)
      braid[mark] = perm_a + i;
  }
```

Hier steht `mid` für die Variable i sowie `perm_a` und `perm_b` für die Werte der inversen Permutation σ^{-1} an den Stellen a und b. Es werden je nach Wert dieser Variablen Artingeneratoren an den Braid gehängt, sodass die Elemente der Permutation an die richtige Stelle ,,geschoben" werden. Der restliche Quellcode der Generierungsfunktion ist trivial und bedarf keiner weiteren Darstellung.

7.3.6 Umformungsfunktionen

Als Umformungsfunktionen wurden wie in der Arbeit zu WalnutDSA die BKL-Normalform und Dehornoys Henkelreduktionsalgorithmus implementiert.

Die Implementierung der links-kanonischen BKL-Normalform richtet sich ganz nach *Efficient Implementation of Braids* [31]. Es wurden die darin vorgestellten Algorithmen von Pseudocode nach C übersetzt. Für die Permutationstabellen und die *Descending Cycle Decomposition Tables* wurden `uint8_t`-Arrays verwendet, um den Speicherplatzverbrauch der Umformungsfunktion zu reduzieren. Es wurden einzelne Funktionen für die Multiplikation, die Berechnung der Inversen und die Äquivalenz von Braids-Permutationen geschrieben. Für die Prozedur zur Berechnung des *Meet* zweier kanonischer Faktoren wurde aufgrund der besseren Laufzeiteigenschaften die Version für Descending Cycle Decomposition Tables gewählt, wobei an entsprechender Stelle zwischen den beiden Repräsentierungen konvertiert wird. Für die Sortierungsoperation im Meet-Algorithmus wurde ein Bucketsort verwendet. Da Braids für WalnutDSA als Artingeneratoren repräsentiert werden, musste zudem der zur links-kanonischen BKL-Normalform konvertierte Braid am Ende der Funktion wieder in ein Produkt aus Artingeneratoren umgewandelt werden.

Für Dehornoys Henkelreduktion existiert eine C-Implementierung für die normale ,,greedy" Version des Algorithmus. Diese ist jedoch sehr unflexibel bezüglich der Speicherverwaltung und hat einige Abhängigkeiten zur C-Standardbibliothek. Daher wurde das Verfahren selbst neu programmiert. Wie in Kapitel 6.7 angesprochen gibt es zwei Varianten des Henkelreduktionsalgorithmus von Dehornoy. Da auf dem verwendeten Raspberry Pi genügend Ressourcen verfügbar sind, wurde die vollständige Reduktion implementiert. Dies führt zu kleineren Signaturen als die normale Version, benötigt jedoch mehr mehr Arbeitsschritte. Zudem kann der Braid während der Reduktion zwischenzeitlich größer als die Ausgangsform werden, wodurch mehr Speicherplatz benötigt wird.

7.4 Einbettung in Linux

Im Folgenden soll die Einbettung der WalnutDSA-Implementierung in Linux dokumentiert werden. Dabei wird zunächst kurz auf das Kernelmodul selbst sowie die Speicherverwaltung

im Kernel eingegangen. Anschließend wird die Einbindung in die Crypto-API dargestellt und ihre Funktionsweise erklärt.

7.4.1 Implementierung des Kernelmoduls

Wie bereits angesprochen bietet Linux die Möglichkeit, neue Funktionalität in Form von Kernelmodulen dynamisch zur Laufzeit nachzuladen. Für die Implementierung wurde ein einfaches Modul mit den entsprechenden Funktionen `module_init` und `module_exit` entworfen, dass als Eintritt in den Kernel dient. Die eigentliche Arbeit wird bei der Implementierung der Funktionen der Crypto-API verrichtet.

Zur Speicherverwaltung stehen eigene Funktionen im Kernel zur Verfügung. Darunter fallen z.B. `kmalloc`, `kcalloc` und `kfree`, welche die Gegenstücke zu den üblichen Funktionen `malloc`, `calloc` und `free` im Userspace bilden. Für die Verwendung des Kernelmoduls vom Userspaceprogramm aus müssen Daten vom einen zum anderen Bereich kopiert werden. Da zusammengehörige Speicherbereiche im Userspace jedoch häufig über den physikalischen Speicher verstreut sind, können sie nicht einfach durch einen simplen Speicherdirektzugriff in den Kontext des Kernels transferiert werden. Daher werden für die Kommunikation zwischen den beiden Bereichen sog. *Scatterlisten* verwendet. Dies sind Strukturen, die eine Abstraktion über im Speicher verstreute Daten bieten und sie als augenscheinlich kontinuierliche Speicherbereiche ansprechbar machen. Dem Benutzer stehen auch einige Hilfsfunktionen zur Verfügung, um Daten einfach in eine Scatterliste zu schreiben und sie wieder aus ihr herauszukopieren. Die relevanten Strukturen und Funktionen sind in `linux/scatterlist.h` definiert.

7.4.2 Eindbindung in die Crypto-API

Die Crypto-API des Linux Kernels stellt eine Programmierschnittstelle bereit, die sowohl für Benutzer von kryptographischen Diensten als auch deren Entwickler ausgerichtet ist. Die durch die API vorhandenen kryptographischen Algorithmen werden *Transformationen* genannt. Dabei kann es sich z.B. um symmetrische und asymmetrische Chiffren, Hashverfahren oder Zufallszahlengeneratoren handeln, welche zum Teil untereinander kombiniert werden können um zusammengesetzte Verfahren wie z.B. einen *Keyed-Hash Message Authentication Code (HMAC)* zu bilden. Für die Transformationen stehen synchrone und asynchrone Schnittstellen zur Verfügung. Die asynchronen Aufrufe können allerdings nur innerhalb des Kernels und nicht vom Userspace aus verwendet werden. [41]

Um eine neue Transformation zur API hinzuzufügen, muss eine entsprechende Registrierungsfunktion aufgerufen werden, der eine Struktur mit den nötigen Informationen der Transformation übergeben wird. Diese Struktur definiert neben Zeigern zu den Implementierungen der entsprechenden API-Funktionen auch den Namen, mit dem das kryptographische Verfahren folglich angesprochen werden kann, sowie die Speichergröße der Kontextstruktur der Transformation. Diese Kontextstruktur wird bei Verwendung der Transformation für den Benutzer erstellt und dient dazu, die zur Operation benötigten Daten über mehrere Funktionsaufrufe hinweg zu speichern. Sie ist wiefolgt aufgebaut:

```
enum operation {
  SIGN,
  VERIFY
};
```

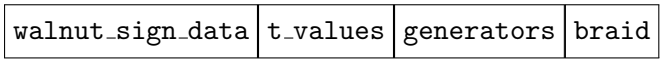
```
union walnut_context {
  enum operation operation;       // Kennzeichnung für die Operation
  struct walnut_sign_data sign_data;   // Daten zur Signierung
  struct walnut_verify_data verify_data; // Daten zur Verifizierung
};
```

Nachdem die Transformation in der Crypto-API registriert wurde, kann der Benutzer über einen Funktionsaufruf ein neues Transformationsobjekt, also eine Instanz der Transformation erzeugen. Anschließend können die verschiedenen Funktionen des Verfahrens verwendet werden.

Zu Beginn wird der Aufruf einer Funktion zur Festlegung des privaten bzw. öffentlichen Schlüssels sowie der damit einhergehenden benötigten Informationen für die Signierung bzw. Verifizierung benötigt. Bei der Signierung wird für die Ansammlung der gefragten Daten die Struktur `walnut_sign_data` verwendet:

```
struct walnut_sign_data {
  int8_t *braid;        // Privater Schlüssel
  unsigned int braid_len;  // Schlüssellänge in Artingeneratoren
  unsigned int a;       // Parameter a für Cloaking-Elemente
  unsigned int b;       // Parameter b für Cloaking-Elemente
  unsigned int sec_level;  // Sicherheitslevel
  enum rewrite_func rewrite; // Kennzeichnung der Umformungsfunktionen
  struct pub_params params; // Öffentliche Informationen
};
```

Wie man sehen kann, enthält die Struktur nur Zeiger zum privaten Schlüssel, den T-Werten und den Kodierungsgeneratoren. Die eigentlichen Daten werden nach folgendem Schema hinter die Struktur im Speicher angehängt:



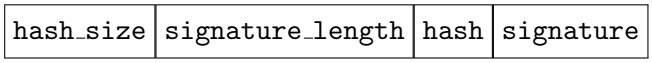
Für die Verifizierung lautet die Struktur `walnut_verify_data`:

```
struct walnut_verify_data {
  uint8_t *matrix;      // Matrix des öffentlichen Schlüssels
  unsigned int *perm;    // Permutation des öffentlichen Schlüssels
  struct pub_params params; // Öffentliche Informationen
};
```

Die Matrix und Permutation des öffentlichen Schlüssels sowie die T-Werte und Kodierungsgeneratoren werden hierbei wiefolgt an die Struktur angehängt:

Die aufbereiteten Daten werden dann an das Kernelmodul übergeben und für die folgenden Operationen gespeichert. Für die Signierung kann anschließend über einen Funktionsaufruf noch die maximale Länge der endgültigen Signatur in Erfahrung gebracht werden. So kann festgestellt werden, wieviel Speicherplatz für den Signaturbraid alloziiert werden muss. Zum

Schluss muss der Anwender die Signierungs- bzw. Verifizierungsfunktion aufrufen, wobei in beiden Fällen ein Nachrichtenhashwert und für die Verifizierung zusätzlich eine Signatur übergeben werden muss. In letzterem Fall müssen beide Datensätze nach folgendem Schema aneinandergehängt werden:



Ist die Operation abgeschlossen, so erhält der Benutzer das entsprechende Ergebnis. Im Falle der Signierung wird die Signatur zusammen mit ihrer Länge in einer Scatterliste in der Kontextstruktur gespeichert, sodass sie anschließend nur noch in den lokalen Speicher kopiert werden muss. Für die Verifizierung erhält der Anwender einen Rückgabewert, der ihn über die erfolgreiche oder fehlgeschlagene Verifizierung informiert.

Nachdem alle Operationen abgeschlossen sind, sollte der Speicher des Transformationsobjekts wieder freigegeben werden. Beim endgültigen Entfernen des Moduls aus dem laufenden Kernel werden alle zwischengespeicherten Daten wieder gelöscht und die Transformation aus der Crypto-API entfernt.

Die Funktionen der Crypto-API werden über Systemaufrufe dem Userspace zugänglich gemacht. Für die asymmetrischen Transformationen ist ein solcher Systemaufruf jedoch nicht im Mainline-Kernel vorhanden. Daher muss ein selbstkompilierter Kernel verwendet werden, für den drei verschiedene Patches [42] eingespielt sowie eine Reihe an Optionen in der Kernelkonfiguration [43] aktiviert werden müssen. Die Kernelpatches sind auf die Version 4.14.0 von Linux ausgelegt, weswegen auch genau diese Version zur Implementierung von WalnutDSA gewählt wurde. Es steht zudem die Softwarebibliothek *libkcapi* [44] zur Verfügung, welche eine einfache Programmierschnittstelle über den besagten Systemaufrufen der Crypto-API bietet. Diese wurde für die Userspacekomponente der Implementierung von WalnutDSA eingesetzt. Die Bibliothek übernimmt die komplette Kommunikation mit dem Kernel, inklusive dem Transferieren der Daten über Scatterlisten, sodass der Anwender sich nicht mit der Kernel-internen Speicherverwaltung auseinandersetzten muss.

Es sei gesagt, dass die Crypto-API für asymmetrische Kryptosysteme auch Funktionen zur generischen Ver- und Entschlüsselung von Daten bereitstellt. Da diese Operationen jedoch nicht für WalnutDSA definiert sind, wurden die entsprechenden Funktionen nicht implementiert. Beim Aufruf wird der Benutzer über eine Fehlermeldung auf die fehlende Unterstützung hingewiesen.

7.5 Evaluierung der Implementierung

Die vorgestellte Implementierung soll nun evaluiert werden. Hierbei wird die Korrektheit des Verfahrens sowie ihre fehlerfreie Speicheralloziierung untersucht. Es wird auf die potentielle Kompatibiliät zu anderen Implementierungen und die Erfüllung von gängigen Sicherheitsanforderungen eingegangen. Zudem wird der Speicherplatzverbrauch und das Laufzeitverhalten der Implementierung analysiert.

7.5.1 Korrektheit der Implementierung

Um die Korrektheit der Implementierung zu überprüfen, wurden drei verschiedene Tests unternommen. Zunächst wurde die Implementierung an sich selbst getestet, indem X Signaturen mit jeweils zufällig generierten Parametern und Schlüsselpaaren erstellt wurden. Bei der Hälfte der Signaturen wurde ein zufälliger Fehler in den Datensatz eingeführt, um die Verifizierung zu vereiteln. Bei der Verifizierung der unmodifizierten Signaturen war diese in jedem Fall erfolgreich, bei den verfälschten Signaturen schlug sie in jedem Fall fehl.

SecureRF bietet ein IoT-SDK an, welches eine Reihe an Implementierungen von WalnutDSA im Binärformat beinhaltet. Leider konnte diese Software jedoch nicht für die Arbeit beantragt werden. Die wissenschaftliche Arbeit zu WalnutDSA enthält jedoch einen beispielhaften Datensatz zur Signierung und Verifizierung. Die Implementierung wurde mit diesem Beispiel getestet und erhielt die korrekten Ergebnisse.

Um die Kompatibilität mit anderen Implementierungen sicherzustellen, wurde ein Testaufbau mit einem ESP8266 und einem Arduino M0 Pro entworfen. Dieser wird in Kapitel 8.1.1 vorgestellt.

7.5.2 Fehlerfreie Speicherverwaltung

Für eine sichere Implementierung muss gewährleistet werden, dass die Speicherbereiche aller verwendeten Daten nach der Benutzung wieder freigegeben werden, sodass keine überbleibenden privaten Informationen mehr im Arbeitsspeicher liegen. Daher wurde sichergestellt, dass keine Speicherlecks in der Implementierung von WalnutDSA auftreten.

Für die Userspacekomponente wurde hierfür das Memcheck-Programm von *Valgrind* [45] eingesetzt. Diese Software klinkt sich in die Speicherverwaltung der C-Standardbibliothek ein und untersucht die Gültigkeitsdauer und Addressierbarkeit der verwendeten Speicherbereiche. Beim Testen des Programms kamen keinerlei Speicherfehler auf.

Zur Überprüfung des Kernelmoduls wurde der *Kernel Memory Leak Detector* [46] eingesetzt. Dieser bietet äquivalent zu Valgrind eine Möglichkeit, Speicherlecks im Kernelquellcode zu finden. Der Test des implementierten Kernelmoduls lieferte auch keine Fehler.

7.5.3 Kompatibilität und Sicherheitsparameter

Da auf dem verwendeten Raspberry Pi genügend Arbeitsspeicher zur Verfügung steht, konnte dem Benutzer die Wahl der zu verwendenden Zopfgruppe B_n und die Ordnung des endlichen Körpers $GF(q)$ weitestgehend freigelassen werden. Die beiden Werte sind nur durch die Verwendung von einem Byte pro Artingenerator bzw. Element im endlichen Körper beschränkt. Somit ergibt sich eine hohe Kompatibilität des implementierten Verfahrens mit potentiellen anderen Implementierungen.

Auch die Wahl des Sicherheitslevels ist nicht durch die Implementierung eingeschränkt. Sowohl die Mindestlänge der Cloaking-Elemente als auch die des privaten Schlüssels werden dynamisch zur Laufzeit des Programms berechnet, wodurch dem Wert des Sicherheitslevels keine künstlichen Grenzen gesetzt sind. Sollten zukünftig höhere Anforderungen bezüglich der Mindestlängen dieser beiden Teile gefordert werden, so kann die Implementierung ohne Änderungen weiterverwendet werden. Das *Bundesamt für Sicherheit in der Informationstechnik* empfiehlt bspw. ab 2022 ein Sicherheitslevel von 128 Bits für die bekannten Verfahren (also z.B. AES-128 oder RSA mit 3072-Bit-Schlüsseln) [47]. Unter der Annahme, dass sich die Empfehlungen des Sicherheitslevels auf WalnutDSA übertragen lassen und keine für

das Verfahren relevanten Angriffe gefunden werden, kann die Implementierung auch nach 2022 noch problemlos diese Sicherheitsanforderungen erfüllen.

7.5.4 Speicherplatzverbrauch und Laufzeitverhalten

Zur Untersuchung der Effizienz der Implementierung wurden der benötigte Speicherplatz und die verwendete Rechenzeit des Verfahrens gemessen.

Der öffentliche Schlüssel ist unabhängig vom verwendeten Sicherheitslevel konstant in seiner Größe. Durch die Verwendung von einem Byte pro Matrixeintrag und einem `unsigned int` (welches auf der verwendeten Plattform 4 Bytes entspricht) pro Permutationseintrag ergibt sich dafür ein Speicherplatzverbrauch von $n^2 + 4n$ Bytes bei Verwendung der Zopfgruppe B_n. Ein Artingenerator wird in einem Byte repräsentiert. Die Speicherung des privaten Schlüssels benötigt bei der Einhaltung seiner Mindestlänge l also l Bytes in Abhängigkeit des Sicherheitslevels. Für eine Signatur mit der Länge l_{sig} ergibt sich analog ein Speicherplatzverbrauch von l_{sig} Bytes.

Zur Analyse der benötigten Rechenzeit wurden Schlüsselpaare für die Sicherheitslevel 112, 138 nud 256 generiert. Mit jedem Schlüsselpaar wurde eine Signatur für einen zufälligen 256-Bit-Hashwert gebildet. Die Zeit zur Generierung des Hashwerts wurde nicht in die Ergebnisse mit einbezogen, da die zur Verfügung stehenden Vergleichsdaten dies auch nicht beinhalten (s. Kapitel 8.1.2). Die Signaturen wurden anschließend verifiziert. Diese Messungen wurden zum Vergleich jeweils ganz ohne Umformungsfunktion, nur mit der BKL-Normalform und mit der BKL-Normalform und Dehornoys Henkelreduktionsalgorithmus durchgeführt. Es wurde stets der endliche Körper $GF($256 eingesetzt, da dieser die Rechenzeit nicht sonderlich stark beeinflusst. N Es wurde der Speicherplatzverbrauch und die Rechenzeit jeder Signatur dokumentiert. Die Ergebnisse sind im Folgenden dargestellt:

SL	l	L	BKL	Deh	min. l_{sig}	max. l_{sig}	∅ l_{sig}	T(Key)	T(Gen)	T(Ver)
112	86	8	nein	nein	696	772	726	7,79 ms	141 μs	92,6 ms
			ja	nein	1544	3168	2551		3,18 s	233 ms
			ja	ja	594	750	659		5,31 s	94,4 ms
128	101	9	nein	nein	682	822	750	9,64 ms	155 μs	89,4 ms
			ja	nein	1700	3018	2362		4,05 s	263 ms
			ja	ja	626	836	704		6,77 s	96,6 ms
256	222	18	nein	nein	1042	1126	1076	22,7 ms	214 μs	133 ms
			ja	nein	2962	4332	3639		7,85 s	394 ms
			ja	ja	1030	1302	1127		18,7 s	135 ms

Wie man sehen kann, nimmt die Umformung der Signatur zur BKL-Normalform die meisten Ressourcen in Anspruch und verzeichnet einen starken Anstieg in der benötigten Rechenzeit. Auch der Speicherplatzverbrauch wird durch diese Funktion stark erhöht, was jedoch durch die anschließende Anwendung von Dehornoys Henkelreduktionsalgorithmus wieder rückgängig gemacht werden kann. Zum Teil ist die Signatur nach der Reduktion sogar kleiner als die ursprüngliche Form vor der Umformung. Wie dargestellt wurde, kann jedoch auf die BKL-Normalform nicht verzichtet werden, da sie essentiell für die Vermischung der einzelnen Elemente der Signatur ist. Eine andere, effizientere Umformungsfunktion könnte dieses Problem beheben. Derzeit ist jedoch keine Alternative bekannt. Die für die Verifizie-

rung benötigte Rechenzeit steigt linear mit dem Sicherheitslevel und der Länge der Signatur. Dies war gemäß den Eigenschaften der E-Multiplikation zu erwarten. Auch die Zeit für die Signaturgenerierung steigt linear mit der Braidlänge.

Zusätzlich wurde die beschriebene Messung mit den Zopfgruppen B_{12} und B_{16} für das Sicherheitslevel 128 durchgeführt, um eine Vergleich bezüglich der verwendeten Zopfgruppen zu bilden. Dies führte zu folgenden Ergebnissen:

n	BKL	Deh	min. l_{sig}	max. l_{sig}	$\varnothing$ l_{sig}	T(Key)	T(Gen)	T(Ver)
8	nein	nein	682	822	750	9,64 ms	155 μs	89,4 ms
	ja	nein	1700	3018	2362		4,05 s	263 ms
	ja	ja	626	836	704		6,77 s	96,6 ms
12	nein	nein	876	1030	932	24,7 ms	148 μs	364 ms
	ja	nein	2900	3950	3535		6,55 s	1,15 s
	ja	ja	604	880	754		11,3 s	313 ms
16	nein	nein	872	1184	1013	68,8 ms	134 μs	820 ms
	ja	nein	3786	5370	4555		11,1 s	3,27 s
	ja	ja	606	848	765		14,1 s	766 ms

Man kann erkennen, dass steigen die benötigte Rechenzeit und der verwendete Speicherplatz für die Signatur weitestgehend linear mit der Anzahl an Strähnen in der Zopfgruppe. Die Zeit für die Verifizierung wächst allerdings weniger stark, während die Schlüsselgenerierung einen höheren Anstieg verzeichnet.

8 Ergebnisse der Evaluierung und weiterführende Diskussion

——— Der folgende Text ist ein direktes Zitat von [19] ———

Nachdem die WalnutDSA-Bibliothek auf dem eigenen System auf Korrektheit, benötigter Speicherplatz und Laufzeitverhalten geprüft wurde, werden die Ergebnisse in diesem Kapitel mit Vergleichswerten aus Tests mit anderen Implementierungen gegenübergestellt und in einem weiteren Test die Kompatibilität der Systeme untereinander getestet. Anschließend wird diskutiert, warum es sich bei WalnutDSA um ein sicheres kryptographisches Verfahren handelt und wie sich die Implementierungen aktuell umsetzen ließen.

8.1 Plattformübergreifende Evaluierung

WalnutDSA wurde für den Linux Kernel auf einem Raspberry Pi, für FreeRTOS auf einem ESP8266 und für Riot auf einem Arduino M0 implementiert. Nun soll überprüft werden, ob die Implementierungen miteinander kompatibel sind. Das bedeutet, dass die von allen drei Systemen generierten Signaturen auch auf allen dreien positiv verifiziert werden. Anschließend werden die Ergebnisse der Evaluationen der einzelnen Systeme miteinander und mit Testwerten von RSA und ECDSA verglichen.

8.1.1 Kompatibilitätstest

Die drei Testgeräte und ein Notebook sind in einem lokalen Netzwerk miteinander verbunden. Für einen Testdurchlauf nimmt ein Mikrocontroller die Rolle des Signatur-Generator und die zwei anderen die des Verifizierers ein. Der Notebook sendet ein Startsignal an den Generator. Dieser erstellt daraufhin eine Signatur mit 128-bit-Sicherheit mithilfe zufällig gewählten Parametern. Bei Erfolg wird die Signatur mitsamt aller nötigen Parametern zu einer Nachricht geparsed. Da bei diesem Test nur die Kompatibilität der WalnutDSA-Implementierungen überprüft werden soll, wurde darauf verzichtet, ganze zu signierende Nachrichten zu verschicken. Stattdessen beinhalten die unter den Geräten ausgetauschten Nachrichten wie in der Vorlage von SecureRF zufällig generierte Hashwerte.[30, p.17] Die Nachricht wird per UDP an die beiden Verifizierer gesendet. Diese zerlegen das Paket wieder in seine Bestandteile und führen die Verifizierung durch, dessen Ergebnis an das Notebook gesendet und dort angezeigt wird. Dieser Vorgang wird eine bestimmte Anzahl mal wiederholt, woraufhin die Rolle des Generators an einen anderen Mikrocontroller weitergegeben wird.

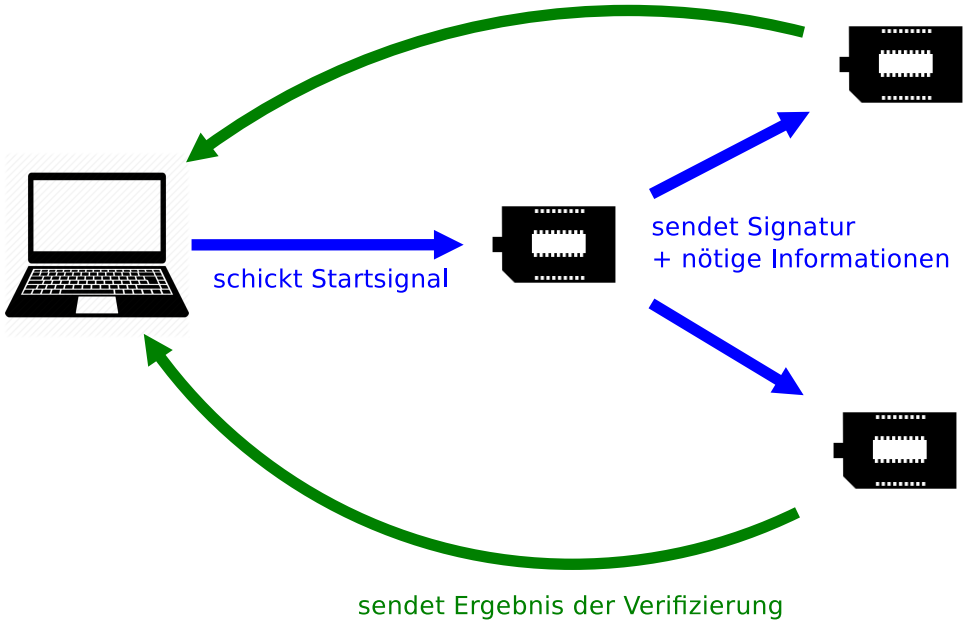


Abbildung 8.1: Aufbau des Kompatibilitätstests

Leider konnte ein derartiger Live-Test aus zeittechnischen Gründen nur mit dem ESP8266 und dem Raspberry Pi durchgeführt werden. Für die Kommunikation mit dem Arduino wurden die Nachrichten separat gespeichert und eingelesen. Alle generierten Signaturen wurden auf den jeweils beiden anderen Geräten erfolgreich verifiziert.

Es konnte leider keine Referenzimplementierung von SecureRF für einen weiteren Kompatibilitätstest verwendet werden. Eine Verwendung des Testdatensatzes aus dem WalnutDSA Paper brachte jedoch dieselben Ergebnisse, weshalb von einer Kompatibilität ausgegangen werden kann.[30, pp. 21-25]

8.1.2 Vergleich von Laufzeit und Signaturgröße

Die Laufzeit der Schlüsselpaargenerierung, Signierung und Verifizierung und der benötigte Speicherplatz der Signatur wurde für verschiedene Sicherheitslevel (n-bit-Sicherheit, angefangen mit der aktuell empfohlenen 112-bit-Sicherheit) auf den drei Geräten ermittelt. Als Vergleich werden Werte einer auf Level O3 optimierten C-Implementierung von SecureRF angegeben, die auf einem ARM Cortex M3 gemessen wurden. In der folgenden Tabelle werden ihnen auf einem Raspberry Pi ermittelte Werte von RSA und ECC gegenübergestellt. Die für das jeweilige Sicherheitslevel benötigte Schlüssellänge wurden aus einem NIST Report entnommen.[48] Es wurden die elliptischen Kurven *secp224k1*, *secp256k1* und *secp521r1* verwendet. Da für ECDSA kein Äquivalent für SL = 256 angegeben ist, wurde 521 Bit ECDSA berechnet. Die Zeitangaben der Verifizierung beinhalten nicht die Berechnung des Hashwertes aus der Nachricht.

	SL	Linux	FreeRTOS	Riot	SecRF	RSA	ECDSA
T(Key)	112	7,79 ms	25,5 ms	3,8 ms	-	6,29 s	75 ms
	128	9,64 ms	29,3 ms	6,2 ms	-	27,0 s	77 ms
	256	22,7 ms	61,0 ms	10,5 ms	-	>2 h	127 ms
T(Sig)	112	5,31 s	46,3 s	15,5 s	-	84,5 ms	3,7 ms
	128	6,77 s	50,3 s	30,5 s	-	263 ms	2,7 ms
	256	18,7 s	150,2 s	47,7 s	-	28,5 s	20,4 ms
T(Ver)	112	94,4 ms	338 ms	59,7 ms	-	2,35 ms	12,6 ms
	128	96,6 ms	366 ms	67,7 ms	5.7 ms	5,03 ms	4,8 ms
	256	135 ms	489 ms	87,2 ms	-	120 ms	78,4 ms
Gr(Sig)	112	659 Byte	337 Byte	371 Bytes	-	256 Byte	64 Byte
	128	704 Byte	461 Byte	560 Bytes	-	384 Byte	72 Byte
	256	1127 Byte	685 Byte	-	-	1920 Byte	138 Byte

Betrachtet man die Laufzeiten der Signaturgenerierung, so fällt auf, dass auf den ersten drei WDSA-Implementierung dazu sehr hohe Werte ermittelt wurden und von SecureRF dazu erst gar keine Angaben gemacht werden. Dies zeugt definitiv von einer aktuellen leistungstechnischen Schwachstelle bei der WalnutDSA Signaturgenerierung. Die Verifizierung wurde hingegen auf allen vier Modulen mittelmäßig bis sehr schnell durchgeführt. Die unterschiedlichen Ergebnisse machen deutlich, wie viel Zeit durch weitere Optimierung der Implementierung eingespart werden könnte. Verglichen mit RSA und ECDSA ist WDSA deutlich schneller.

8.2 Umsetzbarkeit der WalnutDSA-Implementierung

Die Tests der WDSA-Bibliotheken liefern auf allen Systemen selbst bei langen Braids passable Laufzeiten in der Verifizierung, aber zu lange Laufzeiten bei der Generierung. Dieser Abschnitt beinhaltet einige Gedanken, wie aktuelle Implementierungen des Verfahrens (trotzdem) eingesetzt werden könnten.

8.2.1 Auslagerung teurer Operationen

Die Signaturgenerierung benötigt im Vergleich zur Verifizierung sehr viele Rechenschritte und viel Speicherplatz. Will man den Einsatz von WalnutDSA in einem Netz von Geräten mit sehr wenig Ressourcen realisieren, ohne dabei immens hohe Laufzeiten zu erhalten, besteht theoretisch die Möglichkeit, die Generierung für alle Geräte auf eine leistungsfähigere Instanz auszulagern. Die prinzipielle Idee ist folgende: Will Bob eine signierte Nachricht schicken, schickt er zuerst den Hashwert seiner Nachricht an die Signierungsstelle Trent, der daraufhin mithilfe seines privaten Schlüssels eine Signatur erstellt und diese Bob zurückschickt. Bob kann daraufhin die signierte Nachrichten an Alice senden, solange Alice ebenfalls Trent vertraut und seinen öffentlichen Schlüssel kennt.

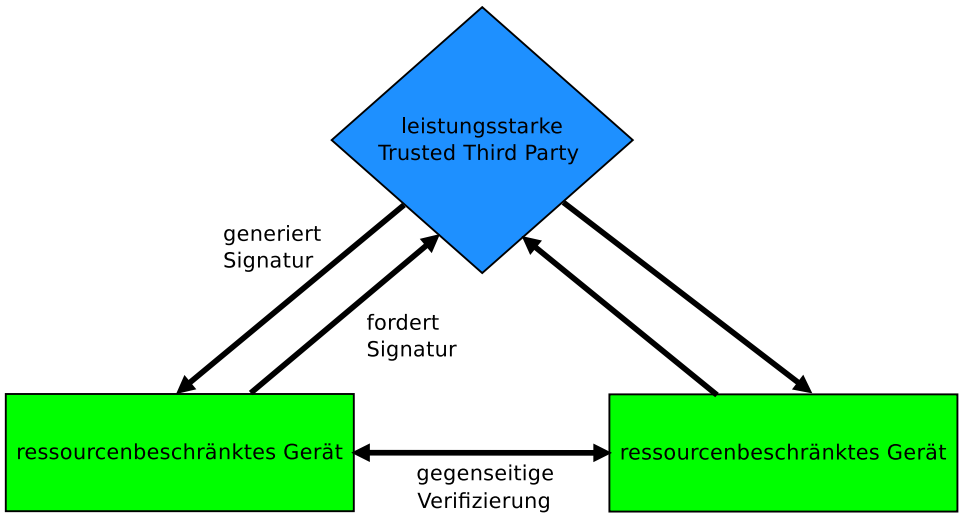


Abbildung 8.2: Prinzipielle Auslagerung der Signaturgenerierung

Eine derartige Struktur würde wahrscheinlich einen effizienteren signierten Nachrichtenaustausch ressourcenarmer Geräte ermöglichen, jedoch verletzt es das Konzept des gegenseitigen Vertrauens der einzelnen Netzteilnehmer. Da Trent Bobs Nachricht an Alice signiert, vertraut Alice niemals Bob, sondern stets nur Trent. Würde Trent ausfallen, wäre keine sichere Kommunikation zwischen den Teilnehmern mehr möglich, weswegen es sich bei der Auslagerung der Signaturgenerierung um keine optimale Lösung zur Effizienzsteigerung von WalnutDSA handelt.

Im Grunde liegt das Problem nicht bei der gesamten Signaturgenerierung, sondern nur bei ihrem letzten Schritt, der Umformung des Signaturbraids. Die Rohsignatur an sich ist sehr schnell erstellt, ohne dabei viel Speicher zu verbrauchen. Die Umformung folgt daraufhin mit der Rohsignatur als einzigen Parameter, daher kann diese genauso gut von einer anderen, evtl. stärkeren Maschine durchgeführt werden. Der Nachteil hierbei ist, dass die Übermittlung der nicht umgeformten Signatur ein Sicherheitsrisiko darstellt, da ohne Umformung die Cloaking-Elemente nur die Position des privaten Schlüssels verschleiern. Dieser liegt aber in Klartext vor und ist daher durch ein Abhören des Nachrichtenaustauschs verhältnismäßig leicht zu extrahieren. Deshalb sollte diese Methode nur in einem sicheren Netz nur mit vertrauenswürdigen Teilnehmern oder in Kombination mit einer (teuren) Verschlüsselung benutzt werden. Ein mögliches Anwendungsszenario wäre ein privates Heimnetz, in dem der Router beim Nachrichtenaustausch nach außen die Umformung übernimmt.

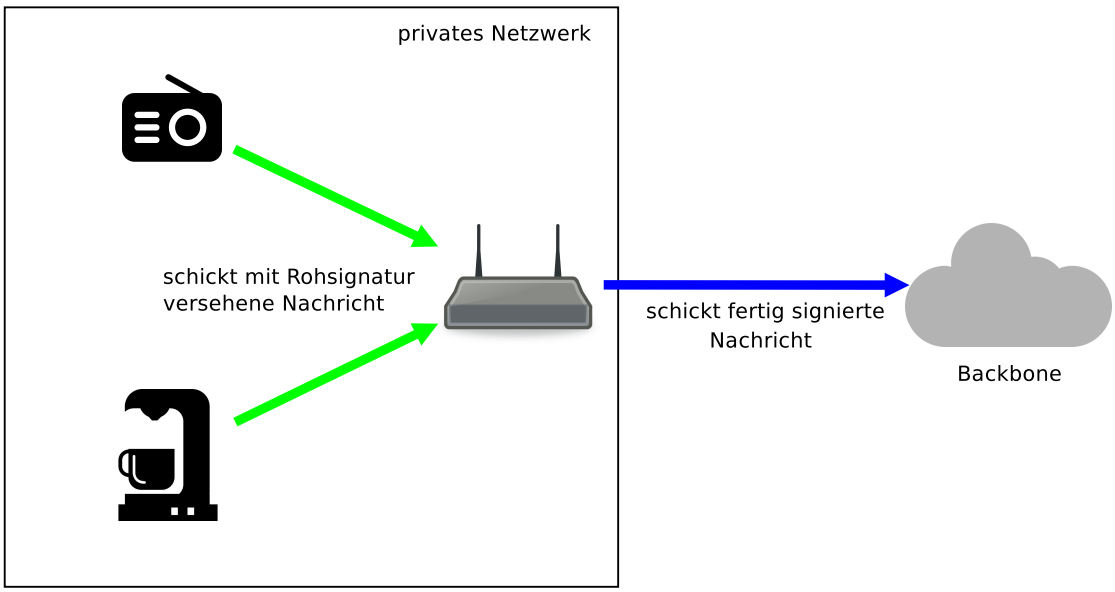


Abbildung 8.3: Beispielszenario für Auslagerung der Umformung

8.2.2 Authentizitätsgarantie durch Zertifizierungsstellen

Eine alleinige Signierung einer Nachricht durch den Absender ist anfällig für einen Man-in-the-middle-Angriff. Schickt Bob eine Nachricht an Alice besteht für Eve unter Umständen die Möglichkeit, die Nachricht abzufangen, zu verändern, den neuen Hashwert berechnen und mit ihrem eigenen privaten Schlüssel zu signieren. Solange die öffentlichen Schlüssel nicht eindeutig an die Identität geknüpft sind, merkt Alice eventuell nicht, dass sie die Nachricht mit Eves Schlüssel verifiziert und nicht mit Bobs. Bei einer Zertifizierungsstelle, im Englischen *Certificate Authority* (CA), handelt es sich um ein Mitglied im Netz, dem alle anderen Teilnehmer vertrauen. Die CA bürgt für die Identität der Mitglieder, indem sie auf Anfrage ein selbst-signiertes Zertifikat erstellt, in dem die Zugehörigkeit eines öffentlichen Schlüssels zu einer Entität beschrieben ist. Da jeder Netzteilnehmer der CA vertraut, kann jeder jedem bekannten oder fremden Gerät mit gültigen Zertifikaten der CA vertrauen.

Eine Möglichkeit der Zertifizierung mit WalnutDSA als Signaturalgorithmus ist die Erstellung von x.509 Zertifikaten. Der Standard bietet ein gutes Gerüst, um alle für die Verifizierung nötigen Informationen zu strukturieren. Die *Signature Algorithm ID* könnte neben den Bezeichner für WDSA zusätzlich die Braidgruppe N, die Größe des Galois-Körpers q und die Kodierungsgeneratoren enthalten. Die T-Werte, die Schlüsselmatrix und die Schlüsselpermutation bilden zusammen das Segment der Informationen zum öffentlichen Schlüssel. Abhängig von N und q beträgt der benötigte Speicher dafür $log_2(q) * N + log_2(q) * N * (N - 1) + N * log_2(N) = N^2 * log_2(q) + N * log_2(N)$ Bits. Bei $N = 8$ und $q = 256$ werden für das Schlüsselsegment 67 Bytes und für eine 128-Bit-Sicherheitslevel-Signatur im Durchschnitt 461 Bytes benötigt.

```
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: bb:7c:54:9b:75:7b:28:9d
 Signature Algorithm: WDSAN8Q256G1347
 Issuer: C=MY, ST=STATE, O=CA COMPANY NAME, L=CITY, OU=X.509, CN=CA ROOT
 Validity
  Not Before: Apr 15 22:21:10 2008 GMT
  Not After : Mar 10 22:21:10 2011 GMT
 Subject: C=MY, ST=STATE, L=CITY, O=ONE INC, OU=IT, CN=www.example.com
 Subject Public Key Info:
  Public Key Algorithm: wdsaEMult
  WDSA Public Key: (536 bit)
   Modulus (536 bit):
   00:ae:19:86:44:3c:dd...
   ...
 Signature Algorithm: WDSAN8Q256
 52:3d:bc:bd:3f:50:92...
```

Abbildung 8.4: potenzielles x.509 Zertifikat mit WDSA

8.3 Sicherheit von Braids

Die getesteten Implementierungen für WalnutDSA können Signaturen mit erwünschten Sicherheitslevel erstellen. Diese n-Bit-Sicherheit kann aber nur garantiert werden, wenn kein effizienterer Angriff als ein *Brute-Force-Angriff* auf das Verfahren existiert. In diesem Abschnitt wird erklärt, warum Braids, oder im speziellen WalnutDSA, diese Eigenschaft auch unter Berücksichtigung der theoretischen Möglichkeiten eines Quantencomputers den Autoren des WDSA-Papers nach erfüllen soll.

8.3.1 Unumkehrbarkeit der E-Multiplikation

Als Einwegfunktion bezeichnet man in der Komplexitätstheorie eine mathematische Funktion, die leicht zu berechnen, aber schwer umzukehren ist. Die E-Multiplikation erfolgt in linearer, von der Braidlänge abhängigen Laufzeit. Beim Versuch die E-Multiplikation umzukehren, um den privaten aus den öffentlichen Schlüssel zu berechnen, stößt man jedoch auf ein kompliziertes Gleichungssystem mit N Variablen und langer Polynome, dessen Lösung zusätzlich durch die Permutationen während der E-Multiplikation erschwert wird. Es existiert noch kein Verfahren, das den privaten Schlüssel in angemessener Zeit aus dem öffentlichen Schlüssel berechnen kann.[30, p. 9]

8.3.2 Cloaked Conjugacy Search Problem

Zwei Elemente einer Braidgruppe $u, w \in B_N$ heißen konjugiert, wenn ein $v \in B_N$ existiert, sodass gilt: $w = v^{-1}uv$. Bei dem „*Conjugacy Search Problem*“ geht es darum für zwei konjugierte Braids u und w jenes v zu finden. Ältere auf Braids basierende Verfahren der asymmetrischen Kryptographie waren sicher unter der Annahme, CSP wäre schwierig. Jedoch existieren mittlerweile effiziente Lösungen für das Problem, weshalb auf Braids basierende kryptographische Verfahren, wie z.B. das Diffie-Hellman-Braid-Protokoll, als unsicher galten.[20] Ohne Cloaking-Elemente besäße auch eine Signatur von WalnutDSA die Form $Sig = R(priv(S)^{-1}E(H(M))priv(S))$ und das Verfahren wäre nur so sicher wie CSP. Die Cloaking-Elemente in der WDSA-Signatur $Sig = R(v_2v_1^{-1}priv(S)^{-1}vE(H(M))priv(S)v_1)$

„*verhüllen*“ den privaten Schlüssel und auch wenn sie trivial zu sein scheinen, da sie in der E-Multiplikation keinen Effekt haben, machen sie längenbasierte Angriffe nutzlos und es existiert kein effizientes Verfahren, sie vom Schlüssel zu trennen. Deshalb sind auch die Techniken zur effizienten Lösung des CSPs nicht anwendbar. SecureRF nennt das Problem eine Instanz des „$Cloaked\,Conjugacy\,Search\,Problems$“, für das noch keine Lösung in sub-exponentieller Zeit existiert. [30, pp. 9-10]

8.3.3 Quantenresistenz

Es ist nicht sicher, wann der erste voll funktionsfähige Quantencomputer fertiggestellt sein wird. Einige Versuche mit Maschinen, die es schaffen, sich in bestimmten Fällen wie jene zu verhalten, zeigen jedoch eindeutig, dass Quantenrechner in Zukunft nicht nur in der Theorie eine Gefahr für viele asymmetrische Verfahren der Kryptographie darstellen. Besonders betroffen sind Methoden, die auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen, basieren, wie zB. RSA, aber auch Methoden diskreter Logarithmen, z.B. ECC. Der Shor-Algorithmus nutzt die Quanten-Fourier-Transformation, um beide Probleme in sub-exponentieller Zeit zu lösen. [25] Im Kontext der Kryptographie auf Quantencomputern wird neben Shor oft ein weiterer Name erwähnt. Beim Grover-Algorithmus handelt es sich um ein sehr effizientes Suchverfahren, das bei einer erfolgreichen Implementierung auf einem Quantencomputer das gesuchte Element unter N Kandidaten stets in $O(\sqrt{N})$ Schritten findet. Eine quadratische Beschleunigung in der Suche würde sich auf alle Verfahren mit Schlüsselpaaren, Hashfunktionen oder anderen Input/Output-Probleme auswirken und ihr Sicherheitslevel auf die Hälfte drücken. Auf Braids basierende Kryptographie oder im Speziellen WalnutDSA stellt in beiden Fällen eine gute Lösung dar. Zum einen ist der Shor-Algorithmus auf Signaturen von WDSA nicht anwendbar, da es sich bei Braids nicht um eine zyklische und abelsche Gruppe mit endlich vielen Elementen handelt. Braids verhalten sich nicht kommutativ und können unendlich lang werden. Mit zunehmender Länge wächst der Aufwand der Validierung der Signaturen nur linear, weshalb ein doppelt so hohes Sicherheitslevel im Gegensatz zu z.B. RSA leicht erreicht und dadurch auch dem Grover-Algorithmus leicht entgegengewirkt werden kann. Somit besitzen Braids nach aktuellem Wissensstand keine gravierenden Sicherheitslücken, die durch das erfolgreiche Fertigstellen eines Quantenrechners ausgenutzt werden könnten.[49, p. 5]

8.4 Die Zukunft von WalnutDSA im Bereich Internet der Dinge

Beim WalnutDSA handelt es sich um eine vielversprechendes Signaturverfahren, das die Vorteile von Braids sinnvoll nutzt. Ob es sich im Bereich Internet der Dinge in naher Zukunft effizient implementieren lässt, ist jedoch aufgrund der ineffizienten Umformungsverfahren nicht garantiert. Des Weiteren lässt sich noch nicht sagen, ob das Verfahren langfristig als sicher gelten wird. Zwar scheint mit den Cloaking-Elementen ein wirksames Werkzeug gegen Lösungen des CSPs, die bisher größte bekannte Schwachstelle von Braids, zu existieren 8.3.2, jedoch wurden auf Braids basierende Algorithmen im Vergleich zu anderen asymmetrischen kryptographischen Verfahren bisher wenig untersucht. Braids verhalten sich ganz anders als andere für die Kryptographie verwendeten algebraischen Konstrukte, daher ist es heute noch ungewiss, ob sie nicht eine bisher völlig unbekannte Schwachstelle besitzen, die evtl. sogar von Quantencomputern ausgenutzt werden könnte. Bis es aber soweit ist beherbergen Braids vor allem Dank ihrer Immunität gegenüber Shors und Grovers Algorihmen 8.3.3 und dem

mit der Braidlänge linear wachsenden Ressourcenaufwand bei der Verifizierung ein großes Potenzial in der Kryptographie für ressourcenbeschränkte Geräte.

—— Ende des Zitats. ——

9 Zusammenfassung und Ausblick

Das Ziel der Arbeit, WalnutDSA als Kernelmodul für Linux auf dem Raspberry Pi zu implementieren, wurde erreicht. Auch die geplante Einbindung in die Crypto-API war erfolgreich. Durch die Variabilität der verwendeten Braidgruppe und der Ordnung des endlichen Körpers wurde eine hohe Kompatibilität mit anderen Implementierungen gewährleistet. Die Einbettung in Linux sorgt zudem für eine starke Plattformunabhängigkeit, zumindest bezüglich vergleichsweise leistungsstärkerer Geräte, die vom Linux Kernel unterstützt werden. Zur Evaluation wurde die Umsetzung erfolgreich gegen sich selbst, zwei andere Implementierungen und einen beispielhaften Datensatz aus offizieller Quelle getestet. Die Leistung der Implementierungen von SecureRF konnte nicht erreicht werden, wenngleich eine Optimierung des Programmcodes auch nicht zum Aufgabenbereich dieser Arbeit gehörte. In Hinblick darauf sind einige Verbesserungen an der Implementierung denkbar.

Wie bereits angesprochen, ist seit der Umsetzung des Verfahrens bereits eine neue Auflage der wissenschaftlichen Arbeit zu WalnutDSA erschienen. Um die theoretische Sicherheit der Implementierung auch in Zukunft zu garantieren, sollten die Änderungen am Verfahren eingearbeitet werden. Die Konvertierung der Signatur in die BKL-Normalform nimmt den größten Teil der Laufzeit bei der Signierung ein. Während die Umformung aufgrund der dargestellten Sicherheitseigenschaften nicht ausgelassen werden kann, so könnte speziell die Implementierung dieser Funktion weiter optimiert werden oder gar an neuen, effizienteren Umformungsfunktionen geforscht werden. Es ist prinzipiell auch denkbar, einige Teiloperationen von WalnutDSA zu parallelisieren. So beinhalten bspw. einige Teile der Signatur keine Abhängigkeiten zueinander und könnten auf mehreren Rechenkernen separat generiert und anschließend zusammengesetzt werden. Auch die BKL-Normalform eignet sich gut zur Paralellisierung [31]. Wenngleich auf dem verwendeten Raspberry Pi nur ein Rechenkern vorhanden ist, so würden doch andere Geräte von dieser Verbesserung profitieren können.

Abschließend sei gesagt, dass WalnutDSA im Kontext von ressourcenschwachen Geräten des IoT-Szenarios effektiv zur Sicherung der Kommunikation beitragen kann. Wie dargestellt, ist die Implementierung des Verfahrens um ein Vielfaches schneller als RSA und liefert sogar bessere Ergebnisse als ECDSA. Durch das lineare Wachstum der benötigten Rechenzeit der E-Multiplikation können sich diese Erfolge mit steigenden Sicherheitsanforderungen nur noch weiter verbessern. Zudem stellen Braid-basierte Kryptosysteme wie WalnutDSA durch den Verzicht auf abelsche Gruppen beim Entwurf der Einwegfunktion einen vielversprechenden Lösungsansatz zur Post-Quanten-Kryptographie dar. Das digitale Signaturverfahren beinhaltet damit viel Potential für ein zukunftsträchtiges asymmetrisches Kryptosystem.

Abbildungsverzeichnis

Literaturverzeichnis

[1] Chris Ip. Hong kong iot conference. In *The IoT opportunity — Are you ready to capture a once-in-a lifetime value pool?*, 2016.

[2] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh. Iot security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 2014.

[3] S. Notra, M. Siddiqi, H. Habibi Gharakheili, V. Sivaraman, and R. Boreli. An experimental study of security and privacy risks with emerging household appliances. In *2014 IEEE Conference on Communications and Network Security*, 2014.

[4] Kerry A. McKay, Larry Bassham, Meltem Sönmez Turan, and Nicky Mouha. Report on lightweight cryptography. Technical report, US National Institue of Standards and Technology, 2017.

[5] Iris Anshel, Derek Atkins, Dorian Goldfeld, and Paul E Gunnells. Walnutdsa(tm): A quantum-resistant digital signature algorithm. Cryptology ePrint Archive, Report 2017/058, 2017. https://eprint.iacr.org/2017/058.

[6] Derek Atkins. Walnut digital signature algorithm: A lightweight, quantum-resistant signature scheme for use in passive, low-power, and iot devices, 2016.

[7] Do Hwan Kim. Implementierung und Evaluation von WalnutDSA als Modul für das Betriebssystem RIOT. Bachelorarbeit, Ludwig-Maximilians-Universität München, 2017.

[8] Hans Delfs. *Introduction to Cryptography.* Springer, 2015.

[9] Stephan Spitz. *Kryptographie und IT-Sicherheit : Grundlagen und Anwendungen.* Viweg + Teubner, 2011.

[10] Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques. Standard, International Organization for Standardization, December 2010.

[11] Elaine Barker. Digital signature standard(dss), 2013. https://csrc.nist.gov/publications/detail/fips/186/4/final.

[12] Daniel J. Bernstein. *Post-quantum cryptography.* Springer, 2009.

[13] Jyrki T. J. Penttinen. *Wireless Communications Security: Solutions for the Internet of Things.* Wiley, 2016.

[14] Amir Manzoor. *Securing Device Connectivity in the Industrial Internet of Things.* Springer, 2016.

[15] Emil Artin. Theorie der Zöpfe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 4*, 1925.

[16] I. Anshel, M. Anshel, and D. Goldfield. An algebraic method for public-key cryptography. *Mathematical Research Letters 6*, 1999.

[17] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. *New Public-Key Cryptosystem Using Braid Groups*, pages 166–183. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[18] Maurice Chiodo. An introduction to braid theory, 2005.

[19] Konrad Haslberger. Implementierung und Evaluation von WalnutDSA als Modul für FreeRTOS. Bachelorarbeit, Ludwig-Maximilians-Universität München, 2017.

[20] David Garber. Braid group cryptography. 2007.

[21] Iris Anshel. Colored burau matrices, e-multiplication, and the algebraic erasertm key agreement protocol. 2015.

[22] Scott Vanstone Darrel Hankerson, Alfred J. Menezes. *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[23] Ecrypt ii yearly report on algorithms and keysizes (2011-2012), 2012.

[24] Nicholas Jansma and Brandon Arrendondo. Performance comparison of elliptic curve and rsa digital signatures, 2004.

[25] Peter W. Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Sci. Statist. Comput.*, 26, 1997.

[26] Chris Peikert. What does gchq's ,,cautionary tale" mean for lattic cryptography?, 2016. https://web.archive.org/web/20160317165656/http://web.eecs.umich.edu/ cpeikert/soliloquy.html.

[27] Vadim Lyubashevsky Tim Güneysu and Thomas Pöppelmann. *Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems*, pages 530–547. Springer Berlin Heidelberg, 2012.

[28] Iris Anshel, Derek Atkins, Dorian Goldfield, and Paul E. Gunnells. Post quantum group theoretic cryptography, 2016.

[29] Ki Hyoung Ko, Doo Ho Choi, Mi Sung Cho, and Jand Won Lee. New signature scheme using conjugacy problem, 2002.

[30] Dorian Goldfeld Iris Anshel, Derek Atkins and Paul E. Gunnells. Walnutdsa: A quantum-resistant digital signature algorithm. 2017.

[31] Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, and Jung Hee Cheon. An efficient implementation of braid groups. In *Advances in Cryptology - ASIACRYPT 2001*, 2001.

[32] Joan Birman, Ki Hyoung Ko, and Sang Jin Lee. A new approach to the word and conjugacy problems in the braid groups. *Advances in Mathematics 139*, 1998.

[33] David Garber. Braid group cryptography. *World Scientific Review*, 2008.

[34] Patrick Dehornoy. A fast method for comparing braids. *Advances in Mathematics 125*, 1997.

[35] Wayne Williams. Raspberry pi founder eben upton talks sales numbers, proudest moments, community projects, and raspberry pi 4 [q&a], 2017.

[36] Markus Montz. c't raspberry pi: Smart home im eigenbau und mehr, 2017.

[37] Cho Jin-young. Iot operating system - linux takes lead in iot market keeping 80% market share, 2017.

[38] As 3955-1991 (c90) standard für die progammiersprache c.

[39] Fast galois field arithmetic library in c/c++.

[40] Gadiel Seroussi. Table of low-weight binary irreducible polynomials. 1998.

[41] Kernel crypto api interface specification.

[42] Github: smuellerdd/libkcapi – linux kernel crypto api user space interface library.

[43] libkcapi dokumentation – kernel interfaces.

[44] libkcapi - linux kernel crypto api user space interface library.

[45] Valgrind home.

[46] Kernel memory leak detector documentation.

[47] Kryptographische verfahren: Empfehlungen und schlüssellängen. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2017.

[48] Recommendation for Key Management. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final.

[49] SecureRF Corporation Derek Atkins. Walnut digital signature algorithm tm : A lightweight, quantum-resistant signature scheme for use in passive, low-power, and iot devices. 2016.