

KronCrypt

Der Approximationssatz von Kronecker in der symmetrischen Kryptografie

Carsten Elsner, Martin Schmidt

Fachhochschule für die Wirtschaft (FHDW) Hannover

9. Kryptotag, 10.11.2008, FH Gelsenkirchen

Überblick

- 1 Diophantische Approximation
- 2 KronCrypt
- 3 Kryptografische Analysen
- 4 Fazit

Überblick

1 Diophantische Approximation

2 KronCrypt

3 Kryptografische Analysen

4 Fazit

Diophantische Approximation

Kettenbrüche

- Ein *Kettenbruch* ist ein Ausdruck der Form:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_{N-1} + \frac{1}{a_N}}}}}$$

- Schreibweise: $[a_0; a_1, \dots, a_N]$
- Die $a_i, i = 0, \dots, N$, heißen *Teilnenner*
- *Einfache* Kettenbrüche: $a_0 \in \mathbb{Z}, a_i \in \mathbb{N}, i = 1, \dots, N$
- *Normierter* Kettenbruch: $a_N \neq 1$

Diophantische Approximation

Rationale Zahl \leftrightarrow Kettenbruch

Euklidischer Algorithmus:

$$43 = 1 \cdot 30 + 13$$

$$30 = 2 \cdot 13 + 4$$

$$13 = 3 \cdot 4 + 1$$

$$4 = 4 \cdot 1$$

Folge der Quotienten ist die Kettenbruchentwicklung der rationalen Zahl:

$$[1; 2, 3, 4] = \frac{43}{30}$$

Diophantische Approximation

Näherungsbrüche 1

- Eine abbrechende Kettenbruchentwicklung

$$[a_0; a_1, \dots, a_n] := \frac{p_n}{q_n}, \quad n \leq N$$

nennt man einen *Näherungsbruch*.

- Rekursionsformeln:

$$\begin{aligned} p_0 &= a_0, & p_1 &= a_1 a_0 + 1, & p_n &= a_n p_{n-1} + p_{n-2}, & (2 \leq n \leq N), \\ q_0 &= 1, & q_1 &= a_1, & q_n &= a_n q_{n-1} + q_{n-2}, & (2 \leq n \leq N). \end{aligned}$$

Diophantische Approximation

Der Approximationssatz von Kronecker (1823-1891)

Für jedes $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, jedes $\eta \in \mathbb{R}$, jedes $n > 0$ und jedes $\delta \in \mathbb{R}$ mit $\delta > 0$ gibt es ganze Zahlen p, q mit $q > n$ und

$$|q\alpha - p - \eta| < \left(\frac{1}{2} + \frac{1}{\sqrt{5}} + \delta \right) \frac{1}{q}.$$

Überblick

1 Diophantische Approximation

2 KronCrypt

3 Kryptografische Analysen

4 Fazit

- 128 Bit Blockchiffre
- Schlüssel κ : Teilnennerfolge/Näherungsbruch (≥ 128 Bit)
- Feistelchiffre: $r = 6$ Runden, interne Rundenfunktion f
- Rundenfunktion f besteht aus ...
 - ▶ ... $s \in \{2, 4, 8\}$ parallel verwendeten schlüsselabhängigen S-Boxen
 - ▶ ... XORs und Additionen modulo 2^{64}
- Schlüsselgenerator: Berechnung der Rundenschlüssel $\kappa_i, i = 1, \dots, r$, aus dem KronCrypt-Schlüssel κ

- Parameter $s_1, s_2, m, l, K \in \mathbb{Z}$ mit
 - ▶ S-Boxen werden iteriert $\rightsquigarrow \sigma : \{0, 1\}^{s_1} \rightarrow \{0, 1\}^{s_2}$
 - ▶ s_1 : Eingabelänge (in Bit) der S-Boxen
 - ▶ l : Anzahl der Iterationen pro S-Box
 - ▶ m : Hinzukommende Bits pro S-Box-Iteration
 - ▶ s_2 : Ausgabelänge (in Bit) der S-Boxen ($s_2 = s_1 + m \cdot l$)
 - ▶ K : Hilfsparameter mit $2^{m-1} \geq K + 2$
- KronCrypt-Schlüssel: Gleichverteilte Folge von Teilennennern aus $l := [K, 2K - 1] \rightsquigarrow \kappa = [0; a_0, a_1, \dots, a_{\nu-1}]$ mit Ganzzahlteil 0
- Äquivalent: via Rekursionsformeln berechneter Näherungsbruch c/d

KronCrypt

Schlüsselgenerator: Berechnung der Rundenschlüssel κ_i aus κ

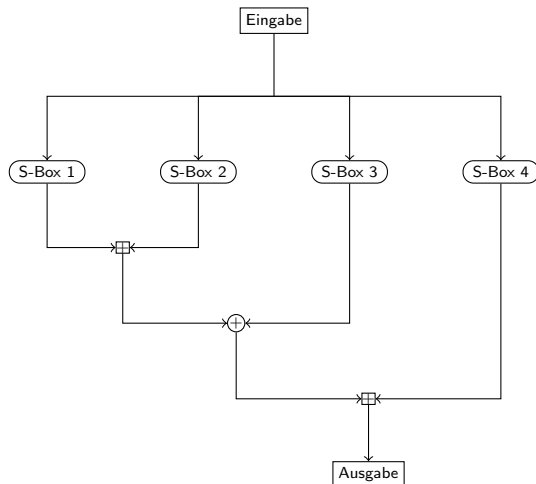
- Zyklisches Durchlaufen der $a_0, a_1, \dots, a_{\nu-1}$
- Start beim Teilnenner a_k mit $k = \lambda \cdot i \bmod \nu$, $\nu, \lambda = \left\lceil \frac{\nu}{r} \right\rceil$
- Ganzzteil = 0 $\rightsquigarrow \alpha_i = [0; a_k, a_{k+1}, \dots, a_{\nu-1}, a_0, a_1, \dots]$
- Simultane Berechnung der Näherungsbrüche $c_{i,j}/d_{i,j}$
- Abschneiden der Teilnennerfolge beim Index μ mit

$$d_{i,\mu-1} \leq \left(1 + \frac{2}{K}\right) 2^{s_1} < d_{i,\mu} \leq 2^{m+s_1}$$

- Entstehende Teilnennerfolge/Näherungsbruch ist Rundenschlüssel κ_i

KronCrypt

Die Rundenfunktion f am Beispiel $s = 4$



- l -fache Iteration
- Eine Iteration der S-Box: Lösen der inhomogenen diophantischen Ungleichung

$$|q\alpha - p - \eta| < \left(\frac{1}{2} + \frac{1}{\sqrt{5}} + \delta \right) \frac{1}{q}$$

basierend auf einem konstruktiven Beweis des Kronecker-Satzes

- Schlüsselgenerator \rightsquigarrow zu approximierendes $\alpha = \alpha_i$
- In einer Runde der Feistelchiffre: Schlüssel für alle S-Boxen gleich
- Von Runde zu Runde ändern sich die S-Boxen schlüsselabhängig
- Inhomogenität: skalierte S-Box-Eingabe
- S-Box-Ausgabe: Nenner q aus der obigen Ungleichung

- Pro Iteration: Vergrößerung der S-Box-Eingabe um $\leq m$ Bits
- Durch die Parameter s, m, l kann die Vergrößerung gesteuert werden
- Verknüpfung der s S-Box-Ausgaben: XOR und Addition modulo 2^{64}
- \rightsquigarrow Rundenfunktion $f : \{0, 1\}^{64} \rightarrow \{0, 1\}^{64}$
- Bedingung 1: $s \geq 2$
- Anzahl der S-Boxen: $s \in \{2, 4, 8\}$

$$\sigma : \begin{cases} \{0, 1\}^{32} \rightarrow \{0, 1\}^{64} & , s = 2 \\ \{0, 1\}^{16} \rightarrow \{0, 1\}^{64} & , s = 4 \\ \{0, 1\}^8 \rightarrow \{0, 1\}^{64} & , s = 8 \end{cases}$$

- Bedingung 2: $64 = s_2 = s_1 + m \cdot l$
- Bedingung 3: $l \neq \emptyset \Leftrightarrow m \geq 3$

- **Satz (Elsner):** Für einen gültigen Rundenschlüssel c/d als Näherungsbruch der Zahl α und

$$r := \left\lfloor 2^{s_1} \|q \cdot \alpha\| \right\rfloor_{\mathbb{Z}}$$

gilt $r = \rho$, wobei ρ die Eingabe der S-Box bezeichnet.

- S-Box-Eingabe lässt sich aus Ausgabe und Rundenschlüssel berechnen
- $\|\xi\| := \xi - [\xi], \xi \in \mathbb{R}_{\geq 0}$
- $\lfloor \xi \rfloor_{\mathbb{Z}} := \max \left\{ z \in \mathbb{Z} : |z - \xi| \leq \frac{1}{2} \right\}, \xi \in \mathbb{R}$

- Verknüpfung der S-Box-Ausgaben
- Ziel: Rundenfunktion

$$f : \{0, 1\}^{64} \rightarrow \{0, 1\}^{64}$$

mit gleicher binärer Ein- und Ausgabegröße

- Verwendung beider Operationen: zusätzliche Nichtlinearität
- Problem: Rundenfunktion verliert Injektivität
- Lösung: Feistel-Struktur
- Durch Elsnert'schen Satz beschriebene Umkehrung wird nicht benötigt
- Theoretische Möglichkeiten gehen über den aktuellen Einsatz hinaus

Überblick

- 1 Diophantische Approximation
- 2 KronCrypt
- 3 Kryptografische Analysen**
- 4 Fazit

Kryptografische Analysen

Untersuchte Eigenschaften

- Konfusion
- Diffusion
- Vollständigkeit
- (striktes) Avalanche-Kriterium, (S)AC

Kryptografische Analysen

Durchgeführte Analysen

- Statistische Auswirkung zufälliger Klartextänderungen
- Statistische Auswirkung zufälliger Schlüsseländerungen
- Analoge Durchführung für die S-Box und das gesamte Kryptosystem
- S-Box: $\forall s \in \{2, 4, 8\}, m, l$
- Kryptosystem: Für $r \in \{2, 4, 6, \dots\}$ Runden

Kryptografische Analysen

Ergebnisse: KronCrypt, Variabilität in der Eingabe

(s_1, s_2)	m	l	Benötigte Rundenanzahl r für SAC
(32,64)	4	8	6
(32,64)	8	4	6
(32,64)	16	2	6
(32,64)	32	1	6
(16,64)	3	16	4
(16,64)	4	12	6
(16,64)	6	8	6
(16,64)	8	6	6
(16,64)	12	4	6
(16,64)	16	3	6
(16,64)	24	2	6
(16,64)	48	1	6
(8,64)	4	14	8
(8,64)	7	8	8
(8,64)	8	7	6
(8,64)	14	4	6
(8,64)	28	2	6
(8,64)	56	1	6

Kryptografische Analysen

Ergebnisse: KronCrypt, Variabilität im Schlüssel

(s_1, s_2)	m	l	Benötigte Rundenanzahl r für SAC
(32,64)	4	8	6
(32,64)	8	4	6
(32,64)	16	2	6
(32,64)	32	1	6
(16,64)	3	16	6
(16,64)	4	12	4
(16,64)	6	8	4
(16,64)	8	6	4
(16,64)	12	4	4
(16,64)	16	3	4
(16,64)	24	2	6
(16,64)	48	1	6
(8,64)	4	14	6
(8,64)	7	8	6
(8,64)	8	7	6
(8,64)	14	4	6
(8,64)	28	2	6
(8,64)	56	1	6

Kryptografische Analysen

Differentielle & lineare Kryptoanalyse

- Enormer Berechnungsaufwand
- Differenzenverteilungstabellen der S-Boxen
 - ▶ Berechnung nur möglich für (8, 64)-S-Box
- Lineare Approximationstabellen der S-Boxen
 - ▶ Keine Berechnung möglich
- Argumente für die Sicherheit gegen DKA & LKA:
 - ▶ Berechnungskomplexität
 - ▶ Schlüsselabhängigkeit
 - ▶ Niedrige maximale Werte
 - ▶ Großer Anteil von Nullen
- Aber: weiterer Untersuchungsgegenstand

Überblick

- 1 Diophantische Approximation
- 2 KronCrypt
- 3 Kryptografische Analysen
- 4 Fazit**

Fazit

Zusammenfassung

- Neue mathematische Idee in der Kryptografie
- Neues symmetrisches Verfahren
- Detaillierte Analysen zu Konfusion, Diffusion, ...
- Erste Ergebnisse zu differentieller & linearer Kryptoanalyse

Fazit

Ausblick

- Untersuchung weiterer differentieller & linearer Attacken
- Untersuchung anderer Attacken
- Untersuchung einer möglichen Hardwareimplementierung
- Einsatzbereiche

Ende

Danke für Ihre Aufmerksamkeit!