

Twister - A new hash function proposal

Ewan Fleischmann, Christian Forler, Michael Gorski, Stefan Lucks

Bauhaus Universität Weimar und Sirrix AG

9. Kryptotag Gelsenkirchen

10. November 2008

Themen

- 1 Einleitung
- 2 Kompressionsfunktion
 - Mini-Runde
 - Maxi-Runde
- 3 Ausgabe-Runde
- 4 Kryptoanalyse
- 5 Performance

Motivation

- August 2004: Xiaoyun Wang, Dengguo Feng, Xuejia Lai und Hongbo Yu publizieren praktischen Angriff auf MD5.
- August 2005: Xiaoyun Wang, Andrew Yao und Frances Yao publizieren praktikablen Angriff auf SHA-1.
- November 2007: NIST kündigt SHA3 Wettbewerb an.
- Oktober 2008: Anmeldeschluss für SHA-3 Kandidaten.

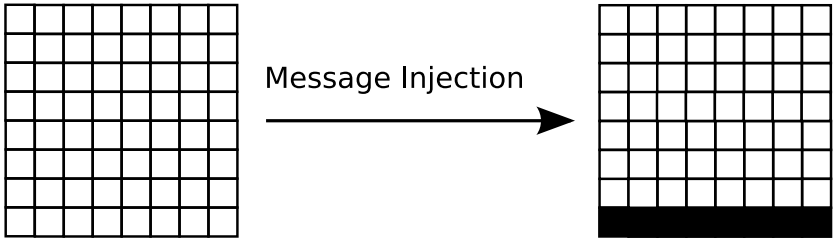
Daten

- Vorbilder: AES und Grindahl.
- Variable Hashlänge: 32-512 Bit.
- Die Kompressionsfunktion verarbeitet 512-Bit Nachrichtenblöcke.
- Kernidee 8x8 Byte Zustandmatrix mit Elementen aus $G(2^8)$.
- Sponge Konstruktion.

Themen

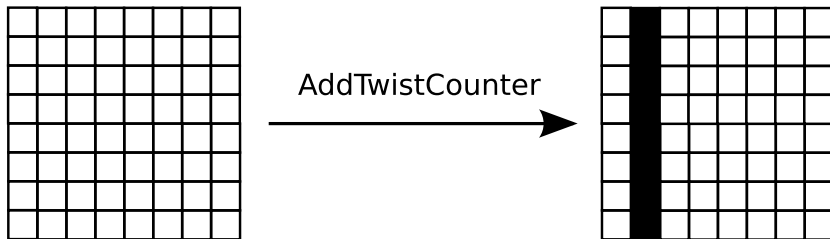
- 1 Einleitung
- 2 **Kompressionsfunktion**
 - Mini-Runde
 - Maxi-Runde
- 3 Ausgabe-Runde
- 4 Kryptoanalyse
- 5 Performance

Message Injection



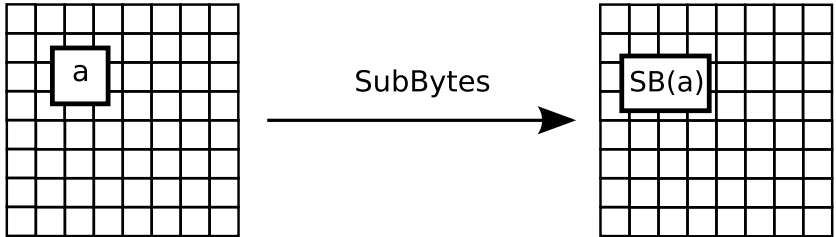
XOR Verknüpfung eines 8-Byte Nachrichtenblockes mit letzten Spalte.

Add TwistCounter



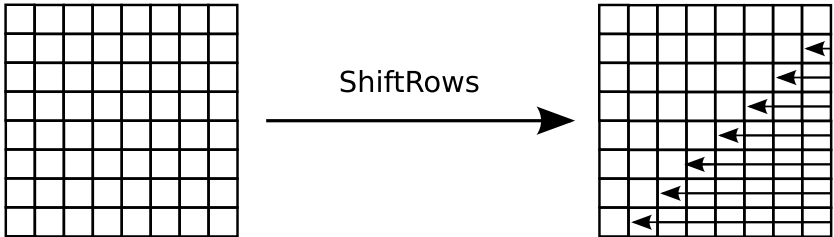
- XOR Verknüpfung TwistCounters mit Spalte 2.
- Dekrementierung des TwistCounters um 1.
- Startwert: $0xFFFFFFFFFFFFFFFF$.
- Immunisiert gegen Slide-Attacken.

Sub Bytes



- Byteweise AES-Sbox Operation.
- Zerstört die Linearität der Mini-Runde.

Shift Rows



Die Einträge der i -ten Spalte werden um $(i-1)$ Felder nach links rotiert.

Mix Columns



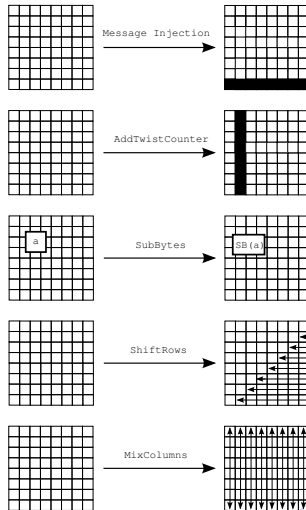
- Multiplikation mit MDS-Matrix.
- Sorgt mit *Shift Rows* für hohe Diffusion.
- Erschwert differentielle Kryptoanalyse.

MDS Matrix

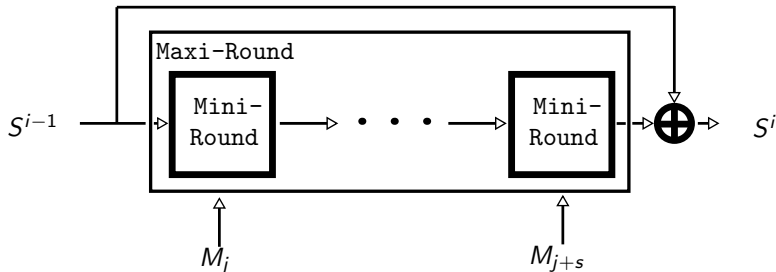
$$MDS = \begin{pmatrix} 02 & 01 & 01 & 05 & 07 & 08 & 06 & 01 \\ 01 & 02 & 01 & 01 & 05 & 07 & 08 & 06 \\ 06 & 01 & 02 & 01 & 01 & 05 & 07 & 08 \\ 08 & 06 & 01 & 02 & 01 & 01 & 05 & 07 \\ 07 & 08 & 06 & 01 & 02 & 01 & 01 & 05 \\ 05 & 07 & 08 & 06 & 01 & 02 & 01 & 01 \\ 01 & 05 & 07 & 08 & 06 & 01 & 02 & 01 \\ 01 & 01 & 05 & 07 & 08 & 06 & 01 & 02 \end{pmatrix}$$

- Zyklische rechts Rotation von (02 01 01 05 07 08 06 01).
- Häufiges auftreten des neutrales Elements der Multiplikation.
- Elemente 3,4 und 9 treten nicht auf.
- Branch number ist 9.

Übersicht



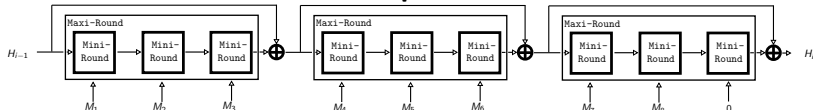
Maxi-Runde



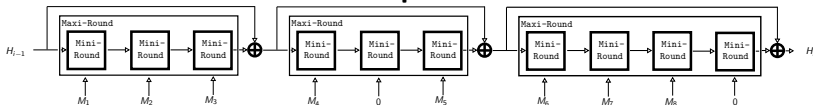
- Eine Maxi-Runde besteht aus
 - Mehreren Mini-Runden.
 - Globales Feedforward.
- Maxi-Runde ist nicht invertierbar wie Mini-Runde.

Kompressionsfunktion

Twister-256 Kompressionsfunktion



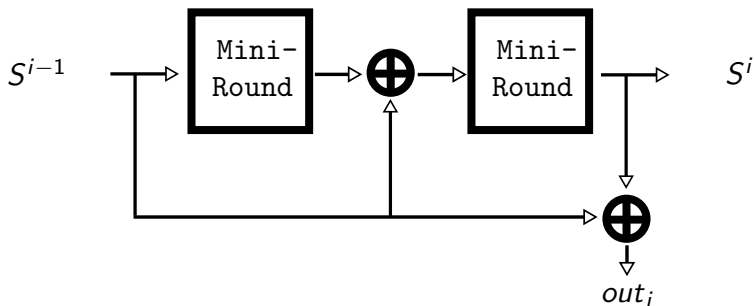
Twister-512 Kompressionsfunktion



Themen

- 1 Einleitung
- 2 Kompressionsfunktion
 - Mini-Runde
 - Maxi-Runde
- 3 Ausgabe-Runde**
- 4 Kryptoanalyse
- 5 Performance

Output-Round



Die Ausgabe-Runde gibt den 64-Bit Block $S_{(1,\downarrow)}^i \oplus S_{(1,\downarrow)}^{i-1}$ aus.

Themen

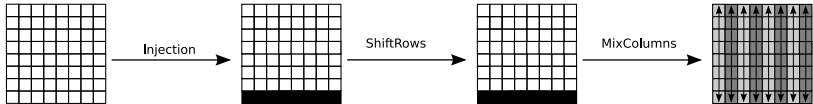
- 1 Einleitung
- 2 Kompressionsfunktion
 - Mini-Runde
 - Maxi-Runde
- 3 Ausgabe-Runde
- 4 **Kryptoanalyse**
- 5 Performance

Kryptoanalyse

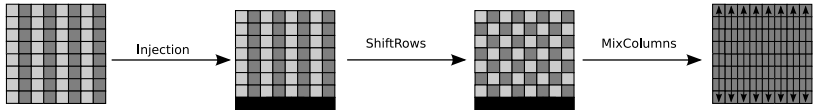
- Innerhalb einer Mini-Runde kann keine Kollision auftreten.
- TwistCounter verhindert Slide-Attacken.
- Vollständige Diffusion nach zwei Mini-Runden.
- Feedforward und Sponge-Design erschweren Preimage- und Kollisions-Angriffe.

Vollständige Diffusion

First Mini-Round



Second Mini-Round



Nach zwei Mini-Runden herrscht vollständige Diffusion.

Themen

- 1 Einleitung
- 2 Kompressionsfunktion
 - Mini-Runde
 - Maxi-Runde
- 3 Ausgabe-Runde
- 4 Kryptoanalyse
- 5 Performance

32-Bit Benchmarks

Setup

- Hardware: Core2Duo T7300 (2.0 GHz), 2048 MB RAM
- OS: GNU Debian *Lenny*, Kernel 2.6.26-1
- Compiler: GCC 4.1

Ergebnisse

<i>SHA-256</i> :	29.3 cycles per byte
<i>Twister-256</i> :	35.8 cycles per byte
<i>SHA-512</i> :	55.2 cycles per byte
<i>Twister-512</i> :	39.6 cycles per byte

64-Bit Benchmarks

Setup

- Hardware: Core2Duo T7300 (2.0 GHz), 2048 MB RAM
- OS: GNU Debian *Lenny*, Kernel 2.6.26-1
- Compiler: GCC 4.3

Ergebnisse

<i>SHA-256</i> :	20.1 cycles per byte
<i>Twister-256</i> :	15.8 cycles per byte
<i>SHA-512</i> :	13.1 cycles per byte
<i>Twister-512</i> :	17.5 cycles per byte

Twister Zusammenfassung

- Kompressionsfunktion besteht aus drei Einfachen Maxi-Runden.
- Eine Maxi-Runde besteht aus 3-4 Mini-Runden.
- Interner Zustand ist eine 8×8 Byte-Matrix.
- Sponge-Ausgabe.
- Sehr schnelle Diffusion.
- Performant auf 32- und 64-Bit Architekturen.

Fragen?