ENTWURF NISTIR 8114
Bericht über Leichtbau Cryptography
Kerry A. McKay
Larry Bassham
Meltem Sönmez Turan
Nicky Mouha

ENTWURF NISTIR 8114
Bericht über Leichtbau Cryptography
Kerry A. McKay
Larry Bassham
Meltem Sönmez Turan
Nicky Mouha
Computer - Sicherheitsabteilung
Laboratorium für *Informationstechnologie*
August 2016
US Department of Commerce
Penny Pritzker, Sekretär
Nationales Institut für Standards und Technologie
Willie May, Under Secretary of Commerce für Standards und Technologie und Direktor

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
ich
National Institute of Standards and Technology Interner Bericht 8114
1
29 Seiten (August 2016)
2
3
4
Bestimmte kommerzielle Einrichtungen, Geräte oder Materialien können in diesem Dokument , um identifiziert werden , um eine zu beschreiben
5
experimentelle Verfahren oder angemessen Konzept. Eine solche Identifizierung wird Empfehlung implizieren nicht beabsichtigt oder
6
Billigung durch NIST, noch ist es , dass die Einrichtungen, Materialien implizieren, oder Geräte sind unbedingt die beste
7
zur Verfügung.

8
Es kann derzeit von NIST unter Entwicklung zu anderen Publikationen Verweise in dieser Veröffentlichung sind in
9
Übereinstimmung mit dem zugewiesenen gesetzlichen Aufgaben. Die Informationen in dieser Veröffentlichung, einschließlich Konzepte und
10
Methoden können von Bundesbehörden noch vor dem Abschluss solcher Begleiter Publikationen verwendet werden. So,
11
bis jeder Veröffentlichung abgeschlossen ist, aktuelle Anforderungen, Richtlinien und Verfahren, in denen sie existieren, bleiben
12
wirksam. Für die Planung und den Übergang Zwecke kann Bundesbehörden wollen eng die Entwicklung folgen
13
diese neuen Veröffentlichungen von NIST.
14
Organisationen werden ermutigt , alle Entwürfe Publikationen bei öffentlichen Kommentierung Fristen überprüfen und Feedback
15
NIST. Viele NIST Cyber - Publikationen, andere als die , die oben erwähnt wurde , sind verfügbar unter
16
http://csrc.nist.gov/publications .
17
18
Öffentliche Kommentierungsfrist: 11. August 2016 bis zum **31. Oktober 2016**
19
Nationales Institut für Standards und Technologie
20
Attn: Computersicherheitsabteilung, Laboratorium für Informationstechnologie
21
100 Büro - Laufwerk (Poststelle 8930) Gaithersburg, MD 20899-8930
22
E - Mail: lightweight-crypto@nist.gov
23
Alle Kommentare unterliegen im Rahmen des Freedom of Information Act (FOIA) zu lösen.
24
25

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY

Berichte über Computer - Systemtechnik

Die Information Technology Laboratory (ITL) am National Institute of Standards und Technologie (NIST) fördert die US - Wirtschaft und der öffentlichen Wohlfahrt durch technische Bereitstellung Führung für die Messung und Standards Infrastruktur der Nation. ITL entwickelt Tests, Test Methoden, Referenzdaten, Proof of Concept Implementierungen und technische Analysen voranzutreiben die Entwicklung und den produktiven Einsatz der Informationstechnologie. ITL verantwortet unter anderem die Entwicklung von Management, administrative, technische und physische Standards und Richtlinien für die kostengünstige Sicherheit und Privatsphäre anderer als nationale sicherheitsrelevanten Informationen in Bundes-Informationssysteme.

Abstrakt

NIST genehmigte Verschlüsselungsstandards wurden entwickelt und für allgemeine Zwecke verwenden auszuführen Computer. In den letzten Jahren wurde es den Einsatz von kleinen Rechenvorrichtungen erhöht , dass haben begrenzte Ressourcen , mit denen Kryptographie zu implementieren. Wenn der Strom von NIST genehmigte Algorithmen können so konstruiert werden , in die begrenzten Ressourcen der stark eingeschränkten Umgebungen zu passen, ihre Leistung kann nicht akzeptabel sein. Aus diesen Gründen gestartet NIST eine leichte Kryptografie Projekt , das mit dem Lernen mehr über die Themen und die Entwicklung einer Strategie für die beauftragt wurde Standardisierung von leichten Verschlüsselungsalgorithmen. Dieser Bericht gibt einen Überblick über die leichte Kryptographie Projekt am NIST und beschreibt Pläne für die Standardisierung von leichte Verschlüsselungsalgorithmen.

45
46
Schlüsselwörter
47
Constrained - Geräte; leichte Kryptographie; Standardisierung
48
49
Danksagungen
50
Die Autoren möchten ihre NIST Kollegen für die Bereitstellung wertvolles Feedback während danken
51
die Entwicklung dieser Publikation.
52

Zusammenfassung
53
Es gibt einige neue Bereiche , in denen stark eingeschränkt Geräte miteinander verbunden sind,
54
im Konzert arbeiten einige Aufgabe zu erfüllen. Beispiele für diese Bereiche sind: Automobil
55
Systeme, Sensornetze, Gesundheitswesen, verteilte Steuerungssysteme, das Internet der Dinge (IoT),
56
Cyber-Physical Systems, und das Smart Grid. Sicherheit und Datenschutz kann sehr wichtig sein in allen
57
Diese Gebiete. Da die Mehrheit der modernen kryptographischer Algorithmen wurden entwickelt für
58
Desktop / Server - Umgebungen, viele dieser Algorithmen können nicht in die umgesetzt werden
59
gelegten Vorrichtungen durch diese Anwendungen eingesetzt. Wenn der Strom von NIST genehmigte Algorithmen können sein
60
engineered in die begrenzten Ressourcen der stark eingeschränkten Umgebungen zu passen, kann ihre Leistung

61
nicht akzeptabel. Aus diesen Gründen hatte die NIST ein Projekt leichte Kryptographie , die war
62
damit beauftragt, mehr über die Themen Lernen und eine Strategie für die Standardisierung der Entwicklungs
63
leichte Verschlüsselungsalgorithmen.
64
Dieser Bericht gibt einen Überblick über leichte Kryptographie, fasst die Ergebnisse der
65
NIST leichte Kryptographie Projekt und umreißt NIST Pläne für die Standardisierung von
66
leichte Primitiven. Insbesondere hat NIST entschieden , ein Portfolio von leichten zu schaffen
67
Primitive durch eine offene ähnliches Verfahren wie die Auswahl der Blockchiffre Betriebsarten.
68
Algorithmen werden nur im Rahmen von Profilen für die Verwendung empfohlen werden, die physikalische beschreiben,
69
Leistung und Sicherheit Eigenschaften. Diese Profile sollen Krypto zu erfassen
70
Algorithmus Anforderungen von Geräten und Anwendungen eingeführt , wo leichte Kryptographie
71
erforderlich. NIST werden Profile in diese basierend auf Community Antworten auf die Fragen, enthalten entwickeln
72
berichten, über Anwendungs- und Geräteanforderungen für leichte Kryptographie.
73

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
iv
Inhaltsverzeichnis
74
75

76

77
2
Überblick über Leichtbau Cryptography 2
78
2.1 Ziel Devices..... 2
79
2.2 Performance Metrics 3
80
2.2.1 Hardware-spezifische Metriken 3
81
2.2.2 Software-spezifische Metriken 4
82
2.3 Leichte kryptographischer Primitive 4
83
2.3.1 Leichte Blockchiffren 4
84
2.3.2 Leichte Hash - Funktionen 5
85
2.3.3 Leichte Message Authentication Codes 6
86
2.3.4 Leichte Stromchiffren 6
87
2.4 NIST genehmigte kryptographischer Primitive in Umgebungen mit beschränktem 6
88
2.5 Leichte Cryptography Standards 7
89
3
NIST Leichte Cryptography Projekt 9
90
3.1 Umfang und Design - Überlegungen 9
91
3.1.1 Allgemeine Überlegungen zum Entwurf 9
92
3.2 Profiles..... 11
93
3.2.1 Profil Entwicklung 11
94
3.2.2 Profilvorlage und Beispielprofile 13
95
3.3 Evaluierungsprozess 15
96
References.....17
97
98

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON

L
IGHTWEIGHT
C
RYPTOGRAPHY
1
1
Einführung
99
Der Einsatz von kleinen EDV - Geräte wie RFID - Tags, Industriesteuerungen, Sensor
100
Knoten und Smartcards ist viel mehr üblich. Die Verlagerung von Desktop - Computern
101
kleine Geräte bringt eine breite Palette an neuen Sicherheits- und Datenschutzbedenken. Es ist eine Herausforderung an
102
herkömmliche Standards für kleine Geräte. In vielen herkömmlichen Verschlüsselungsstandards,
103
der Kompromiss zwischen Sicherheit, Leistung und Ressourcenbedarf wurde für Desktop - optimiert
104
und Server - Umgebungen, und das macht sie schwer oder gar nicht zu realisieren in ressourcen-
105
erzwungener Geräte. Wenn sie umgesetzt werden können, können ihre Leistung nicht akzeptabel.
106
Leichte Kryptographie ist ein Teilgebiet der Kryptographie , die Lösungen bieten soll zugeschnitten
107
für ressourcenbeschränkte Geräte. Es hat getan , eine erhebliche Menge an Arbeit durch den
108
akademischen Gemeinschaft zu leichten Kryptographie im Zusammenhang; Dazu gehören effiziente
109
Implementierungen von herkömmlichen Verschlüsselungsstandards, und das Design und die Analyse neuer
110
leichte Primitiven und Protokolle.
111
Im Jahr 2013 initiierte NIST eine leichte Kryptographie Projekt die Leistungsfähigkeit der Studie
112
aktuelle NIST genehmigte Verschlüsselungsstandards auf begrenzten Geräten und zu verstehen , die
113
müssen für leichte Kryptographiestandards gewidmet und wenn der Bedarf festgestellt wird, zu entwerfen ein
114
transparentes Verfahren für die Standardisierung. Im Jahr 2015 hielt NIST die erste Leicht Cryptography

115
Workshop in Gaithersburg, MD, öffentliche Feedback zu den Einschränkungen und Grenzen des zu bekommen
116
Zielgeräte und Anforderungen und Eigenschaften von realen Anwendungen von leichten
117
Kryptographie.
[1]
118
Vor kurzem hat NIST entschieden , ein Portfolio von leichten Primitiven durch eine offene erstellen
119
Verfahren ähnlich der Auswahl der Betriebsmodi des Blockchiffren [48] . In diesem Bericht haben wir
120
Ziel ist die Feststellung des leichten Kryptographie Projekt zusammenzufassen und NIST Pläne umreißen
121
für die Standardisierung von leichten Primitiven. Dieser Bericht enthält auch eine Liste von Fragen zu
122
die Akteure von leichten Kryptographie, die als Grundlage dienen für die Bestimmung
123
Anforderungen. Die Antworten auf die Fragen sollten geschickt werden mit der zu lightweight-crypto@nist.gov~~V
124
Betreffzeile "Antworten auf Fragen zu leichten Krypto - Anforderungen" vor dem 1. Oktober
125
2016.
126
Der Rest dieses Berichts ist wie folgt aufgebaut . Sectio n 2 gibt einen Überblick über
127
leichte Kryptographie, einschließlich Metriken und Entwicklungen. Abschnitt 3 liefert Informationen
128
über leichte Kryptographieprojekt NIST, einschließlich der vorgeschlagenen Weg für die
129
Standardisierung von leichten Algorithmen, Design - Überlegungen und eine Profilvorlage das wird
130
im Auswertungsverfahren verwendet werden.
131
132
1
Für Workshop - Präsentationen, besuchen http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm .

R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
2
2
Überblick über Leichtbau Cryptography
133
In diesem Abschnitt werden verschiedene Aspekte der leichten Kryptographie, einschließlich Zielgeräten,
134
Performance - Metriken, Anwendungen und spezielle Designs.
135
2.1
Zielgeräte
136
Leichtbau Kryptografie zielt auf eine Vielzahl von Geräten , die auf einem breiten implementiert werden kann
137
Spektrum von Hardware und Software. Am oberen Ende der Vorrichtung Spektrums Server und
138
Desktop - Computer von Tablets und Smartphones gefolgt. Herkömmliche Verschlüsselungsalgorithmen
139
gut in diesen Geräten können; Daher können diese Plattformen nicht leichte erfordern
140
Algorithmen. Schließlich, am unteren Ende des Spektrums sind Vorrichtungen , wie beispielsweise eingebettete Systeme,
141
RFID - Geräte und Sensornetzwerke. Leichte Kryptographie ist in erster Linie konzentrierte sich auf die hoch
142
gelegten Vorrichtungen , die in dem unteren Ende des Spektrums zu finden sind.
143
Server und Desktops
konventionell
Geheimschrift
Tablets und Smartphones
Eingebettete Systeme
Leicht
Geheimschrift
RFID und Sensornetzwerke
144
Mikrocontroller sind mit einer Vielzahl von Leistungsmerkmalen zur Verfügung. Obwohl 8-bit, 16-bit
145
und 32-Bit - Mikrocontroller sind die häufigsten, gibt es erhebliche Umsatz von 4-Bit
146

Mikrocontroller für bestimmte Ultra-Low - Cost - Anwendungen. Eine Vielzahl von Befehlssätzen vorhanden ist ,
147
typischerweise nur einfache Befehle unterstützt werden , und die Anzahl der Befehle ist oft sehr
148
begrenzt. Dies kann in einer hohen Anzahl von Zyklen führen gemeinsame Verschlüsselungs auszuführen
149
Algorithmen, die sie zu langsam oder energieaufwendig für die beabsichtigte Anwendung machen kann.
150
Dies ist insbesondere dann ein Problem , wenn es notwendig ist , Echtzeitbedingungen zu erfüllen unter Verwendung eines begrenzten
151
Menge an Energie.
152
Für einige Mikrocontroller, kann die Menge an RAM und ROM extrem begrenzt. Für
153
Beispiel der TI COP912C [62] Hat 64 Bytes RAM und der NXP RS08 [52] kann so wenig haben
154
als 63 Byte RAM. Der Microchip PIC10 / 12/16 - Mikrocontroller [45] Gibt es in vielen Varianten
155
mit 64 Byte RAM und weniger, gehen so wenig wie 16 Byte RAM nach unten.
156
Auf der Unterseite des Spektrums gibt es RFID und Sensornetzwerke, die in oft realisiert
157
Hardware (ASIC), um einige der strengsten Umsetzung Einschränkungen zu erfüllen. Von
158
Besonders interessant sind UHF - RFID - Tags, zum Beispiel die weit verbreitete EPCGlobal Gen2 mit
159
[22] Und ISO / IEC 18.000 bis 63 [39] Standards.
160
Für RFID - Tags , die nicht batteriebetrieben sind, wird nur eine begrenzte Menge an Energie von der zur Verfügung
161
Umwelt. Solche Vorrichtungen erfordern Kryptographiealgorithmen , die nicht nur durchgeführt werden
162
eine sehr kleine Menge von Gate - Äquivalenten (GES), aber müssen strenge Timing und Leistung erfüllen
163
Abbildung 1 Gerätespektrum

Wünsche. Eine Studie der Einschränkungen solcher Vorrichtungen für kryptographische Anwendungen
164
in wurde durchgeführt [57] .
165
Leichte Algorithmen können auf verschiedene andere Beschränkungen unterliegen, ein Thema , das untersucht werden
166
während der ersten Phase des Standardisierungsbemühungen. Die vorgenannten Beispiele sind deswegen
167
nicht abschließende Aufzählung zu verstehen sein, aber die Einstellungen zu veranschaulichen , wo herkömmliche Algorithmen können nicht
168
umgesetzt werden, um die Notwendigkeit für leichte Alternativen zu verstehen.
169

2.2 Performance Metrics

170
In Kryptografiealgorithmus Design, gibt es einen Kompromiss zwischen der Leistung und den Ressourcen
171
für eine bestimmte Sicherheitsstufe erforderlich. Die Leistung kann in Begriffen wie Macht ausgedrückt werden und
172
Energieverbrauch, Latenzzeit und Durchsatz. Die Mittel für eine Hardware erforderlich
173
Implementierung werden in der Regel in Gate - Bereich, Gatteräquivalenten oder Scheiben zusammengefasst. In der Software dieser
174
wird im Register, RAM und ROM Nutzung wider. Ressourcenbedarf werden manchmal bezeichnet
175
die Kosten, da mehr Tore oder Hinzufügen von Speicher dazu neigt , die Herstellungskosten der Vorrichtung zu erhöhen.
176
Strom- und Energieverbrauch relevant Metriken aufgrund der Natur vieler eingeschränkt
177
Geräte. Leistung kann in Vorrichtungen von besonderer Bedeutung sein , die Energie aus ihrer Ernte
178
Umgebung. Ein Beispiel dafür wäre ein RFID - Chip sein, der das elektromagnetische Feld verwendet übertragen
179

von einem Lesegerät seine interne Schaltung zu versorgen. Energieverbrauch (dh Energieverbrauch über eine
180
bestimmten Zeitraum) ist besonders wichtig bei batteriebetriebenen Geräten , die einen festen Betrag haben
181
der gespeicherten Energie. Die Batterien in einigen Geräten kann es schwierig oder unmöglich sein , zu laden oder
182
ersetzen einmal im Einsatz. Es sollte auch angemerkt werden , dass der Energieverbrauch von vielen Faktoren abhängt,
183
die Taktfrequenz und die Technologie für die Implementierung wie die Schwellenspannung ist , verwendet.
184
Latenz ist besonders relevant für bestimmte Echtzeit - Anwendungen, beispielsweise Automobil
185
Anwendungen , bei denen sehr schnelle Reaktionszeiten für Komponenten wie Lenkung, Bremsen oder Airbags
186
sind erforderlich. Es kann als das Maß der Zeit zwischen dem anfänglichen Anforderung einer Operation definiert werden und
187
Herstellung des Ausgangs. Zum Beispiel ist die Latenz einer Verschlüsselungsoperation die Zeit zwischen
188
die ursprüngliche Anforderung für die Verschlüsselung eines Klar- und die Antwort, die die entsprechenden zurückgibt
189
Geheimtext.
190
Der Durchsatz ist die Geschwindigkeit , mit der neue Ausgaben (zB Authentifizierung Tags oder Chiffretext) sind
191
hergestellt. Im Gegensatz zu herkömmlichen Primitiven werden, darf nicht mit hohem Durchsatz Ziel ein Design - in
192
Leichtbau. Allerdings wird mit einem moderaten Durchsatz noch in den meisten Anwendungen erforderlich ist .
193

2.2.1 Hardwarespezifische Metrics

194
Ressourcenanforderungen für Hardware - Plattformen werden typischerweise in Bezug auf die Gate - Bereich beschrieben. Das
195
Bereich einer Implementierung hängt von der Technologie und der Standardzellenbibliothek und ist
196
gemessen in *& mgr; m*

2
. Die Umgebung kann in Form von Scheiben für FPGAs angegeben werden oder durch *Gatteräquivalenten* (GES)
197
für ASIC - Implementierung.
198
Auf FPGAs, ist ein Stück der Grund rekonfigurierbare Einheit, die eine Reihe von Look-up - Tabellen enthält
199
(LUTs), Flip-Flops und Multiplexer. Scheiben sind unterschiedlich auf verschiedene FPGAs implementiert. Das
200

4
Anzahl von LUTs, Flip-Flops und Multiplexer hängt von der FPGA - Familie, sowie der Zahl
201
der Eingangs- und Ausgangsbits des LUTs.
202
Für ASICs, ist eine GE auf den Bereich äquivalent, der von den zwei Eingängen NAND - Gatter erforderlich. Das
203
Bereich in GE wird durch Teilen der Fläche in *& mgr; m* erhalten
2
durch die Fläche des NAND - Gatters. Die Anzahl der
204
GEs einer Hardware - Implementierung ist daher sehr spezifisch für eine bestimmte Technologie, so dass es
205
nicht möglich ist , direkt die Anzahl der GEs von Implementierungen in unterschiedlichen vergleichen ,
206
Technologien.
207
Eine kostengünstige RFID - Tag kann eine Gesamtgatterzahl von 1.000-10.000 Tore, von denen nur 200-
208
2000 kann für Sicherheitszwecke verwendet werden [41]. Flächenbedarf und Stromverbrauch kann
209
korreliert, wobei in diesem Fall die Minimierung Bereich neigt auch dazu , den Stromverbrauch zu reduzieren.

210
2.2.2
Software-spezifische Metriken
211
Für Softwareanwendungen können Ressourcenanforderungen durch die Anzahl der Register gemessen werden, wie
212
und die Anzahl von Bytes von RAM und ROM , die erforderlich sind. Funktionen , die eine kleine verwenden
213
Anzahl der Register haben eine niedrigere Overhead - Aufruf, wie müssen weniger Variablen auf die gesetzt werden
214
stapeln , bevor die Register überschrieben werden. ROM wird verwendet , um den Programmcode zu speichern und können
215
sind feste Daten, wie zum Beispiel S-Boxen oder hartcodierte runden Tasten, während RAM zu speichern , verwendet wird ,
216
Zwischenwerte , die in Berechnungen verwendet werden können. Dies kann zu weiteren Kompromissen führen
217
zwischen den Werten on the fly im Vergleich zu der oben schaut Werte in einer Tabelle zu berechnen.
218
2.3
Leichte Cryptographic Primitives
219
Im letzten Jahrzehnt eine Reihe von leichten Krypto - Primitiven (einschließlich Blockchiffren, Hash
220
Funktionen, Nachrichtenauthentifizierungscodes und Stromchiffren) wurden zu bringen vorgeschlagen
221
Leistungsvorteile gegenüber herkömmlichen Verschlüsselungsstandards. Diese unterscheiden sich von Primitiven
222
herkömmliche Algorithmen mit den Annahmen , dass leichte Primitive sind nicht für eine beabsichtigte
223
breite Palette von Anwendungen, und verhängen können Grenzen für die Kraft des Angreifers. Beispielsweise die
224
Menge der verfügbaren Daten an den Angreifer unter einer einzigen Taste kann begrenzt werden. Jedoch sollte es sein ,
225
stellte fest , dass dies nicht bedeutet , dass die leichten Algorithmen schwach sind - eher die Idee zu verwenden ,
226
Fortschritte in der Ausführung mit einem besseren Gleichgewicht zu führen zwischen Sicherheit, Leistung und

227
Ressourcenanforderungen für spezifische ressourcenbeschränkte Umgebungen.
228
2.3.1
Leichte Blockchiffren
229
Eine Reihe von leichten Blockchiffren wurden zu erreichen Leistungsvorteile vorgeschlagen
230
über NIST Advanced Encryption Standard (AES) [63], Insbesondere AES-128. Einige davon
231
Chiffren wurden durch die Vereinfachung der herkömmlichen entworfen, gut analysiert Blockchiffren ihre zu verbessern
232
Effizienz. Als Beispiel DESL [42] Ist eine Variante des DES, wo die Rundungsfunktion eine nutzt
233
einzelne S-Box anstelle von acht und lässt die erste und letzte Permutationen die Größe zu verbessern
234
die Hardware - Implementierung. Alternativ sind einige der Algorithmen dedizierten Blockchiffren
235
dass wurden von Grund auf neu gestaltet. GESCHENK [8] Ist einer der ersten, leichten Blockchiffre
236
Entwürfe , die für eingeschränkte Hardware vorgeschlagen Umgebungen wurde. SIMON und SPECK [6] sind
237
Familien aus leichtem Blockchiffren, die als gut einfach, flexibel und durchführen entworfen wurden
238

---

in Hard- und Software. Es gibt Algorithmen auch aus der 1990er Jahre wie RC5 [56], TEA [68] und
239
XTEA [51], Die aus einfachen runden Strukturen bestehen, die sie geeignet für eingeschränkte machen
240

Software - Umgebungen. Eine nicht erschöpfende Liste von leichten Blockchiffren in bereitgestellt [67] .
241
Die Performance - Vorteile von leichten Blockchiffren gegenüber herkömmlichen Blockchiffren sind
242
mit leichten Design - Entscheidungen erreicht, wie zum Beispiel:
243
- Kleinere Blockgrößen: Um Speicherplatz zu sparen, leichte Blockchiffren verwenden kleinere Block
244
Größen als AES (zB 64 oder 80 Bits, statt 128). Es sollte auch , dass die Verwendung zu beachten ,
245
kleinen Blockgrößen reduziert Grenzen für die Länge der Klartexte verschlüsselt werden. Für
246
Beispiel Ausgänge eines 64-Bit - Blockchiffre aus einer Zufallssequenz unterschieden werden
247
mit etwa 2
32
Blöcke für einige der zugelassenen Betriebsarten. Abhängig von
248
Algorithmus, kann dies zu Klartextrückgewinnung, die Schlüsselwiederherstellung oder Authentifizierung Tag führen
249
Fälschungen mit nicht zu vernachlässigenden Wahrscheinlichkeiten.
250
- Kleinere Schlüsselgrößen: Einige leichte Blockchiffren verwenden kleine Schlüsselgrößen (weniger als 96 Bit)
251
Effizienz (zB 80-Bit vorhanden ist). Zum Zeitpunkt des Schreibens dieses Artikels, die Mindestschlüsselgröße
252
erforderlich durch NIST ist 112 Bits [4] .
253
- Einfachere Runden: Die Komponenten und Vorgänge im Leichtbau Blockchiffren verwendet werden ,
254
typischerweise einfacher als jene von herkömmlichen Blockchiffren. In Leichtbauweise mit
255
S-Boxen, 4-Bit - S-Boxen sind bevorzugt über 8-Bit - S-Boxen. Diese Verringerung der Größe führt zu
256
erhebliche Flächeneinsparung. Zum Beispiel benötigt der 4-Bit - S-Box in der Gegenwart verwendet 28GEs,
257
während AES S-Box erforderlich 395 GEs in [20]. Für Hardware-orientierten Designs, Bit
258
Permutationen (wie sie in derzeit verwendeten) oder rekursive MDS - Matrizen (wie in

259
PHOTON [23] Und LED [24]) Können über komplexe lineare Schichten bevorzugt werden. Wenn Runden
260
sind einfacher, können sie brauchen , um mehrmals wiederholt werden , um Sicherheit zu erreichen.
261
- Einfachere Schlüsselpläne: Komplexe Schlüsselpläne erhöhen die Speicher - Latenz und die
262
Stromverbrauch von Implementierungen; Daher werden die meisten der leichten Blockchiffren
263
verwenden einfache Schlüssel Pläne , die Unterschlüssel on the fly generieren können. Dies kann Angriffe ermöglichen
264
mit bezogene Schlüssel, schwache Schlüssel, bekannt Tasten oder sogar gewählte Schlüssel. Wenn dies der Fall ist , es
265
um sicherzustellen , ist erforderlich , dass alle werden einen sicheren Schlüssel unabhängig Schlüssel erzeugt mit
266
Ableitungsfunktion (KDF) [10 , 11 , 14 , 60] .
267
2.3.2
Leichte Hash - Funktionen
268
Herkömmliche Hash - Funktionen können nicht für Umgebungen mit beschränktem geeignet sein, vor allem wegen
269
ihrer großen inneren Zustand Größen und hohe Stromverbrauchsanforderungen. Dies hat zu der LED
270
Entwicklung leichter Hash - Funktionen, wie beispielsweise PHOTON [23], Quark [2] SPONGENT [7] ,
271
und Lesamnta-LW [26]. Die erwartete Nutzung von konventionellen und leichten Hash-Funktionen
272
unterscheidet sich in verschiedenen Aspekten , wie beispielsweise [54] :
273
- Kleinere interne Zustand und Ausgangsgrößen: Große Ausgabegrößen sind wichtig für Anwendungen
274
die erfordern Kollisionsresistenz von Hash - Funktionen. Für Anwendungen , die erfordern keine
275
Kollision Widerstand, kleinere interne und Ausgangsgrößen verwendet werden könnten. Wenn ein kollisions
276

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
6
beständige Hashfunktion erforderlich ist, kann es akzeptabel sein , dass diese Hash - Funktion hat die
277
gleiche Sicherheit gegen Urbild, Second-Urbild und Kollisionsangriffe. Dies kann zu reduzieren
278
die Größe des internen Zustands.
279
- Kleinere Nachrichtengröße: Herkömmliche Hash - Funktionen werden voraussichtlich Eingänge unterstützen mit
280
sehr große Größen (etwa 2
64
Bits). In den meisten der Ziel Protokolle für leichte hash
281
Funktionen sind typische Eingangsgrößen viel kleiner (beispielsweise höchstens 256 Bits). Hash - Funktionen
282
dass deshalb kann für kurze Nachrichten optimiert sind besser geeignet für den Leichtbau
283
Anwendungen.
284

2.3.3 Leichte Message Authentication Codes

285
Ein Message Authentication Code (MAC) ein Tag aus einer Nachricht und einem geheimen Schlüssel, das ist
286
verwendet , um die Authentizität der Nachricht zu überprüfen. Tag Größen werden empfohlen , mindestens 64 Bit zu sein
287
für typische Anwendungen. Für bestimmte Anwendungen wie VoIP (Voice over IP), gelegentlich
288
kann nur begrenzte Auswirkungen eine unecht Nachricht akzeptieren auf die Sicherheit der Anwendung, so
289
dass kürzere Tags können nach sorgfältiger Abwägung eingesetzt werden. Chaskey [47], Tulp [21], und
290

LightMAC [43] Sind einige der Beispiele für Leichtbau MAC-Algorithmen.
291
2.3.4
Leichte Stromchiffren
292
Stromchiffren sind ebenfalls vielversprechende Primitiven für Umgebungen mit beschränktem. Die eSTREAM
293
Wettbewerb [19], Die von der Europäischen Exzellenznetzwerk für Kryptologie organisiert, richtet zu
294
Identifizierung neuer Stromchiffren , die für die weit verbreitete Annahme geeignet sein könnten. Die Finalisten des
295
Wettbewerb wurden im Jahr 2008 und umfasste drei Stromchiffren für Hardware - Anwendungen angekündigt
296
mit eingeschränkten Ressourcen:
297
- *Getreide* [25] wird allgemein analysiert und liefert die Umsetzung Flexibilität, und hat auch eine
298
Version , die Authentifizierung unterstützt.
299
- *Trivium* [15] ist eine weit analysiert, elegant und flexibles Design; jedoch nur unterstützt
300
80-Bit - Schlüssel.
301
- *Mickey* [3] ist weniger analysiert im Vergleich zu Getreide und Trivium, und seine Sicherheit meist
302
ist abhängig von der Härte der Analyse. Es bietet weniger Flexibilität und Implementierung
303
anfällig für Timing und Power - Analyse, aufgrund unregelmäßiger Taktung.
304
2.4
NIST genehmigte kryptographischer Primitive in Umgebungen mit **beschränktem**
305
In diesem Abschnitt wird die Leistung von NIST genehmigte Verschlüsselungsstandards in ressourcen-
306
Umgebungen mit beschränktem.
307

IGHTWEIGHT
C
RYPTOGRAPHY
7
- ***Blockchiffren:*** Es gibt zwei NIST genehmigte Blockverschlüsselungsalgorithmen; AES und Triple
308
DES (TDEA) [5] .
2
Die AES - Familie von Blockchiffren umfasst drei Varianten AES-128,
309
AES-192 und AES-256 , die Schlüsselgrößen von 128, 192 und 256 Bit unterstützen, beziehungsweise. Alle
310
AES - Varianten arbeiten mit einer Blockgröße von 128 Bit aufweisen. Für leichte Kryptographie
311
das am besten geeignete Variante der Familie Zwecke ist AES-128, durch die Anzahl der Runden
312
und die Größe des Schlüsselplan. Bestehende kompakte Implementierungen von AES-128 erfordern
313
2090 GEs [44] Bis 2400 GEs [46]. AES ist vor allem für Software-Anwendungen.
314
Bei Verwendung von 8-Bit - AVR - Mikrocontroller, Verschlüsselung ist in Zyklen pro Byte 124,6 erreicht
315
und Entschlüsselung in 181,3 Zyklen pro Byte, mit einer Codegröße von weniger als 2 Kbyte [53]. AES
316
führt sehr gut auf bestimmte 8-Bit - Mikrocontroller, hat es eine gute Wahl für diejenigen,
317
Plattformen. Beide Ver- und Entschlüsselungsvorgänge in Blockchiffren wie AES und
318
Triple-DES kann nicht auf einem Renesas RL78 16-Bit - Mikrocontroller [implementiert werden 55] wann
319
die Menge des ROM ist auf 512 Bytes beschränkt und RAM ist auf 128 Bytes begrenzt [13]. Für
320
wo Anwendungen die Leistung von AES akzeptabel ist, sollte AES verwendet werden für
321
Verschlüsselung.
322
- ***Hash*** - ***Funktionen:*** NIST genehmigte Hash - Funktionen sind in zwei FIPS - Standards festgelegt:
323
FIPS 180-4 [65] Gibt SHA-1,
3
der SHA-2 - Familie (nämlich, SHA-224, SHA-256,

SHA-384, SHA-512, SHA-512-224 und SHA-512/256) und FIPS 202 [66] Gibt die Permutation-basierte SHA-3 - Familie (nämlich SHA3-224, SHA3-256, SHA3-384 und SHA3-512). Keine dieser zugelassenen Hash - Funktionen sind für den Einsatz in sehr Umgebungen mit , vor allem wegen ihrer großen inneren Zustandsgröße Anforderungen. Ideguchi et al. [27] Untersuchten die RAM-Anforderungen von SHA-256, SHA-512 und verschiedene SHA-3 - Kandidaten auf Low-Cost - 8-Bit - Mikrocontroller, und stellte fest , dass keine der NIST zugelassenen Hash - Funktionen innerhalb 64 Byte RAM implementiert werden. Die interne Zustandsgröße für die Familie SHA-3 wird hauptsächlich durch die Breite des zugrunde liegenden bestimmt 1600-Bit - Permutation. FIPS 202 definiert zusätzlich kleinere Permutationen mit Größen 25, 50, 100, 200, 400 und 800; einige dieser Varianten später verwendet werden können , zu definieren , leichte Varianten von SHA-3, aber derzeit diese kleineren Varianten sind nicht zugelassen für den Einsatz in Hash - Funktionen.

- ***Authentifizierte Verschlüsselung und MACs:*** authentifizierte Verschlüsselung bietet Leistung und Vorteile Ressourcenbedarf, denn es bietet gleichzeitig Vertraulichkeit und Schutz der Integrität von Nachrichten. NIST genehmigt den CCM [16] Und GCM [18] Block Chiffre - Modi , die gleichzeitig die Authentifizierung und Verschlüsselung zur Verfügung stellen. NIST auch genehmigt Standalone - MACs, CMAC [17], GMAC [18] Und HMAC [64], Um verwendet werden für Erzeugen und Nachrichtenauthentifizierung zu überprüfen.

2.5

Leichte Cryptography Standards

ISO / IEC 29192, *leicht Cryptography,* ist ein sechsteilige Standard, der leicht spezifiziert

Ein dritter Block - Chiffre, Bonito, ist nur für Legacy-Anwendung Entschlüsselung genehmigt. Siehe [SP800-131A] für weitere Informationen.
3
SHA-1 ist nicht für alle gängigen Anwendungen einer Hash - Funktion freigegeben. [4] Siehe für weitere Details.

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
8
Verschlüsselungsalgorithmen für die Vertraulichkeit, Authentifizierung, Identifizierung, Nachweisbarkeit und
345
Schlüsselaustausch. Teil 1 [28] enthält allgemeine Informationen wie Sicherheit, Klassifizierung und Bewertung
346
Anforderungen für die Umsetzung. Teil 2 gibt den Blockchiffren PRESENT und CLEFIA [29] .
347
Teil 3 gibt die Stromchiffren Enocoro und Trivium [ISO29192-3]. Teil 4 gibt drei
348
nämlich asymmetrische Techniken *(i)* Identifikationsschema cryptoGPS, *(ii)* die Authentifizierung und Schlüssel
349
Austauschmechanismus ALIKE, und *(iii)* ID-basierten Signaturschema IBS [30]. Teil 5 legt fest,
350
drei Hash - Funktionen: PHOTON, SPONGENT und Lesamnta-LW [40]. Teil 6 widmet sich der
351
MACs und befindet sich derzeit in der Entwicklung.
352
ISO / IEC 29167, *Automatische Identifikation und Datenerfassungsverfahren*, bietet Sicherheit
353
Services für RFID - Luftschnittstellenkommunikation. Teil 1 [31] beschreibt die Architektur, Sicherheit
354
Merkmale und Anforderungen für die Sicherheitsdienste für RFID - Geräte. Crypto Suiten sind definiert in
355
zusätzliche Teile. Derzeit sind sieben Suiten veröffentlicht in [32-38]. Weitere Dokumente sind
356

in Entwicklung.
357
Cryptography Research and Evaluation Committees (Cryptrec) ist ein Projekt zu bewerten und
358
Sicherheit kryptographischer Techniken überwachen in der japanischen E-Government - Systemen verwendet [12] .
359
Cryptrec veröffentlicht drei Arten von Chiffre Listen: E-Government Empfohlen Chiffren List,
360
Candidate Empfohlen Chiffren Liste und Wachte Chiffren Liste. Der Leichtbau
361
Cryptography Arbeitsgruppe von Cryptrec, im Jahr 2013 gegründet, zielt darauf ab , zu studieren und zu unterstützen
362
geeignete leichte Kryptografie - Lösungen für E-Government - Systeme und alle Anwendungen
363
wo Leichtbaulösungen benötigt werden . Die Arbeitsgruppe Durchführung einer Marktforschung über Stand der Technik in
364
leichte Kryptographie und deren Anwendungen und führt die Umsetzung Auswertungen und
365
einen Bericht (auf Japanisch) veröffentlicht [13] Als lieferbar im Jahr 2015. Die Ziel Algorithmen für
366
Umsetzung im Bericht waren AES, Camellia [1], CLEFIA [59], PRESENT [8], LED [24] ,
367
Piccolo [58], TWINE [61] Und PRINCE [9] .
368

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
9

3

NIST Leichte Cryptography Projekt

369
NIST - Standards entwickelt verschiedene Ansätze verwendet, wie beschrieben in [50]. NIST hat entschieden
370

Wettbewerbe mit dem AES - Blockchiffre und die SHA-3 - Hash - Funktionen auszuwählen. Diese Wettbewerbe
371
erhebliche Anstrengungen waren, die sich über viele Jahre in Anspruch nahm. Zum Beispiel Wettbewerb der SHA-3
372
im Jahr 2007 bekannt gegeben wurde, wurde der Sieger im Jahr 2012 angekündigt, und der Normungsprozess war
373
abgeschlossen im Jahr 2015 ist ein weiterer Ansatz Standards anderer anerkannten Standards anzupassen
374
Entwicklungsorganisationen, wie es mit HMAC und RSA - Standards durchgeführt. NIST - Forscher auch
375
Entwicklung von Standards und Richtlinien in Zusammenarbeit mit Experten aus Wissenschaft, Industrie und
376
Regierung, wenn kein passender Standard existiert.
377
Die Landschaft für leichte Kryptographie bewegt sich so schnell , dass ein Standard unter Verwendung hergestellt
378
das Wettbewerbsmodell ist wahrscheinlich vor der Standardisierung überholt zu sein. Daher ist die am meisten
379
geeigneter Ansatz für leichte Kryptographie, in Bezug auf die Timeline und Projektziele, ist zu
380
neue Empfehlungen entwickeln eine offene Aufforderung zur Einreichung von Vorschlägen unter Verwendung von Algorithmen zu standardisieren.
381
NIST plant ein Portfolio von leichten Primitiven und Modi zu entwickeln und zu pflegen , dass
382
sind für den begrenzten Einsatz zugelassen. Jeder Algorithmus im Portfolio wird auf ein oder mehrere *Profile* gebunden werden,
383
die aus Algorithmus Ziele und akzeptablen Bereiche für Metriken. Dies steht im Gegensatz zu anderen
384
Primitiven und Modi , die für den allgemeinen Gebrauch zugelassen sind. Jede Einschränkung der Anwendung werden ebenfalls behandelt werden
385
in der Empfehlung oder Standard, in dem die Primitiven und Modi des Portfolios angegeben sind.
386
Algorithmus Übergänge und deprecation Leitlinien werden als Algorithmen im Portfolio zur Verfügung gestellt werden
387
auslaufen. Das leichte Portfolio ist nicht alternative Algorithmen zu bieten, die für

388
allgemeiner Gebrauch.
389
3.1
Überlegungen Scope and Design
390
Der Umfang der NIST leichte Kryptographie Projekt umfasst alle kryptographischer Primitive und
391
Modi, die in Umgebungen mit beschränktem benötigt werden. Der anfängliche Schwerpunkt des Projekts ist jedoch
392
auf Blockchiffren, Hash-Funktionen und Nachrichtenauthentifizierungscodes. Wenn langfristige Sicherheit ist
393
benötigt wird, sollte diese Algorithmen entweder Ziel für Post-Quantum Sicherheit [49] , oder die Anwendung
394
sollte es ihnen ermöglichen, durch Algorithmen mit Post-Quantum Sicherheit leicht austauschbar zu sein.
395
Während Kryptographie mit öffentlichem Schlüssel wird in der Ausgangsfokus enthalten, ist es im Rahmen dieser
396
Projekt. Es sollte jedoch, dass Public-Key-Systeme werden nur dann berücksichtigt werden, zu beachten, für
397
Aufnahme in das Portfolio unter zwei Bedingungen: 1) sie robust gegenüber Quanten Angriffe sind, oder 2)
398
verwenden eine Kombination aus allgemeinen öffentlichen Schlüssel Verschlüsselungssysteme mit leichten Primitive (zB
399
leichte Hash-Funktion). Protokoll-Design ist auch ein wichtiger Teil der gewünschte erreichen
400
Maß an Sicherheit, während Anforderungen einer eingeschränkten Umgebung zu erfüllen, ist aber nicht innerhalb der
401
Rahmen dieses Projekts.
402
3.1.1
Allgemeine Überlegungen zum Entwurf
403
Während spezifische Anforderungen durch Anwendung variieren, gibt es mehrere allgemein gewünschten Eigenschaften
404
dass NIST verwenden werden Entwürfe zu bewerten.
405

FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
10
- ***Sicherheit Stärke*** : Jeder Algorithmus für das Portfolio ausgewählt werden, müssen eine ausreichende Sicherheit bieten.
406
Genauer gesagt, sollte die Sicherheitsstärke mindestens 112 Bit betragen.
407
- ***Flexibilität*** : Effiziente Implementierungen eines Algorithmus sollte möglich sein , über eine
408
Sortiment von Plattformen. Algorithmen sollte auch eine Vielzahl von Implementierungen auf ein erlauben
409
Plattform. Tunable-Algorithmen, die Parameter verwenden, um Eigenschaften wie Zustand
410
Größe und die Schlüsselgröße, sind wünschenswert, da sie Implementierungen mit mehreren Optionen erlauben mit
411
weniger Ressourcen als mehrere Algorithmen, die Logik nicht teilen und unterstützt damit eine breitere
412
Array von Anwendungen.
413
- ***Geringer Aufwand für mehrere Funktionen*** : Mehrere Funktionen (wie zB Verschlüsselung und
414
Entschlüsselung), die den gleichen Kern teilen werden über Funktionen bevorzugt, die vollständig haben
415
andere Logik. Zum Beispiel wird eine Blockchiffre wobei die Verschlüsselungs- und Entschlüsselungsoperationen
416
verwenden ähnliche Rundenfunktionen können über ein vorzuziehen sein, die unterschiedliche Runde Funktionen für
417
Verschlüsselung und Entschlüsselung. Verschiedene Primitive, wie beispielsweise eine Hash-Funktion und die Blockchiffre,
418
kann auch eine Logik teilen, wodurch die Ressourcen zu reduzieren benötigt mehrere Algorithmen zu implementieren, in
419
das gleiche Gerät.
420
- ***Ciphertext Expansion*** : Die Größe der verschlüsselten Text hat einen Einfluss auf die Speicherung und Übertragung

421
Kosten. Algorithmen und Modi, die nicht wesentlich die Menge der Daten erhöhe sind
422
wünschenswert.
423
- *Seitenkanal und Fehlerangriffe* : Implementationen können sensible Informationen auslaufen, insbesondere
424
Informationen über den Schlüssel oder Klartext, in einer Vielzahl von Möglichkeiten. Seitenkanalangriffe nutzen
425
Eigenschaften der Umsetzung während der Ausführung der kryptografischen Operationen, wie beispiels
426
Timing, Stromverbrauch und elektromagnetische Emissionen, diese empfindlich zu entdecken
427
Information. Fehlerangriffe erholen diese sensiblen Informationen durch Fehler in der Einführung
428
Berechnung. Im Falle der allgegenwärtigen Geräte ist dies besonders bemerkenswert, da Angreifer kann
429
haben physischen Zugriff auf die Geräte und Gegenmaßnahmen für solche Angriffe nicht vorhanden sein kann
430
aufgrund eingeschränkten Ressourcen. Algorithmen, die gegen Seitenkanal leicht zu schützen sind und
431
Fehlerangriffe sind wünschenswert.
432
- *Begrenzung der Anzahl von Klartext-Chiffretext - Paaren* : Es ist für Algorithmus zulässig sein kann ,
433
Designer eine obere von der Anzahl der Klartext / Chiffretext-Paaren, da diese Grenze gebunden zu übernehmen
434
kann für einige Anwendungen durch die Beschränkungen der Vorrichtungen (zB Beschränkungen gerechtfertigt werden
435
die Datenmenge, die durch den gleichen Schlüssel verarbeitet werden) oder Nachrichtenformate definiert durch
436
Protokolle. Es muß jedoch erkannt werden, dass ein Angreifer Angriffe montieren kann unter Verwendung von Klartext
437
dass unter mehreren unabhängigen Schlüsseln verschlüsselt (Multi-Key-Attacken), die relevant sind
438
selbst wenn die Menge der Daten unter einem einzelnen Schlüssel verschlüsselt ist begrenzt.
439

- ***Ähnliche schlüssel Angriffe*** : Diese Angriffe erlauben ein Widersacher Informationen über einen Schlüssel zu entdecken
440
von Operationen mit mehreren Tasten, die, obwohl unbekannt, haben eine bekannte Durchführung
441
Beziehung. Dies ist vor allem eine Bedrohung in Protokolle, bei denen die Schlüssel nicht gewählt unabhängig und
442
zufällig. Die Schlüssel können permanent in die Hardware von erzwungener Geräte verbrannt werden, mit
443
keineswegs von Ersatz. Wenn dies der Fall ist, dann im Zusammenhang mit Schlüssel Angriffe sind nur ein praktisches
444
Bedrohung, wenn ein Gegner mehrere Geräte erhalten, die Schlüssel mit einer bekannten Beziehung haben. Dies
445

11
Angriff Modell bleibt immer noch sehr relevant für Geräte, bei denen die Fähigkeit, den Schlüssel zu aktualisieren,
446
besteht. Die Algorithmen werden erwartet, einen gewissen Widerstand gegenüber nahe stehenden Schlüssel Angriffe zu bieten (zB
447
Angriffe erfordern große Anzahl verwandter Tasten).
448
Es kann nicht möglich sein, alle Eigenschaften zu erfüllen, insbesondere wenn diese die Ressourcen erhöht
449
jenseits dessen, was für eine gegebene Anwendung zur Verfügung steht. Noch für das Portfolio jeder Algorithmus ausgewählt
450
eine angemessene Sicherheit muss. Insbesondere sollte die Sicherheit gegen Schlüssel Recovery-Attacken
451
zumindest 112 Bits.
452

3.2 Profile

453
NIST werden Algorithmen auf Basis von Profilen zu bewerten und empfehlen, die aus einer Reihe von Design bestehen
454
Ziele, die physikalischen Eigenschaften von Zielgeräten, Leistungseigenschaften durch die auferlegte
455
Anwendungen und Sicherheitsmerkmale.
456
Cryptographic Primitive kann mit einer Vielzahl von Zielen konzipiert werden. Die Entscheidungen in
457
die Designziele können die verschiedenen Merkmale beeinflussen. Zunächst wird dieses Projekt auf Block konzentrieren
458
Chiffren, authentifizierte Verschlüsselungsverfahren, Hash-Funktionen und Nachrichtenauthentifizierungscodes.
459
Profile sollten auf Zielklassen von Geräten und Anwendungen entwickelt werden - nicht unbedingt
460
spezifische Anwendungen. Profile sollten in einer Vielzahl von Anwendungen nützlich sein. Das
461
Eigenschaften, die in den Profilen identifiziert wurden, zu richten sind:
462
Physikalische Eigenschaften
Leistungsmerkmale Sicherheitsmerkmale
Area (in GE)
Latenz (in Taktzyklen)
Mindestsicherheitsstärke (Bits)
Speicher (RAM / ROM)
Durchsatz (Zyklen pro Byte)
Angriff Modelle
Implementierungsart
(Hardware, Software oder
beide)
Power (uW)
Seitenkanalwiderstand
Anforderungen
463
Die Eignung eines Algorithmus hängt von den physikalischen Einschränkungen der Vorrichtung und die
464
Ziele Performance und Sicherheit durch die Anwendung auferlegt.
465
3.2.1
Profil Entwicklung
466
Wenn Profile für leichte Kryptographie Gebäude, die Zahlen, die die physische Ausdruck bringen,

467
Merkmale Leistung und Sicherheit, die einem bestimmten eingeschränkten Umgebung anwenden können
468
allein nicht aussagekräftig. Die Argumentation hinter ihnen muss auch verstanden werden.
469
Fragen zur Anwendungs- und Geräteanforderungen
470
Für die Entwicklung Profile, fragt NIST eine Reihe von Fragen an die Beteiligten von leichten
471

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
12
Kryptographie, um relevante Profile für eine Vielzahl von Anwendungen aufzubauen. Dies kann dazu beitragen,
472
erhalten ein umfassendes Verständnis für eine bestimmte Anwendung und die Engpässe zu identifizieren, oder sogar
473
zusätzliche Beschränkungen zu identifizieren, die nicht sofort sichtbar sind. Antworten auf die Fragen
474
sollte mit der Betreffzeile "Antworten auf Fragen geschickt auf lightweight-crypto@nist.gov~~V
475
leichte Krypto Anforderungen "vor 1. Oktober 2016.
476
Die Liste der Fragen ist wie folgt. Für eine Anwendungsumgebung gegeben, nicht alle Fragen können
477
gelten.
478
1. Was ist die Zielanwendung?
479
2. Welche Arten von Funktionen sind durch die Anwendung erforderlich ist (beispielsweise Verschlüsselung,
480
Authentifizierung, Hashing, Unterschriften, etc.)?
481
3. Sind alle Verschlüsselungsalgorithmen derzeit von der Anwendung verwendet? Wenn ja, welche
482

Algorithmen? Was die Wahl für diese Algorithmen motiviert? Wenn nicht, warum wurden bestimmte
483
Algorithmen als ungeeignet gefunden?
484
4. Sind die Algorithmen in erster Linie lokal (zB die direkte Kommunikation zwischen einem Tag verwendet und
485
ein Leser) oder über ein Netzwerk?
486
5. die Anwendung gegeben, wie schwierig es ist, einen Verschlüsselungsalgorithmus zu ersetzen?
487
6. Ist die Anwendung in erster Linie Hardware oder Software-Implementierung Ziel oder beide
488
ebenso relevant? Wenn ja, warum?
489
7. Wenn Software-Implementierungen sind relevant, welche Plattformen betrachtet werden (Server, Desktop,
490
Laptop, Smartphone, eingebettet, etc.)? Welche spezifischen Arten von Prozessoren (Anbieter und
491
Architektur) sind die wichtigsten Ziele?
492
8. Wenn Hardware-Implementierungen relevant sind, welche Arten von Hardware betrachtet werden
493
(FPGA, ASIC, etc.)? Welche spezifischen Plattformen sind unter Berücksichtigung (Anbieter,
494
Architektur, Technologie, Standard-Zellenbibliothek, etc.)?
495
9. Für Software-Implementierungen, die Ressourcen für die Verschlüsselungs verfügbar sind
496
Berechnung? Gibt es auf der Menge von Registern, RAM und ROM begrenzt, die
497
erhältlich? Wenn ja, welche technischen oder praktischen Erwägungen können diese Grenzen zu erklären?
498
10. Bei Hardware-Implementierungen gibt es auf die Menge an Scheiben oder GEs begrenzt, die
499
für die Umsetzung zur Verfügung? Wenn ja, welche technischen oder praktischen Erwägungen
500
können diese Grenzen zu erklären?
501
11. Ist die Plattform eine von Natur aus Serien ein oder können die Daten parallel verarbeitet werden?
502

12. Ist eine integrierte Unterstützung für Verschlüsselungsoperationen auf der Plattform zur Verfügung? (Hardware
503
Sicherheitsmodule, kryptographischer Anweisungen, kryptografisch sicheren Zufalls oder pseudo-
504
Zufallsbitgeneratoren?)
505
13. In dem Fall von Software-Implementierungen ist es notwendig, die Umsetzung zu verschleiern?
506
Wenn ja, warum?
507
14. ist Widerstand gegen Seitenkanal oder Fehlerangriffe erforderlich? Wenn nein, warum nicht?
508
15. Gibt einige benutzerprogrammierbaren nichtflüchtigen Speicher zur Verfügung?
509
16. Wie werden die Schlüssel generiert? Wo sind sie gespeichert sind, und für wie lange?
510
17. Wie viele Daten werden unter dem gleichen Schlüssel verarbeitet? Gibt es inhärente Beschränkungen auf die
511
Datenmenge, die verarbeitet wird, beispielsweise aus dem Protokoll oder aus technischen
512
Einschränkungen?
513
18. Sind die Geräte batteriebetriebenen, oder haben sie ihre Strom aus der Umgebung ziehen?
514
Welche Grenzen sind dem Energie auferlegt und / oder Leistung, die mit dem Gerät zur Verfügung steht?
515

13
19. Hat das Gerät innerhalb einer bestimmten Zeit zu reagieren? Ist das eine weiche Echtzeit (reduziert
516
Nutzen nach Ablauf der Frist) oder harte Echtzeit (Daten werden nach dem Stichtag nutzlos)
517
Anforderung? Wie übersetzen diese Anforderungen zu Einschränkungen auf jedem Verschlüsselungs

518
Algorithmen, die in der Anwendung verwendet werden?
519
20. Was sind die typischen Größen für einen Klartext, verschlüsselten Text, Nachricht, Authentifizierung Tag, usw.? Was
520
technologische oder praktische Faktoren bestimmen ihre Größe? Würde Chiffre Expansion
521
akzeptabel ist, und wenn ja, um wie viele Bytes?
522
21. Was sind die konkreten Anforderungen an die Sicherheit der Anwendung? Welche Arten von
523
Angriffe werden als für die jeweilige Anwendung relevant oder nicht relevant zu sein? Warum so?
524
22. Gibt es eine andere Informationen, die relevant sein können, die Anwendung von einem zu verstehen
525
Sicherheit oder Effizienz Sicht?
526

3.2.2 Profilvorlage und Beispielprofile

527
Es wird nicht erwartet, dass ein Algorithmus notwendigerweise alle Merkmale Ziele zu erreichen
528
gleichzeitig. Als solches wird Profile entwickelt einen Satz von Eigenschaften und das Design zu unterstützen
529
Ziele. Die vorgeschlagene Vorlage ist wie folgt:
530

Profil < *Profilname* >
Primitive
Art primitiver
physikalisch
Charakteristik
Name des physikalischen Eigenschaft (en) und bieten akzeptablen Bereich (e)
(Beispielsweise 64 bis 128 Bytes RAM)
Performance
Charakteristik
Name des Leistungsmerkmal (e) und bieten akzeptablen Bereich (e)
(ZB Latenzzeit von nicht mehr als 5 ns)
Sicherheit
Charakteristik
Mindestsicherheits Stärke, relevante Angriffsmodelle, Seitenkanal Beständigkeitsanforderungen usw.
Entwurfsziele
Liste Design-Ziele.
531

Die folgenden Beispielprofile werden beispielsweise nur zur Verfügung gestellt. Profile für die Aufnahme in
532
Das Portfolio wird mit der Gemeinschaft in einem offenen Prozess entwickelt werden. Beispielanwendungen sind
533
vorgesehen, aber ausgewählte Algorithmen sollten für eine Vielzahl von Anwendungen geeignet sein.
534
Beispielprofil # 1
535
Die erste Probe-Profil ist für einen MAC-Algorithmus, um einen Low-Bereich Implementierung in Hardware mit,
536
und ist für kurze Eingangsnachrichten entwickelt.
537
538

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
14
Profil Sample_1
Primitive
MAC
Physikalische Eigenschaften
1600-1900 GEs, ASIC Hardware-Implementierung
Leistungsmerkmale
Latency ≤ 15 ns
Sicherheitsmerkmale
128-Bit-Sicherheit, Beständigkeit gegenüber nahe stehenden Schlüssel-Attacken, Timing Analyse
Entwurfsziele
Effiziente für kurze Eingangsnachrichten
539
Eine Beispielanwendung mit Profil Sample_1 würde ein RFID-Tag für Asset-Tracking sein.
540
541
Beispielprofil # 2
542
Die zweite Probe Profil ist für einen authentifizierten Verschlüsselungsalgorithmus mit geringer Latenz. Das
543

Implementierung in Hardware oder Software sein, sollte aber für die Entschlüsselung / Überprüfung ermöglichen.
544
Profil Sample_2
Primitive
Blockchiffre
Physikalische Eigenschaften
Hardware oder Software-Implementierung
Leistungsmerkmale
Latency ≤ 20 ns
Sicherheitsmerkmale
128-Bit-Sicherheit, Beständigkeit gegenüber Leistungsanalyse
Entwurfsziele
authentifizierte Verschlüsselung
545
Ein Anwendungsbeispiel Profil Sample_2 Verwendung würde Befehl Validierung auf einem Controller Area sein
546
Network (CAN) Bus.
547
Beispielprofil # 3
548
Die dritte Probe Profil ist für einen MAC-Algorithmus, die eine minimale Energie verbraucht.
549

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
15
Profil Sample_3
Primitive
MAC
Physikalische Eigenschaften
Hardware-Implementierung
Leistungsmerkmale
Leistung ≤ 10 & mgr; W
Sicherheitsmerkmale
128-Bit-Sicherheit, Widerstand gegen verwandte Schlüssel Angriffe, Strom Analyse
Entwurfsziele
Der Widerstand gegen Tag-Fälschungen
Ein Sensornetzwerkknoten ist ein Beispiel für eine Anwendung, die mit Profil kompatibel sind
550

Sample_3. Beachten Sie, dass der gleiche Algorithmus kann sowohl mit diesem Profil und das Profil in Verbindung gebracht werden
551
Sample_1.
552
3.3
Bewertungsvorgang
553
NIST eine Vorlage und Bewertung für besonders leichte Kryptoalgorithmen entwickeln
554
das ist ähnlich der Blockchiffre Modi Projekt [48] . Es wird eine offene Aufforderung zur Profile sein
555
und leichte Verschlüsselungsalgorithmen. Die Einreichung Anforderungen, Richtlinien und Sätze
556
Bewertungskriterien werden auf der Lightweight Cryptography Projektseite veröffentlicht
557
(http://www.nist.gov/itl/csd/ct/lwc-project.cfm) .
558
NIST werden Workshops in regelmäßigen Abständen halten leichte Algorithmen zu diskutieren, die unter sind
559
Gegenleistung für das Portfolio. Diese Workshops werden um Vorschläge von der Gemeinschaft auf
560
Kryptoanalyse, Implementierungen und Anwendungen der Vorschläge.
561
Die lwc-forum@nist.gov E-Mail-Liste wurde für den Dialog in Bezug auf NIST etabliert
562
Leichte Cryptography Projekt. an die NIST leichte Kryptographie Mailing zu abonnieren
563
Liste, eine E-Mail-Nachricht an lwc-forum-request@nist.gov~~V, mit einer Betreffzeile "subscribe".
564
Vorläufiger Zeitplan:
565
- NIST erbittet Antworten auf der mitgelieferten Liste von Fragen zu den Anforderungen aus der
566
Gemeinschaft, die auf den gegenwärtigen und zukünftigen Anwendungen und Geräte benötigt. Antworten auf
567
Die Fragen sollten mit der Betreffzeile gesendet werden lightweight-crypto@nist.gov~~V
568
"Antworten auf Fragen zu leichten Krypto-Anforderungen" vor 1. Oktober 2016.
569
NIST werden Profile auf die Antworten basierend entwickeln sie empfängt, und diese Profile werden
570
bieten einen Ausgangspunkt für die Diskussion und fordern Primitiven.

571
- NIST wird die zweite Leicht Cryptography Workshop über 17-18, Oktober 2016 halten.
572
Das Ziel dieses Workshops wird dieses Dokument zu diskutieren, vorgeschlagen Profile,
573
Vergleich Werkzeuge und Methoden, und die jüngsten Arbeiten auf cryptanalysis und Implementierungen
574
leichte Kryptographie Designs.
575
- NIST wird eine Aufforderung zur Einreichung von leichten Primitiven Anfang 2017. Der Anruf veröffentlichen
576
wird darum ersuchen Beiträge, die gute Lösungen für die genannten Profile sind.
577

- Ende 2017, etwa sechs Monate nach der Telefonkonferenz , veröffentlicht wird, wird NIST beginnen
578
Überprüfung der Vorschläge.
579
- NIST wird die dritte Leichte Cryptography Workshop Anfang 2018 halten zu diskutieren
580
Vorschläge und Pläne für die Standardisierung.
581
582

Referenzen
583

[1]
Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., und Tokita, T.,
584
Camellia: Ein 128-Bit - Block Cipher Geeignet für mehrere Plattformen - Design - andAnalysis . Proc.
585
7. Annual International Workshop on Ausgewählte Bereiche in Cryptography (SAC 2000) Waterloo,
586
Ontario, Kanada, 14-15 August 2000, pp. 39-56, http://dx.doi.org/10.1007/3-540-44983-3_4
587
[2]
Aumasson, J.-P., Henzen, L., Meier, W., und Naya-Plasencia, M., *Quark: Ein Leichtgewicht*
588
Hash , Journal of Kryptologie, 2013, Vol. 26, (2), pp. 313-339,
http://dx.doi.org/10.1007/s00145-
589
012-9125-6
590
[3]
Babbage, S., und Dodd, M., *Der MICKEY Stromchiffren* : "Neue Stream - Cipher Designs
591
-. Die eSTREAM Finalisten (Springer, 2008), LNCS 4986, S. 191-209,
592
http://dx.doi.org/10.1007/978-3-540-68351-3_15
593
[4]
Barker, E., und Roginsky, A., *Transitions: Empfehlung für die Überführung des Einsatzes von*
594
Kryptoalgorithmen und Schlüssellängen , NIST Special Publica (SP) 800-131A Revision
595
1, National Institute of Standards and Technology, Gaithersburg, Maryland November 2015,
596
http://dx.doi.org/10.6028/NIST.SP.800-131Ar1
597
[5]
Barker, WC, und Barker, E., *Empfehlung für den Triple Data Encryption Algorithm*
598
(TDEA) Blockchiffre , NIST Special Publica (SP) 800-67 Revision 1, Nationales Institut für
599
Standards and Technology, Gaithersburg, Maryland, Januar 2012
600
http://dx.doi.org/10.6028/NIST.SP.800-67r1
601
[6]
Beaulieu, R., Schoren, D., Smith, J., Treatman-Clark, S., Wochen, B., und Wingers, L., *The*
602
SIMON und SPECK Familien von Leichtbau Blockchiffren , IACR Kryptologie ePrint - Archiv,
603
2013 http://eprint.iacr.org/2013/404

604
[7]
Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., und Verbauwhede, I.,
605
SPONGENT: Ein leichtes Hash - Funktion . Proc. 13. Internationaler Workshop über
606
Cryptographic Hardware und Embedded Systems (CHES 2011), Nara, Japan, den 28. September -
607
1. Oktober 2011, LNCS 6917, pp. 312-325, http://dx.doi.org/10.1007/978-3-642-23951-9_21
608
[8]
Bogdanov, A., Knudsen, LR, Leander, G., Paar, C., Poschmann, A., Robshaw, MJB,
609
Seurin, Y., und Vikkelsoe, C., *PRESENT: ein ultraleichtes Blockchiffre* . Proc. 9.
610
International Workshop on Cryptographic Hardware und Embedded Systems (CHES 2007),
611
Wien, Österreich, September 10-13, 2007, LNCS 4727, S.. 450-466,
612
http://dx.doi.org/10.1007/978-3-540-74735-2_31
613
[9]
Borghoff, J., Canteaut, A., Güneysu, T., Kavun, EB, Knezevic, M., Knudsen, LR,
614
Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, SS, und Yalçın, T.,
615
PRINCE - Ein Low-Latency - Block Cipher für Pervasive Computing Applications . Proc. 18.
616
Internationale Konferenz über die Theorie und Anwendung von Kryptologie und Informationssicherheit
617
(ASIACRYPT 2012), Beijing, China, im Dezember 2-6, 2012, pp. 208-225,
618
http://dx.doi.org/10.1007/978-3-642-34961-4_14
619

NISTIR 8114 (D
FLOSS
)
R
ERICHT ON
L
IGHTWEIGHT
C
RYPTOGRAPHY
18
[10]
Chen, L., *Empfehlung für die Schlüsselableitung Mit Pseudozufallsfunktionen*
620

(Überarbeitet) , NIST Special Publica (SP) 800-108, National Institute of Standards und
621
Technologie, Gaithersburg, Maryland, im Oktober 2009,
http://dx.doi.org/10.6028/NIST.SP.800-108
622
[11]
Chen, L., *Empfehlung für die Schlüsselableitung durch Extraktion-then-Expansion* , NIST
623
Sonderveröffentlichung (SP) 800-56C, National Institute of Standards and Technology,
Gaithersburg,
624
Maryland, November 2011, http://dx.doi.org/10.6028/NIST.SP.800-56C
625
[12]
Cryptographic Forschung und Bewertungsausschüsse, http://www.cryptrec.go.jp/english/
626
[Zugegriffen 11. August 2016]
627
[13]
Cryptographic Forschung und Bewertungsausschüsse, *Cryptrec Bericht 2014* , Bericht des
628
die Cryptographic Technology Evaluation Committee, 296 Seiten, März 2015
629
http://www.cryptrec.go.jp/report/c14_eval_web.pdf
630
[14]
Dang, Q., *Empfehlung für bestehende Anwendungsspezifische Schlüsselableitungsfunktionen* ,
631
NIST Special Publica (SP) 800-135 Revision 1, National Institute of Standards und
632
Technologie, Gaithersburg, Maryland, Dezember 2011
http://dx.doi.org/10.6028/NIST.SP.800-
633
135r1
634
[15]
De Cannière, C., und Preneel, B., *Trivium* : 'New Stream - Cipher Designs - The
635
eSTREAM Finalisten (Springer, 2008), LNCS 4986, S.. 244-266,
http://dx.doi.org/10.1007/978-
636
3-540-68351-3_18
637
[16]
Dworkin, M., *Empfehlung für Block Cipher Betriebsmodi: Der CCM - Modus*
638
für die Authentifizierung und Vertraulichkeit , NIST Special Publica (SP) 800-38C, National
639
Institute of Standards and Technology, Gaithersburg, Maryland, im Mai 2004,
640
http://dx.doi.org/10.6028/NIST.SP.800-38C

641
[17]
Dworkin, M., *Empfehlung für Block Cipher Betriebsmodi: Der CMAC - Modus*
642
für die Authentifizierung NIST Special Publica (SP) 800-38B, National Institute of Standards und
643
Technologie, Gaithersburg, Maryland, im Mai 2005, http://dx.doi.org/10.6028/NIST.SP.800-38B
644
[18]
Dworkin, M., *Empfehlung für Block Cipher Betriebsmodi: Galois / Zähler*
645
Mode (GCM) und GMAC , NIST Special Publica (SP) 800-38D, National Institute of
646
Standards and Technology, Gaithersburg, Maryland, im November 2007,
647
http://dx.doi.org/10.6028/NIST.SP.800-38D
648
[19]
ECRYPT, *eSTREAM: die ECRYPT Stream - Cipher - Projekt* ,
649
http://www.ecrypt.eu.org/stream/ [Zugegriffen 10. August 2016],
650
[20]
Feldhofer, M., Dominikus, S., und Wolkerstorfer, J., *starke Authentifizierung für RFID*
651
Systeme können mit dem AES - Algorithmus . Proc. 6. International Workshop on Cryptographic Hardware
652
und Embedded Systems (CHES 2004), Cambridge, MA, USA, August 11-13, 2004, S.. 357-
653
370, http://dx.doi.org/10.1007/978-3-540-28632-5_26
654
[21]
Gong, Z., Hartel, P., Nikova, S., Tang, S.-H., und Zhu, B., *Tulp: Eine Familie von*
655

Leichte Message Authentication Codes für Body Sensor Networks , Journal of Computer
656

Wissenschaft und Technik, 2014, Vol. 29, (1), pp. 53-68, http://dx.doi.org/10.1007/s11390-013-
657
1411-8
658
[22]
GS1 EPCglobal Inc., EPC Hochfrequenz-Identitätsprotokolle der Generation 2 UHF-RFID,
659
Spezifikation für RFID Air Interface Protokoll für die Kommunikation bei 860 MHz - 960
660
MHzVersion 2.0.1 Ratifizierter 2015
661
http://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf
662
[23]
Guo, J., Peyrin, T., und Poschmann, A., *Die PHOTON Familie von Leicht Hash*
663
Funktionen . Proc. 31. Annual International Conference Kryptologie (CRYPTO 2011), Santa
664
Barbara, CA, USA, August 14-18, 2011, pp. 222-239, http://dx.doi.org/10.1007/978-3-642-
665
22792-9_13
666
[24]
Guo, J., Peyrin, T., Poschmann, A., und Robshaw, M., *Die LED - Block Cipher* . Proc. 13.
667
International Workshop on Cryptographic Hardware und Embedded Systems (CHES 2011),
668
Nara, Japan, den 28. September -. 1. Oktober 2011, S. 326-341,
http://dx.doi.org/10.1007/978-3-
669
642-23951-9_22
670
[25]
Hölle, M., Johansson, T., und Meier, W., *Korn: Ein Stromchiffre für Constrained*
671
Umwelt , International Journal of Wireless - und Mobile Computing (IJWMC), 2007, Vol. 2,
672
(1), S.. 86-93, http://dx.doi.org/10.1504/IJWMC.2007.013798
673
[26]
Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., und Yoshida, H., *A*
674
Leichte 256-Bit - Hash - Funktion für Hardware und Low-End - Geräte: Lesamnta-LW . Proc.
675
13. Internationale Konferenz für Informationssicherheit und Kryptologie (ICISC 2010),
Seoul,
676
Korea, Dezember 01-3 2010, LNCS 6829, pp. 151-168, http://dx.doi.org/10.1007/978-3-642-
677
24209-0_10

678
[27]
Ideguchi, K., Owada, T., und Yoshida, H., *eine Studie über die RAM - Anforderungen der verschiedenen*
679
SHA-3 - Kandidaten auf Low-Cost - 8-Bit - CPUs , IACR Kryptologie ePrint - Archiv 2009
680
http://eprint.iacr.org/2009/260
681
[28]
ISO, ISO / IEC 29192-1: 2012, *Informationstechnologie - Sicherheitsverfahren -*
682
Leichte Cryptography - Teil 1: Allgemeine 2012,
683
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=56425
684
[29]
ISO, ISO / IEC 29192-2: 2012, *Informationstechnologie - Sicherheitsverfahren -*
685
Leichte Cryptography - Teil 2: Blockchiffren , 2012,
686
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=56552
687
[30]
ISO, ISO / IEC 29192-4: 2013, *Informationstechnologie - Sicherheitsverfahren -*
688
Leichte Cryptography - Teil 4: Mechanismen der asymmetrischen Techniken , 2013
689
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=56427
690
[31]
ISO, ISO / IEC 29167-1: 2014, *Information Technology - Automatische Identifikation und*
691
Datenerfassungsverfahren - Teil 1: Sicherheitsdienste für die RFID - Luftschnittstellen , 2014,
692

---

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=61128
693
[32]
ISO, ISO / IEC 29167-11: 2014, *Information Technology - Automatische Identifikation und*

694
Datenerfassungsverfahren - Teil 11: Crypto Suite PRESENT-80 Security Services für Air
695
Interface - Kommunikation 2014
696
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=60441
697
[33]
ISO, ISO / IEC 29167-10: 2015, *Information Technology - Automatische Identifikation und*
698
Datenerfassungsverfahren - Teil 10: Crypto Suite AES-128 Security Services für Air Interface
699
Kommunikation 2015
700
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=60440
701
[34]
ISO, ISO / IEC 29167-12: 2015, *Information Technology - Automatische Identifikation und*
702
Datenerfassungsverfahren - Teil 12: Crypto Suite ECC-DH Security Services für Air Interface
703
Kommunikation 2015
704
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=60442
705
[35]
ISO, ISO / IEC 29167-13: 2015, *Information Technology - Automatische Identifikation und*
706
Datenerfassungsverfahren - Teil 13: Crypto Suite Grain-128A Sicherheitsdienste für Air Interface
707
Kommunikation 2015
708
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=60682
709
[36]
ISO, ISO / IEC 29167-14: 2015, *Information Technology - Automatische Identifikation und*
710
Datenerfassungsverfahren - Teil 14: Crypto Suite AES OFB Security Services für Air Interface
711
Kommunikation 2015
712
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=61130
713
[37]
ISO, ISO / IEC 29167-16: 2015, *Information Technology - Automatische Identifikation und*
714
Datenerfassungsverfahren - Teil 16: Crypto Suite ECDSA-ECDH Security Services für Air
715
Interface - Kommunikation 2015

716
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=61321
717
[38]
ISO, ISO / IEC 29167-17: 2015, *Information Technology - Automatische Identifikation und*
718
Datenerfassungsverfahren - Teil 17: Crypto Suite CryptoGPS Security Services für Air Interface
719
Kommunikation 2015
720
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=61942
721
[39]
ISO, ISO / IEC 18000-63: 2015, *Informationstechnologie - Radio Frequency Identification*
722
für das Management - Teil 63: Parameter für die Kommunikation auf der 860 MHz bis 960
723
MHz Typ C , 2015,
724
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_icshtml?csnumber=63675
725
[40]
ISO, ISO / IEC 29192-5: 2016, *Informationstechnologie - Sicherheitsverfahren -*
726
Leichte Cryptography - Teil 5: Hash-Funktionen , 2016,
727
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detailhtml?csnumber=67173
728
[41]
Juels, A., und Weis, SA, *Authentifizieren von Pervasive Devices mit Menschen Protokolle* . Proc.
729

---

25. Annual International Conference Kryptologie (CRYPTO 2005), Santa Barbara, Kalifornien,
730
USA, August 14-18, 2005, LNCS 3621, S.. 293-308, http://dx.doi.org/10.1007/11535218_18
731
[42]

Leander, G., Paar, C., Poschmann, A., und Schramm, K., *New Leichtbau DES Varianten* .
732
Proc. 14. Internationaler Workshop über schnelle Software Encryption (FSE 2007),
Luxemburg,
733
Luxemburg, 2007, LNCS 4593, S.. 196-210, http://dx.doi.org/10.1007/978-3-540-74619-5_13
734
[43]
Luykx, A., Preneel, B., Tischhauser, E., und Yasuda, K., *MAC - Modus für den Leichtbau*
735
Blockchiffren . Proc. 23. Internationale Konferenz für schnelle Software Encryption (FSE
2016),
736
Bochum, Deutschland, März 20-23, 2016, LNCS 9783, pp. 43-59,
http://dx.doi.org/10.1007/978-3-
737
662-52993-5_3
738
[44]
Mathew, S., Satpathy, S., Suresh, V., Anders, M., Kaul, H., Agarwal, A., Hsu, S., Chen,
739
G. und Krishnamurthy, R., *340 mV-1,1 V, 289 Gbps / W, 2090-Tor NanoAES Hardware*
740
Beschleuniger mit flächenoptimierten Verschlüsseln / Entschlüsseln GF (2
4
)
2
Polynomials in 22 nm Tri-Gate-
741
CMOS , IEEE Journal of Solid-State Circuits, 2015, Vol. 50, (4), pp. 1048-1058,
742
http://ieeexplore.ieee.org/ielx7/4/7066864/07019004.pdf?tp=&arnumber=7019004&isnumber
=7
743
066864
744
[45]
Microchip Technology Inc., *New / Beliebte 8-Bit - Mikrocontroller Produkte* ,
745
http://www.microchip.com/ParamChartSearch/chart.aspx?branchID=1012 [abgerufen am 9.
August
746
2016]
747
[46]
Moradi, A., Poschmann, A., Ling, S., Paar, C., und Wang, H., sind *die Grenzen: A Very*
748
Kompakt und eine Schwelle Implementierung von AES . Proc. 30. Annual International
Conference
749
auf der Theorie und Anwendungen von Kryptotechniken (EUROCRYPT 2011), Tallinn,

750
Estland, 15-19 Mai 2011, LNCS 6632, pp. 69-88, http://dx.doi.org/10.1007/978-3-642-20465-
751
4_6
752
[47]
Mouha, N., Mennink, B., Van Herreweghe, A., Watanabe, D., Preneel, B., und
753
Verbauwhede, I., *Chaskey: Eine effiziente MAC Algorithmus für die 32-Bit - Mikrocontroller* .
Proc. 21.
754
Internationale Konferenz über Ausgewählte Bereiche in Cryptography (SAC 2014), Montreal,
QC,
755
Kanada, August 14-15, 2014, pp. 306-323, http://dx.doi.org/10.1007/978-3-319-13051-4_19
756
[48]
National Institute of Standards and Technology, *Block - Cipher - Modi* ,
757
http://csrc.nist.gov/groups/ST/toolkit/BCM/indexhtmll [zugegriffen 9. August 2016]
758
[49]
National Institute of Standards and Technology, *Post-Quantum Crypto - Projekt* ,
759
http://csrc.nist.gov/groups/ST/post-quantum-crypto/indexhtmll [Zugegriffen 2016, den 11.
August]
760
[50]
National Institute of Standards and Technology, *NIST Cryptographic Standards und*
761
Leitlinien - Entwicklungsprozess , NISTIR 7977, im März 2016
762
http://dx.doi.org/10.6028/NIST.IR.7977
763
[51]
Needham, RM, und Wheeler, DJ, *Tea - Erweiterungen* , Technischer Bericht, Computer
764
Laboratory, University of Cambridge, Oktober 1997
http://www.cix.co.uk/klockstone/xtea.pdf
765

22
[52]
NXP, *8-Bit - RS08* , http://www.nxp.com/products/microcontrollers-and-processors/more-
766
Prozessoren / 8-16-Bit-MCUs / 8-Bit-RS08: RS08FAMILY [zugegriffen 9. August 2016]
767
[53]
Osvik, DA, Bos, JW, Stefan, D., und Canright, D., *Verschlüsselung Schnelle Software AES* .
768
Proc. 17. Internationaler Workshop über schnelle Software Encryption (FSE 2010), Seoul, Korea,
769
07-10 Februar 2010, LNCS 6147, pp. 75-93, http://dx.doi.org/10.1007/978-3-642-13858-4_5
770
[54]
Poschmann, AY: *Leichte Cryptography: Cryptographic Engineering für eine*
771
Pervasive Welt . Ph.D. Thesis, Ruhr-Universität Bochum, 2009, http://d-nb.info/996578153
772
[55]
Renesas Electronics Corporation, *RL78 Familie* , https://www.renesas.com/en-
773
uns / products / Mikrocontroller-Mikroprozessoren / rl78htmll [Zugegriffen 11. August 2016],
774
[56]
Rivest, RL, *Der RC5 Verschlüsselungsalgorithmus* . Proc. Zweiter Internationaler Workshop zu
775
Schnelle Software Encryption (FSE 1994), Leuven, Belgien, von 14 bis 16 Dezember, 1994, LNCS 1008,
776
pp. 86-96, http://dx.doi.org/10.1007/3-540-60590-8_7
777
[57]
Saarinen, M.-JO, und Engels, DW, *ein Do-It-All-Cipher für RFID: Design - Anforderungen*
778
(Extended Abstract) , IACR Kryptologie ePrint - Archiv 2012, http://eprint.iacr.org/2012/317
779
[58]
Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., und Shirai, T., *Piccolo:*
780
Ein extrem leichter Blockverschlüsselung . Proc. 13. Internationaler Workshop über Cryptographic
781
Hardware und Embedded Systems (CHES 2011), Nara, Japan, den 28. September - 1. Oktober 2011
782
pp. 342-357, http://dx.doi.org/10.1007/978-3-642-23951-9_23
783
[59]

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., und Iwata, T., *The 128-Bit Blockverschlüsselung*
784
CLEFIA (Extended Abstract) . Proc. 14. Internationaler Workshop über schnelle Software-Verschlüsselung
785
(FSE 2007), Luxemburg, Luxemburg, 26-28 März, 2007, S.. 181-195,
786
http://dx.doi.org/10.1007/978-3-540-74619-5_12
787
[60]
Sönmez Turan, M., Barker, E., Burr, W., und Chen, L., *Empfehlung für die Passwort-*
788
Basierend Key Ableitung: Teil 1: Speicheranwendungen , NIST Special Publica (SP) 800-132,
789
National Institute of Standards and Technology, Gaithersburg, Maryland, Dezember 2010
790
http://dx.doi.org/10.6028/NIST.SP.800-132
791
[61]
Suzaki, T., Minematsu, K., Morioka, S., und Kobayashi, E., *TWINE: Ein Leichtbau - Block*
792
Cipher für mehrere Plattformen . Proc. 19. Internationale Konferenz über Ausgewählte Bereiche
793
Cryptography (SAC 2012), Windsor, ON, Kanada, August 15-16 2012, S.. 339-354,
794
http://dx.doi.org/10.1007/978-3-642-35999-6_22
795
[62]
Texas Instruments, *COP912C 8-Bit - Mikrocontroller* ,
796
http://www.ti.com/product/COP912C [zugegriffen 9. August 2016]
797
[63]
US Department of Commerce, *Advanced Encryption Standard (AES)* , Bundes
798
Information Processing Standards (FIPS) Veröffentlichung 197, November 2001
799
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
800

RYPTOGRAPHY
23
[64]
US Department of Commerce, *der Keyed-Hash Message Authentication Code (HMAC)* ,
801
Federal Information Processing Standards (FIPS) 198-1 Veröffentlichung Juli 2008,
802
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
803
[65]
US Department of Commerce, *Secure Hash Standard (SHS)* Federal Information
804
Processing Standards (FIPS) 180-4 Veröffentlichung August 2015
805
http://dx.doi.org/10.6028/NIST.FIPS.180-4
806
[66]
US Department of Commerce, *SHA-3 Standard: Permutation-basierte Hash und*
807
Ausziehbare-Ausgabefunktionen , Federal Information Processing Standards (FIPS)
Publication 202,
808
August 2015, http://dx.doi.org/10.6028/NIST.FIPS.202
809
[67]
Université du Luxemburg, *Leichte Blockchiffren* ,
810
https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers [Zugegriffen 10. Mai
2016],
811
[68]
Wheeler, DJ, und Needham, RM, *TEA, A Tiny Encryption Algorithm* . Proc. Zweite
812
Internationaler Workshop über schnelle Software Encryption (FSE 1994), Leuven, Belgien,
Dezember
813
14-16, 1994, LNCS 1008, S.. 363-366, http://dx.doi.org/10.1007/3-540-60590-8_29
814
815

Originaltext

Bessere Übersetzung vorschlagen