Entropieberechnung des inneren Zustandes eines FCSR's

Andrea Röck

Projet CODES, INRIA Paris-Rocquencourt, France

Lineare rückgekoppelte Schieberegister (LFSR) sind weitverbreitete Primitive in der Kryptographie. Um deren Linearität zu vermeiden, kann auf die nichtlineare Variante des rückgekoppelten Schieberegisters mit Übertrag (engl. Feedback with Carry Shift Register, kurz FCSR) ausgewichen werden, wie z.B. im Fall des eSTREAM Kandidaten F-FCSR [AB05] für eine Stromchiffre.

Ein FCSR ist ein endlicher Automat, welcher unabhängig von Klapper und Goresky [KG97], Marsaglia und Zamand [MZ91] und Couture und L'Ecuyer [CL94] eingeführt wurde. Er ist ähnlich aufgebaut wie ein LFSR, jedoch wird für die Rückkopplung nicht ein XOR, sondern eine Addition mit Übertrag angewandt. Daher benötigen wir an jeder Rückkopplungsposition einen zusätzlichen Speicherplatz für den Übertrag. Im Folgenden betrachten wir binäre FCSR's.

Wir interessieren uns für die Entropie des inneren Zustandes des FCSR's. Eine verringerte Entropie erleichtert es einem Angreifer, den Wert des Zustandes und somit die nachfolgende Ausgangssequenz des FCSR's zu erraten. Nehmen wir an, der innere Zustand des FCSR's bestehe aus einem Hauptregister der Länge n und ℓ Übertragsbits an den Rückkopplungspositionen. Unter der Vorraussetzung, dass der Anfangszustand jeden der $2^{n+\ell}$ möglichen Werte mit der gleichen Wahrscheinlichkeit annimmt, hat dieser FCSR eine Anfangsentropie von $n+\ell$ Bits. Da die Iteration des FCSR's keine bijektive Funktion ist, wird die Entropie mit jeder Iteration solange verringert, bis der FCSR einen periodischen Kreislauf erreicht. Ab diesem Zeitpunkt verhält sich eine Iteration wie die Anwendung einer Permutation, und die Entropie bleibt konstant.

Im Allgemeinen sinkt die Entropie des inneren Zustandes relativ schnell. Arnault, Berger und Minier zeigen in [ABM07], dass ein FCSR mit maximaler Periode seinen periodischen Kreislauf und somit seine endgültige Entropie nach maximal $n+3$ Iterationen erreicht. Indem wir betrachten, von wie vielen Zuständen ein bestimmter Zustand erzeugt werden kann, können wir zeigen, dass schon nach einer Iteration die Entropie auf $n+\frac{\ell}{2}$ Bits absinkt. Zusäztlich können wir einen Algorithmus angeben, welcher die endgültige Entropie für einen beliebigen FCSR berechnet. Dieser Algorithmus kann auch verwendet werden, um zu zeigen, dass die Entropie immer größer als n Bits ist, und dass die Verschiebung einer Rückkopplungsposition um eine Stelle in Richtung des höchstwertigen Bits die Entropie erhöht.

Literatur

[AB05] F. Arnault and T. P. Berger. F-FCSR: Design of a new class of stream ciphers. In *FSE*, Lecture Notes in Computer Science, pages 83–97. Springer, 2005.

[ABM07] F. Arnault, T. P. Berger, and M. Minier. On the security of FCSR-based pseudorandom generators. In *SASC 2007 - ECRYPT Workshop on stream ciphers*, January 2007.

[CL94] R. Couture and P. L'Ecuyer. On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. *Math. Comput.*, 62(206):799–808, 1994.

[KG97] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptology*, 10(2):111–147, 1997.

[MZ91] G Marsaglia and A Zaman. A new class of random number generators. *Annals of Appl. Prob.*, 1(3):462–480, 1991.