Auf der Suche nach schwachen Schlüsseln bei Trivium

Deike Priemuth-Schmid und Alex Biryukov

Laboratory of Algorithmics, Cryptology and Security
University of Luxembourg
e-mail: deike.priemuth-schmid@uni.lu, alex.biryukov@uni.lu

Die Stromchiffre Trivium wurde als Kandidat für das eSTREAM-Projekt [ECR05] im Jahr 2005 von C. De Cannière und B. Preneel [CP05] entwickelt. Seit der Veröffentlichung von Trivium wurde das Design der Chiffre nicht geändert, denn auch nach $2\frac{1}{2}$ Jahren gibt es keine wirklichen Angriffe auf Trivium. Dies und seine sehr guten Eigenschaften im Bereich Performanz und das geringe Zeit-Flächen-Produkt machen Trivium zu einer interessanten Stromchiffre.

Trivium verwendet einen 80 Bit Schlüssel, einen 80 Bit Initialwert und eine nichtlineare Update-Funktion. Von den Designern wurde die Chiffre mit einem 288 Bit Register vorgestellt, welches jedoch auf natürliche Weise in drei Register der Länge 93, 84 und 111 Bit zerfällt. Mit jeder Taktung der Chiffre wird diese aktualisiert und ein Schlüsselstrombit ausgegeben. Die maximale Anzahl an Schlüsselstrombits pro Schlüssel-Initialwert-Paar wurde von den Designern mit 2^{64} Bits festgelegt. Im Key-Setup wird der Schlüssel in das erste und der Initialwert in das zweite Register geladen, jeweils beginnend mit den ersten 80 Bit. Alle restlichen Bits werden mit Null initialisiert, mit Ausnahme der letzten 3 Bit des dritten Registers, welche auf Eins gesetzt werden. Dieser Zustand mit Schlüssel, Initialwert und den fest gesetzten Bits ist der Startzustand. Nachdem alle Bits initialisiert sind, wird das Register 4×288 mal unter Verwendung der Update-Funktion getaktet, ohne dass Schlüsselstrombits produziert werden. Danach beginnt die Erzeugung des Schlüsselstroms.

Wir untersuchen die Fragestellung, ob es Paare von Schlüsseln und Initialwerten gibt, welche wieder einen Startzustand reproduzieren, wie erstmals von Jin Hong [JH05] erwähnt. Im Startzustand sind 128 Bits festgelegt. Nutzen wir diese festen Positionen, um den zweiten Startzustand als Gleichungssystem darzustellen, so erhalten wir 128 Gleichungen in 160 Variablen, davon jeweils 80 Schlüssel- und Initialwertbits. Der maximale Grad dieser Gleichungen beträgt entweder 3 oder 4. Da die Anzahl der Variablen größer ist, als die der Gleichungen, erhalten wir 2^{32} mögliche Lösungen für das Gleichungssystem. Unser Ziel ist die effiziente Beschreibung dieser Lösungen. Desweiteren wollen wir auch andere Chiffren auf solche schwachen Schlüssel untersuchen.

Literatur

[CP05] C. De Cannière and B. Preneel. *TRIVIUM - a stream cipher construction inspired by block cipher design principles.* eSTREAM, ECRYPT Stream Cipher Projekt, Report 2005/030, 2005. http://www.ecrypt.eu.org/stream

[ECR05] eSTREAM: The ECRYPT Stream Cipher Projekt, http://www.ecrypt.eu.org/stream/

[JH05] Jin Hong. Discussion Forum. *certain pairs of key-IV pairs for Trivium*, created September 13, 2005 05:11PM. http://www.ecrypt.eu.org/stream/phorum/read.php?1,152