

BDD-basierte Kryptanalyse von Flusschiffren am Beispiel des A5/1 Schlüsselstromgenerators

Dirk Stegemann

Universität Mannheim

Viele praktisch eingesetzte Flusschiffren basieren auf einer kleinen Zahl linear rückgekoppelter Schieberegister (*Linear Feedback Shift Registers*, kurz LFSRs), deren Ausgabebitströme mit Hilfe einer nichtlinearen Kompressionsfunktion zu einem Schlüsselstrom $y \in \{0, 1\}^*$ verdichtet werden.

[Kra02] identifiziert die *best case* Kompressionsrate γ und die durchschnittliche Informationsrate α der Kompressionsfunktion als entscheidende Sicherheitsparameter und beschreibt einen Angriff auf LFSR-basierte Flusschiffren, der den geheimen Initialzustand $x \in \{0, 1\}^n$ in einer Laufzeit von $n^{O(1)} 2^{\frac{1-\alpha}{1+\alpha}n}$ aus den ersten $\lceil \gamma \alpha^{-1} n \rceil$ aufeinanderfolgenden Bits des Schlüsselstroms y rekonstruiert. Die Grundlage dieses Angriffs bildet die Repräsentation der Zwischenergebnisse in Binären Entscheidungsdiagrammen (*Binary Decision Diagrams*, kurz BDDs), die bisher vor allem zur formalen Schaltkreisverifikation im VLSI-Design eingesetzt wurden. Von [Sch02] und [Ste04] durchgeführte Experimente mit verschiedenen Flusschiffren scheinen die theoretischen Resultate zu bestätigen, zeigen jedoch gleichzeitig die durch hohen Speicherbedarf bedingten Grenzen der praktischen Durchführbarkeit von BDD-basierten Angriffen auf. Am Beispiel des A5/1 Schlüsselstromgenerators [BGW99] aus dem GSM-Standard soll die BDD-basierte Kryptanalyse vorgestellt und auf Implementationsaspekte und experimentelle Resultate eingegangen werden.

Literatur

- [Kra02] M. Krause. BDD-based cryptanalysis of keystream generators. In *EUROCRYPT 2002*, Band 2332 der Reihe *Lecture Notes in Computer Science*, Seiten 222–237. Springer Verlag, Heidelberg, 2002.
- [BGW99] M. Briceno, I. Goldberg, and D. Wagner. *A pedagogical implementation of A5/1*, May 1999. <http://jya.com/a51-pi.htm>.
- [Sch02] F. Schler. Einsatz von OBDDs zur Kryptanalyse von Flusschiffren. Diplomarbeit, Universität Mannheim, 2002.
- [Ste04] D. Stegemann. Fbdd-basierte Kryptanalyse des A5/1 Schlüsselstromgenerators. Diplomarbeit, Universität Mannheim, 2004.