

**Praktikum Rechnerarchitektur**Gruppe 155 – Abgabe zu Aufgabe A501  
Sommersemester 2019

Mete Polat

Jonas Hübötter

Simon Martin Bohnen

## 1 Einleitung

Im Folgenden wird die symmetrische Blockchiffre RC5 sowie die Implementierung dieser beschrieben. Zunächst wird der Algorithmus näher spezifiziert und auf dessen Sicherheit eingegangen. Daraufhin werden Aspekte der Lösungsfindung besprochen und der Implementierung dokumentiert. Abschließend wird die Implementierung gegen eine Referenzimplementierung getestet und die Performanz analysiert.

## 2 Problemstellung und Spezifikation

### 2.1 RC5-16/16/b

#### 2.1.1 Schlüsselerweiterung mit P und Q

RC5 ist rundenbasiert, weshalb zunächst aus dem gegebenen Schlüssel mehrere Runden-schlüssel erzeugt werden. Für den Schritt der Schlüsselexpansion von RC5 werden die beiden ungeraden Ganzzahlen  $P$  und  $Q$  benötigt. Diese sind jeweils für eine gegebene Blockgröße von RC5 konstant. Für das von uns implementierte RC5-16/16/b gilt:

$$\begin{aligned} P &= \text{Odd}((e - 2) \cdot 2^{16}) & Q &= \text{Odd}((\phi - 1) \cdot 2^{16}) \\ &= \text{Odd}(0,71828 \cdot 65.536) & &= \text{Odd}(0,61803 \cdot 65.536) \\ &= \text{Odd}(47.073,19808) & &= \text{Odd}(40.503,21408) \\ &= 47.073 = 0xb7e1 & &= 40.503 = 0x9e37 \end{aligned}$$

#### 2.1.2 Sicherheit

Durch die Parametrisierung von RC5- $w/r/b$  hat die Chiffre eine variable Halblockgröße  $w$ , Rundenanzahl  $r$  und Schlüssellänge  $b$  [8, p.2]. Zusammen mit dem Betriebsmodus bestimmen diese Parameter die Sicherheit von RC5.

**Schlüssellänge** So wie im Allgemeinen bei Blockchiffren ist auch bei RC5 die Sicherheit der Chiffre stark von der gewählten Schlüssellänge abhängig. Der Parameter  $b \in \{k \in \mathbb{N}_0 : k \leq 255\}$  gibt die Länge des Schlüssels in Bytes an [8, p.3]. Die Länge der erweiterten Schlüsseltabelle in Bits ergibt sich durch  $2^{(2r+2)w}$  [8, p.2]. Der Aufwand für eine erschöpfende Suche ist damit  $\min\{2^{8b}, 2^{(2r+2)w}\}$  [13, p.29]. Für RC5-16/16/b ist damit der Aufwand einer erschöpfenden Suche allein von  $b$  abhängig, solange  $b < 68$  gilt.

---

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt für Blockchiffren wie RC5 eine minimale Schlüssellänge von 128 Bits vor [11, p.21].

**Betriebsmodus** Ist der durch den Betriebsmodus generierte Ciphertext nicht pseudorandom — resultieren äquivalente Plaintext-Blöcke beispielsweise in äquivalenten Ciphertext-Blöcken —, dann enthält der Ciphertext Informationen zur Struktur des Plaintextes [11, p.22]. In diesem Fall können Teile des Plaintextes durch *Häufigkeitsanalyse* rekonstruiert [11, p.22], oder sogar der verwendete Schlüssel durch einen *Codebook Attack* gewonnen werden [2, p.2].

Sichere Modi sind beispielsweise *Cipher Block Chaining (CBC)* und der *Counter Mode (CTR)*, da dort der  $n$ -te Ciphertext-Block nicht nur von dem  $n$ -ten Plaintext-Block und dem genutzten Schlüssel abhängt, sondern zudem noch von einem weiteren Wert, wie dem  $(n - 1)$ -ten Ciphertext-Block oder einem Zähler [11, p.22].

**Rundenanzahl** Nach Kaliski und Yin werden für eine *differenzielle Kryptoanalyse* von RC5-32/16/b entweder  $2^{61}$  selbst gewählte Plaintexte oder  $2^{63}$  bekannte Plaintexte benötigt. Ein solcher Angriff auf ein 16-rundiges RC5 ist damit überaus unwahrscheinlich. Da die Anzahl der möglichen Plaintexte bei dieser Konfiguration von RC5 jedoch bei  $2^{64}$  liegt, kann ein solcher Angriff nicht theoretisch ausgeschlossen werden [13, p.6]. Weiterhin sei eine *lineare Kryptoanalyse von RC5* nur bei einer sehr geringen Rundenanzahl von RC5 effektiv [13, p.28].

Knudsen und Meier zeigen zwar, dass die Komplexität des von Kaliski und Yin vorgeschlagenen differenziellen Angriffs um einen Faktor von bis zu 512 reduziert werden kann [6, p.2], allerdings bleibt ein solcher Angriff damit weiterhin sehr unwahrscheinlich. Zudem wurde gezeigt, dass für bestimmte Teile des Schlüsselraums die differentiellen Kryptoanalysen weiter verbessert werden können [6, p.13]. Für einen effektiven Angriff sind dennoch entweder zu wenige Schlüssel betroffen oder die Anzahl der benötigten Plaintexte ist weiterhin zu hoch. Ähnliches konnte Heys für lineare Kryptoanalyse zeigen [3, p.5].

**Blockgröße** Durch die 32 Bit Blockgröße von RC5-16/16/b ist die Komplexität eines *generischen Angriffs* durch  $2^{32}$  nach oben beschränkt. Bellare et al. zeigen für CBC, dass die Unsicherheit eines generischen Angriffs durch

$$\epsilon \geq \left( \frac{\mu^2}{l^2} - \frac{\mu}{l} \right) \cdot \frac{1}{2^l}$$

gegeben ist, wobei  $l = 2w$  der Blockgröße,  $\mu = q \cdot l$  der Länge der verarbeiteten Plaintexte und  $q$  der Anzahl der verarbeiteten Blöcke entspricht [5, p.5;24]. Damit kann eine untere Schranke  $\epsilon$  für die Erfolgswahrscheinlichkeit eines solchen Angriffs durch

$$\epsilon \geq \frac{q^2}{2^l}$$

---

abgeschätzt werden. Die minimale Erfolgswahrscheinlichkeit eines generischen Angriffs auf eine 32-Bit Blockchiffre ist somit  $2^{-32}$ . Aus diesem Grund eignen sich 32-Bit Blockchiffren im Allgemeinen und RC5-16/16/b im Speziellen nicht für die Verschlüsselung von großen Datenmengen. Die RC5-Chiffre kann damit bei für die Anwendung ausreichend großer Blockgröße und Rundenanzahl,  $b \geq 16$  und Nutzung eines geeigneten Betriebsmodus als sicher gelten. RC5-16/16/b eignet sich in der Regel lediglich zur Verschlüsselung von kleinen Datenmengen für die  $q \ll 2^{16} = 2^{l/2}$  gilt.

## 2.2 Feistelchiffren

Die folgende allgemeine Darstellung von Feistelchiffren soll auf klassische (auch ausgewogene) Feistelchiffren begrenzt werden. Wie für RC5, gilt für klassische Feistelchiffren, dass die Längen der beiden Halblöcke eines Blocks gleich sein müssen. Zudem wird sich auf das für die umkehrbare Verknüpfung von zwei Halblöcken übliche  $\oplus$  (XOR) beschränkt.

### 2.2.1 Einrundige Feistelnetzwerke

Eine Feistelchiffre ist eine rundenbasierte Blockchiffre, die nach der Art eines Feistelnetzwerks aufgebaut ist. Sei

$$F_n := \{f \mid f: \{0, 1\}^n \rightarrow \{0, 1\}^n\}$$

die Familie der Rundenfunktionen. Zunächst soll ein klassisches einrundiges Feistelnetzwerk  $\Psi$  betrachtet werden. Dieses wird definiert durch eine beliebige Abbildung  $f \in F_n$  und eine umkehrbare Bitoperation — durch obige Einschränkung der Allgemeinheit  $\oplus$ .

$$\Psi(f): \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}: [L, R] \mapsto [S, T] \Leftrightarrow \begin{cases} S = R \\ T = L \oplus f(R) \end{cases}$$

für  $\forall (L, R) \in (\{0, 1\}^n)^2$  [12, p.11] (siehe Abbildung 1). Wichtig für jede Verschlüsselung ist Bijektivität, damit jedem Codewort eine eindeutige Plaintext-Nachricht zugeordnet werden kann.  $\Psi(f)$  ist unabhängig von  $f \in F_n$  eine Permutation, d.h.  $f$  selbst muss nicht bijektiv sein [12, p.12]. Aus der Definition von  $\Psi(f)$  ergibt sich ihr Inverses als

$$\Psi(f)^{-1} = \sigma \circ \Psi(f) \circ \sigma$$

mit  $\sigma$  definiert als  $\sigma([L, R]) = [R, L]$  für  $L, R \in \{0, 1\}^n$ , der Vertauschung beider Halblöcke [12, p.12] (siehe Abbildung 2).

### 2.2.2 r-rundige Feistelnetzwerke

Üblicherweise werden Feistelnetzwerke in mehreren Runden angewendet. Im Allgemeinen ist ein klassisches Feistelnetzwerk mit  $r \geq 1$  Runden und  $f_1, f_2, \dots, f_r \in F_n$  Rundenfunktionen definiert durch

$$\Psi^r(f_1, \dots, f_r) = \Psi(f_r) \circ \dots \circ \Psi(f_2) \circ \Psi(f_1).$$

[12, p.12] (siehe Abbildung 3)

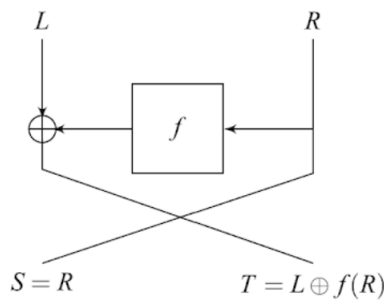


Abbildung 1: Einrundiges Feistelnetzwerk  
[12, Fig. 2.1]

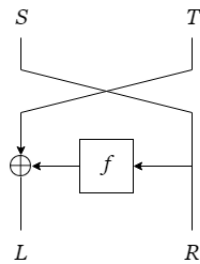


Abbildung 2: Inverses eines einrundigen  
Feistelnetzwerks

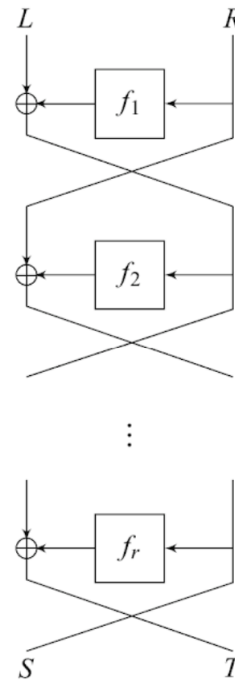


Abbildung 3: r-rundiges Feistelnetzwerk  
[12, Fig. 2.2]

Da ein einrundiges Feistelnetzwerk eine Permutation über  $\{0,1\}^{2n}$  ist, sind auch  $r$ -rundige Feistelnetzwerke Permutationen. Weiterhin ist das Inverse eines  $r$ -rundigen Feistelnetzwerks die Komposition der Inversen der einzelnen Runden [12, p.13].

$$\begin{aligned} (\Psi^r(f_1, \dots, f_r))^{-1} &= \sigma \circ \Psi(f_1) \circ \sigma \circ \dots \circ \sigma \circ \Psi(f_r) \circ \sigma \\ &= \sigma \circ \Psi^r(f_r, \dots, f_1) \circ \sigma \end{aligned}$$

Eine Feistelchiffre ist nun ein spezielles Feistelnetzwerk, dessen Rundenfunktionen von einem Rundenschlüssel aus dem Schlüsselraum  $K$  abhängen. Seien die Rundenschlüssel  $(k_1, \dots, k_r) \in K^r$  und die Familie der Rundenfunktionen

$$F_{n,K} := \{f_k \mid k \in K, f_k: \{0,1\}^n \rightarrow \{0,1\}^n\}.$$

Dann ist eine Feistelchiffre das Feistelnetzwerk  $\Psi^r(f_{k_1}, \dots, f_{k_r})$ . Also die  $r$ -rundige Permutation von der Nachricht  $\{0,1\}^{2n}$  in Abhängigkeit vom Schlüssel  $(k_1, \dots, k_r)$  [12, p.14].

### 2.2.3 RC5 als Feistelchiffre

RC5 baut zu Beginn die erweiterte Schlüsseltabelle  $S$  auf, die aus  $2r+2$  Schlüsseln besteht und von  $K$  abhängt. Seien  $\Sigma := (S_2, S_3, \dots, S_{2r+1}) = (\Sigma_0, \Sigma_1, \dots, \Sigma_{2r-1})$  mit  $|\Sigma| = 2r$  die Schlüssel aus der erweiterten Schlüsseltabelle, die während der Runden von RC5 zum

Verschlüsseln benutzt werden —  $S_0$  und  $S_1$  werden für das Key-Whitening genutzt. Zudem sei  $(g_{\Sigma_0}, g_{\Sigma_1}, \dots, g_{\Sigma_{2r-1}})$  definiert durch

$$g_k: \{0, 1\}^w \times \{0, 1\}^w \rightarrow \{0, 1\}^w:$$

$$(\tau, R) \mapsto (\tau \lll R) + k$$

mit  $\tau = L \oplus R$ ,  $k \in \Sigma$  und  $L, R \in \{0, 1\}^w$  wobei  $x \lll y$  die Linksrotation von  $x$  um  $y$  Bits angibt. Dann zeigt die folgende Tabelle die Zusammenhänge von RC5 und Feistelchiffren.

RC5	Feistelchiffre
$r$	$2r$
$w$	$n$
$\Sigma$	$K^{2r}$
$(g_{\Sigma_0}, g_{\Sigma_1}, \dots, g_{\Sigma_{2r-1}})$	$(f_{k_1}, \dots, f_{k_{2r}}) \in F_{n,K}^{2r}$

Die Reihenfolge der Anwendung der umkehrbaren Bitoperation ( $\oplus$ ) und der Rundenfunktion unterscheidet sich leicht zwischen RC5 und einer allgemeinen klassischen Feistelchiffre. Dieser Unterschied soll in der folgenden Abbildung skizziert werden.

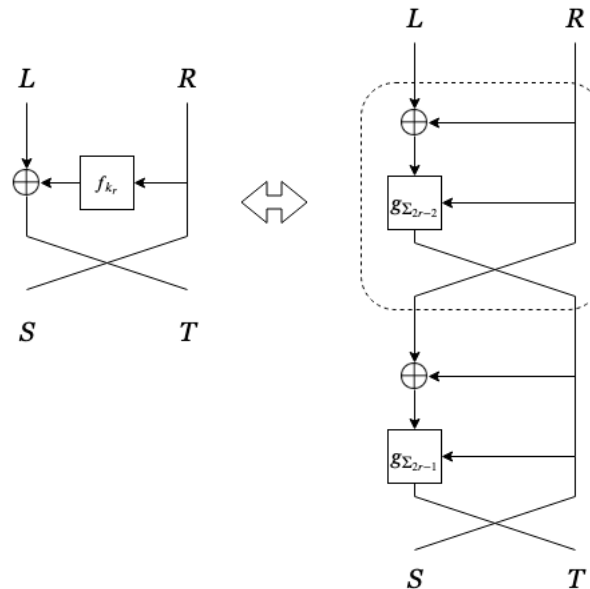


Abbildung 4: Links eine Runde einer Feistelchiffre, rechts eine Runde (zwei Halbrunden) von RC5

wobei  $r$  die aktuelle Runde angibt. Wie dargestellt, ist eine Halbrunde von RC5 im Aufbau ähnlich zu einer Runde einer Feistelchiffre.

Durch den leicht modifizierten Aufbau einer Feistelchiffre in RC5, verändert sich bei RC5 die Berechnung der Inversen. Für eine RC5-Runde gilt

$$RC5_{r,\Sigma}: \{0, 1\}^{2w} \rightarrow \{0, 1\}^{2w}: [L, R] \mapsto [S, T] \Leftrightarrow \begin{cases} S = ((L \oplus R) \lll R) + \Sigma_{2r-2} \\ T = ((R \oplus S) \lll S) + \Sigma_{2r-1} \end{cases}.$$

Damit gilt für die Berechnung der Inversen von einer RC5-Runde

$$RC5_{r,\Sigma}^{-1}: \{0,1\}^{2w} \rightarrow \{0,1\}^{2w}: [S,T] \mapsto [L,R] \Leftrightarrow \begin{cases} L = ((S - \Sigma_{2r-2}) \ggg R) \oplus R \\ R = ((T - \Sigma_{2r-1}) \ggg S) \oplus S \end{cases}$$

für  $\forall(S,T) \in (\{0,1\}^w)^2$  wobei  $x \ggg y$  die Rechtsrotation von  $x$  um  $y$  Bits angibt.

## 2.3 PKCS#7-Padding

Da eine Blockchiffre nur Nachrichten vollständig verschlüsseln kann, die restfrei in Blöcke geteilt werden können, muss die Länge dieser Nachrichten zunächst auf ein Vielfaches der Blockgröße erweitert werden. Diese Erweiterung wird im Allgemeinen als Padding bezeichnet.

Das PKCS#7-Padding ist eine Form der Erweiterung des Plaintextes auf ein Vielfaches der Blocklänge und soll im Folgenden erläutert werden. Es sei  $\Delta$  definiert als

$$\Delta = b - (l \bmod b)$$

mit  $b$  als der Länge eines Blocks und  $l$  als der Länge des Plaintextes in Byte. Vor der Anwendung eines Verschlüsselungsalgorithmus, der als Länge des Inputs ein Vielfaches von  $b$  Bytes erwartet, werden  $\Delta$  Bytes jeweils mit dem Wert  $\Delta$  an den Plaintext angefügt [4, p.28].

Das heißt, dass der Input in Abhängigkeit von  $b$  und  $l$  um eine der folgenden Byte-Sequenzen erweitert wird:

```

01 -- if l mod b = b-1
02 02 -- if l mod b = b-2
.
.
.
b b ... b b -- if l mod b = 0

```

Nach dem Entschlüsseln des Codewortes, kann das Padding auf eindeutige Weise entfernt werden, da jeder Plaintext — einschließlich jener, deren Länge selbst ein Vielfaches der Blockgröße ist — vor der Verschlüsselung mit PKCS#7-Padding erweitert wurde. Die Anzahl der zu entfernenden Bytes wird durch das letzte Byte des letzten Blocks angegeben. PKCS#7-Padding ist wohldefiniert für  $b < 256$  [4, p.28].

## 3 Lösungsfindung

### 3.1 Initialisierungsvektor

Eine Herausforderung ist die Erzeugung und Speicherung des Initialisierungsvektors, der beim Cipher Block Chaining Mode benötigt wird. Es ist einerseits entscheidend,

dass dieser nicht aus zuvor bekannten Informationen erzeugt wird, wie es zum Beispiel bei SSL 3.0 und TLS 1.0 der Fall war. Dort führte dies zu einer Schwäche, falls dem Angreifer zwei aufeinanderfolgende Ciphertext-Blöcke bekannt waren [9]. Andererseits ist eine ausreichende Länge wichtig, um einem Related-Key-Attack vorzubeugen, der zum Beispiel das WEP-Protokoll betraf [7].

Aufgrund der Blocklänge bietet sich nur ein 32-Bit-Initialisierungsvektor an, der pseudozufällig generiert wird. Eine Geheimhaltung des Initialisierungsvektors ist nicht erforderlich [10, p.194], weshalb der Vektor am Ende der verschlüsselten Datei gespeichert und dort bei der Entschlüsselung wieder ausgelesen wird.

### 3.2 Optimierung durch SIMD

Eine Optimierung durch SIMD ist möglich und sinnvoll, wenn ein Algorithmus auf mehreren Datenblöcken die selbe Operation ohne Abhängigkeiten zwischen Blöcken ausführt. Bei RC5 und dem CBC-Mode werden jedoch häufig Abhängigkeiten verwendet, um statistischen Analysen, wie sie zum Beispiel beim ECB-Mode möglich sind, vorzubeugen.

Beim Key-Mixing hängt der nächste Rundenschlüssel beispielsweise direkt vom vorherigen ab, wodurch eine Parallelisierung unmöglich wird. Ähnliches gilt für die Ver- und Entschlüsselung, da dort zur Erzeugung des nächsten Ciphertextblocks der vorherige benötigt wird. Die einzige mögliche Optimierung ist das gleichzeitige Laden mehrerer Rundenschlüssel oder Blöcke aus dem Speicher, um die Anzahl der Zugriffe zu minimieren. Beim CBC-Betriebsmodus ist nur ein Laden mehrerer Rundenschlüssel möglich. Wir verwenden ein XMM-Register, um 8 16-Bit-Rundenschlüssel gleichzeitig zu laden. Für die tatsächliche Verwendung müssen diese jedoch aus dem XMM-Register entnommen werden, da nur eine Runde gleichzeitig berechnet werden kann.

Beim Counter-Betriebsmodus ist eine Optimierung durch SIMD möglich. Da der Counter leicht für mehrere Blöcke berechnet werden kann und die Verschlüsselung der Blöcke nicht voneinander abhängt, kann diese auf 8 Blöcken parallel erfolgen, indem die linken und rechten Halblöcke jeweils in ein XMM-Register geladen werden.

## 4 Dokumentation der Implementierung

Die hier bereitgestellte RC5-Implementierung kann zur sicheren Ver- und Entschlüsselung von kleinen Datenmengen genutzt werden. Voraussetzung dafür, ist das Wählen eines geeigneten Schlüssels mit mindestens 16 Byte Länge (siehe 2.1.2 Sicherheit). Es stehen die Betriebsmodi Cipher Block Chaining (CBC), Counter Mode (CTR) und der unsichere Electronic Codebook (ECB) zur Verfügung, wobei letztere effizienter sind.

---

Im Folgenden ist die Gebrauchsanweisung der RC5-Implementierung beschrieben:

rc5 <command>

```
enc [-m <mode>] [-v] <key> <inputFile> [<outputFile>]
dec [-m <mode>] [-v] <key> <inputFile> [<outputFile>]
test [<testId>]
perf
```

where <mode> is one of:

cbc, ctr, ecb

Es kann entweder verschlüsselt oder entschlüsselt werden. Sofern keine Ausgabedatei angegeben ist, wird das Ergebnis in die Eingabedatei geschrieben. Der test-Command kann zur Überprüfung der Korrektheit verwendet werden. Die Performance lässt sich mit dem perf-Command messen.

**Sicherheitshinweise** Solange der Rechner nicht während einer Ver-/Entschlüsselung in den Suspend-Modus versetzt wird, stellt unsere Implementierung sicher, dass der Schlüssel nicht durch Swapping auf die Festplatte geschrieben wird. Nach abgeschlossener Ver-/Entschlüsselung werden die sensiblen Daten aus dem Arbeitsspeicher entfernt. Allerdings ist es möglich, dass durch Swapping, Teile der zu verschlüsselnden/entschlüsselten Daten auf die Festplatte geschrieben wird. Eine Komprimierung des Schlüssels ist auf diese Weise zwar nicht möglich, dennoch ist es empfehlenswert, die Swap-Partition zu verschlüsseln.

## 4.1 Struktur der Implementierung

Die Implementierung ist in die folgenden sieben Module gegliedert:

rc5	Enthält die Implementierung der RC5-Chiffre, sowie der Betriebsmodi CBC, CTR und ECB.
test	Enthält die Funktion zum Ausführen der Korrektheits-Tests.
perf	Enthält die Funktion zum Ausführen der Performance-Tests.
key_expansion	Enthält die Implementierung zur Vorberechnung der Runden-schlüssel.
enlighten	Enthält die Implementierung für das Kopieren des BMP-Datei-Headers aus der ursprünglichen in die verschlüsselte Datei, damit diese durch ein Bildprogramm dargestellt werden kann.
bufferio	Enthält Library-Funktionen, die das Lesen aus und Schreiben in Dateien ermöglichen.
references	Enthält die RFC2040-Referenzimplementierung.



## 4.2 Dateiaufbau

Im Folgenden ist der Aufbau einer von der RC5-Implementierung verschlüsselten Datei aufgezeigt, wobei der Initialisierungsvektor selbst nicht verschlüsselt wird.

Plaintext	Padding	Initialisierungsvektor
-----------	---------	------------------------

Siehe 3.1 Initialisierungsvektor für dessen nähere Beschreibung.

## 4.3 Optimierungen

**Einmaliges Ausführen der Schlüsselexpansion** Ein bei gleicher Rundenanzahl und Blockgröße stets gleich bleibender Schritt bei der Ver- und Entschlüsselung ist die Schlüsselexpansion. Diese hängt nur von den Nothing-Up-My-Sleeve-Zahlen  $P$  und  $Q$  ab und muss daher im Voraus nur einmal berechnet werden. Die resultierenden Rundenschlüssel werden in der data-Section unseres Assemblerprogramms gespeichert, um sie beim Key-Mixing weiterzuverwenden. Der Code zur Schlüsselexpansion ist separat in den Dateien `key_expansion.c` und `key_expansion.S` zu finden.

**Laden der Rundenschlüssel in SSE-Register** Für jede Runde von RC5 werden zwei der  $2r + 2$  Rundenschlüssel verwendet. Um die Anzahl der Speicherzugriffe zu minimieren, laden wir alle vier Runden acht neue 16-Bit Schlüssel in ein SSE-Register. Die Schlüssel werden daraufhin nacheinander in die niederwertigsten Bits rotiert und von dort zur Weiterverarbeitung in ein Standardregister geladen.

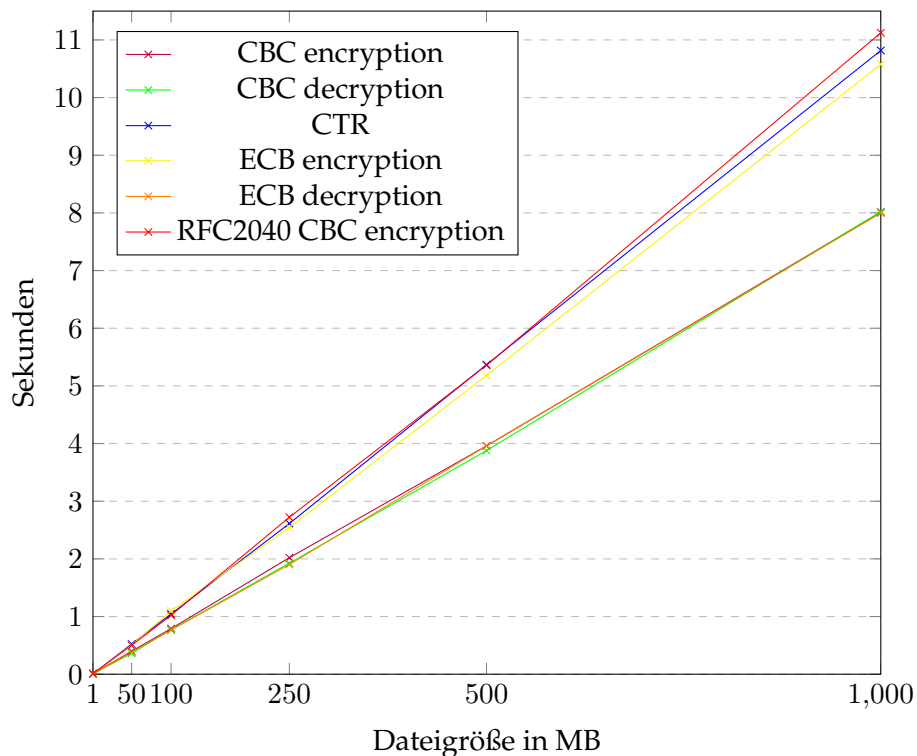
# 5 Ergebnisse

## 5.1 Korrektheit

Zur Überprüfung der Korrektheit haben wir die Ergebnisse unserer Implementierung mit denen einer Referenzimplementierung verglichen. Die Referenzimplementierung, die wir verwenden, ist in RFC2040 der IETF enthalten [1]. Testfälle können mit dem `test-Command` ausgeführt werden.

## 5.2 Performance

Vergleich der Betriebsmodi inkl. der Referenzimplementierung



Die Entschlüsselung mit dem CBC/ECB-Modus nutzt jeweils die Assemblerfunktion `rc5_dec` und hat daher eine vergleichbare Laufzeit. Die Laufzeit der Verschlüsselung mit CBC ist ähnlich, da hier die zu `rc5_dec` vergleichbare Assemblerfunktion `rc5_enc` verwendet wird. Im Vergleich zur RFC2040-Implementierung ist unsere Assemblerimplementierung um bis zu 26% schneller.

Obwohl der Counter Mode sowie die Verschlüsselung im ECB-Modus mit SIMD-Instruktionen 8 Blöcke parallel verschlüsseln, sind sie deutlich langsamer als die übrigen Implementierungen. Die Konstruktion der Chiffre bedingt, dass die beiden Halblöcke jedes Blocks um den Wert des jeweils anderen Block rotiert werden müssen. Daher müssen die 8 Blöcke hier temporär aus den SSE-Registern geladen und einzeln rotiert werden.

### 5.2.1 Vergleich des Assembler-Codes

Für die Performance ist entscheidend, wie ein einzelner Block verschlüsselt wird. Im Folgenden ist der Code für eine Runde der RC5-Chiffre von unserer und der RFC2040-Implementierung zu sehen:

**Unsere Implementierung**

```
movd r11d, xmm0
pshufd xmm0, xmm0, 0b00111001
xor r9w, r10w
mov cl, r10b
rol r9w, cl
add r9w, r11w
```

```
shr r11d, 16
xor r10w, r9w
mov cl, r9b
rol r10w, cl
add r10w, r11w
add rax, 2
```

**RFC2040-Implementierung**

```
mov ecx, eax
xor r8d, eax
add rdx, 0x4
and ecx, 0xf
rol r8w, cl
add r8w, WORD PTR [rdx-0x4]
```

```
mov ecx, r8d
xor eax, r8d
and ecx, 0xf
rol ax, cl
add ax, WORD PTR [rdx-0x2]
```

Der Code ist in die Verschlüsselung des linken und des rechten Halbblocks aufgeteilt. Es ist deutlich zu erkennen, dass wir während der Verschlüsselung auf ein Laden der Rundenschlüssel verzichten. Stattdessen werden bei Bedarf acht neue Rundenschlüssel in `xmm0` geladen (hier nicht gezeigt). Bei der RFC2040-Implementierung wird jeder Rundenschlüssel einzeln aus dem Speicher geladen.

## 6 Zusammenfassung

Die RC5-Chiffre wurde mit unterschiedlichen Betriebsmodi erfolgreich implementiert und mit einer Referenzimplementierung verglichen. Es konnte gezeigt werden, dass der Einsatz von SSE-Registern zum Laden der Rundenschlüssel für eine deutliche Performance-Steigerung sorgt.

Aufgrund der Konstruktion der RC5-Chiffre eignet sich hingegen der Einsatz von SSE-Instruktionen für das parallele Verschlüsseln mehrerer Blöcke in SSE-Registern nicht. Die Implementierung der Modi CTR und ECB könnte durch das parallele Verschlüsseln der Blöcke auf mehreren Hardware-Threads weiter beschleunigt werden. Weiterhin könnte das Anwendungsspektrum der Implementierung durch eine variable Wahl der Blockgröße und Rundenanzahl erweitert werden.

## Literatur

- [1] Ronald L. Rivest & Robert W. Baldwin.  
*[RFC2040] The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms.*  
URL: <https://tools.ietf.org/html/rfc2040>. (aufgerufen: 22.07.2019).
  - [2] Limor Elbaz & Hagai Bar-El. „Strength Assessment of Encryption Algorithms“. In: (Okt. 2000). URL: <https://pdfs.semanticscholar.org/03cb/17aad62a46d0fad1133f9656ff0f8a4e39dc.pdf>. (aufgerufen: 06.07.2019).
  - [3] H. M. Heys. „Linearly Weak Keys of RC5“. In: (Mai 1997). URL: <https://pdfs.semanticscholar.org/f4cb/0acab4eb24a74e49f9ce909496b10d62b266c.pdf>. (aufgerufen: 06.07.2019).
  - [4] R. Housley. *[RFC5652] Cryptographic Message Syntax (CMS).*  
URL: <https://tools.ietf.org/html/rfc5652>. (aufgerufen: 29.06.2019).
  - [5] E. Jorjipii & P. Rogaway M. Bellare A. Desai.  
„A Concrete Security Treatment of Symmetric Encryption“. In: (Sep. 2000).  
URL: <https://web.cs.ucdavis.edu/~rogaway/papers/sym-enc.pdf>.  
(aufgerufen: 23.07.2019).
  - [6] Lars R. Knudsen & Willi Meier. „Improved Differential Attacks on RC5“. In: Nov. 1998.  
URL: [https://link.springer.com/content/pdf/10.1007%2F3-540-68697-5\\_17.pdf](https://link.springer.com/content/pdf/10.1007%2F3-540-68697-5_17.pdf).  
(aufgerufen: 06.07.2019).
  - [7] Ian Goldberg & David Wagner Nikita Borisov.  
*Intercepting Mobile Communications: The Insecurity of 802.11.*  
URL: <http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>.  
(aufgerufen: 19.07.2019).
  - [8] Ronald L. Rivest. „The RC5 Encryption Algorithm\*“. In: (März 1997).  
URL: <http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf>.  
(aufgerufen: 06.07.2019).
  - [9] Thai Duong & Juliano Rizzo. „Here Come The  $\oplus$  Ninjas“. In: (Mai 2011). URL:  
[https://pdfs.semanticscholar.org/6446/4198f4e6c10611cfb7dfe26bbb7ca4ddd344.pdf?\\_ga=2.101213126.61480899.1563551514-712018161.1563551514](https://pdfs.semanticscholar.org/6446/4198f4e6c10611cfb7dfe26bbb7ca4ddd344.pdf?_ga=2.101213126.61480899.1563551514-712018161.1563551514).  
(aufgerufen: 19.07.2019).
  - [10] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.*  
John Wiley & Sons, 1996. ISBN: 0471117099.
  - [11] Bundesamt für Sicherheit und Informationstechnik.  
*Cryptographic Mechanisms: Recommendations and Key Lengths.*  
Technical Guideline TR-02102-1. Jan. 2019.  
URL: [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?\\_\\_blob=publicationFile&v=9](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=9).  
(aufgerufen: 06.07.2019).
  - [12] Jacques Patarin & Emmanuel Volte Valerie Nachev.  
*Feistel Ciphers: Security Proofs and Cryptanalysis.* Springer, 2017. ISBN: 9783319495309.
  - [13] Burton S. Kaliski Jr. & Yiqun Lisa Yin. *On the Security of the RC5 Encryption Algorithm.*  
Technical Report TR-602. Version 1.0. RSA Laboratories, Sep. 1998.
-