Ein Angriff auf Bivium mittels SAT Solver

Tobias Eibach* and Enrico Pilz†

* Universität Ulm † Universität Ulm

Trivium (und damit auch die reduzierte Variante Bivium) ist ein aussichtsreicher Stufe 2 Kandidat in dem europäischen eSTREAM Projekt. Das Design der Stromchiffre ist schlicht und elegant, vorgestellt wurde die Chiffre 2005 von Cannière und Preneel [CB05]. Bislang wurde noch kein wirkungsvoller Angriff auf die Chiffre gefunden.

Zu den bekanntesten Angriffen auf Strom Chiffren zählen die Algebraischen Angriffe, die darauf abzielen ein Gleichungssystem aufzustellen und zu lösen. Bekannte Verfahren hierbei sind der F4- und F5-Algorithmus die auf Gröbner Basen basieren, die sich in Softwarepaketen wie Magma und Singular finden.

In [BCJ07] wird vorgeschlagen SAT Solver zum Lösen solcher (dünner) Gleichungssysteme zu verwenden und dieser Gedanke wird in [MCP07] speziell auf Bivium angewendet und durchgeführt. Hierin wurden auch erste interessante experimentelle Ergebnisse veröffentlicht.

SAT Solver sind seit langer Zeit Forschungsgegenstand der Theoretischen Informatik, es geht darum, die Erfüllbarkeit von Booleschen Formeln (in CNF) zu überprüfen und ggf. eine Lösung auszugeben. Das Erfüllbarkeitsproblem ist das kanonische NP-vollständige Problem, man geht davon aus, dass es keinen Algorithmus gibt, der das Problem in polynomieller Laufzeit lösen kann. Trotz dieser theoretisch nicht-effizienten Laufzeit ging viel Forschungsarbeit in die Entwicklung von möglichst effizienten SAT Algorithmen, die hoch optimiert sind und auf Teilklassen (hier: „industrial instances“) besonders schnell arbeiten.

Für den Angriff auf Stromchiffren bedeutet das: Zuerst muss das Problem in ein Gleichungssystem umgeformt werden (dessen Lösung der gesuchte interne Zustand der Chiffre ist). Das algebraische Gleichungssystem wird dann in eine äquivalente CNF transformiert, die dann als Eingabe für einen SAT Solver dient.

Den oben beschriebenen Angriff haben wir implementiert und damit die Ergebnisse aus [MCP07] überprüft und weitere Experimente durchgeführt. Teilweise konnten wir Ergebnisse bestätigen, teilweise nicht. Neue Ergebnisse betreffen Fragestellungen auf dem Weg zu einem möglichst effizienten Angriff und sollen in dem Vortrag vorgestellt werden. Zum Bsp. geben wir eine empirische Antwort darauf, welche Bits des internen Zustandes am 'wertvollsten' sind und somit am besten 'erraten' werden sollten. Auerdem haben wir untersucht welcher SAT solver am Besten für diese Problemklasse geeignet ist und ob mehr Redundanz im Gleichungssystem das Problem einfacher macht. Abschlieend wird noch vorgestellt welche Fragestellungen wir in den nchsten Wochen noch untersuchen werden.

Literatur

[CB05] Cannière and Preneel. *TRIVIUM - a stream cipher construction inspired by block cipher design principles*, 2005.

[BCJ07] Bard and Courtois and Jefferson. *Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariat Polynomials over GF(2) via SAT-Solvers*,2007.

[MCP07] Cameron McDonals and Chris Charnes and Josef Pieprzyk. *Attacking Bivium with MiniSat*, 2007.