Dirk Fox

Linear Rückgekoppelte Schieberegister

Nach wie vor spielen linear rückgekoppelte Schieberegister eine wichtige, wenn auch gelegentlich unrühmliche Rolle in der Kryptographie, da deren Sicherheitsschwächen oft durch Geheimhaltung „vertuscht" werden – mit zumeist begrenztem Erfolg.

Hintergrund

Unter einem Schieberegister versteht man eine Folge von *n* hintereinander geschalteten „Registern" (in der Regel binäre Speichereinheiten), deren Inhalte getaktet „weitergeschoben" werden. Schieberegister lassen sich in Hardware sehr einfach realisieren und arbeiten sehr schnell, da jede „Schiebeoperation" unabhängig von der Länge *n* des Schieberegisters nur einen Prozessortakt erfordert.

Für kryptographische Anwendungen interessant sind Schieberegister, deren Inhalte „rückgekoppelt" werden, d. h. deren Ausgabebits mit den Werten einzelner Register logisch verknüpft (in der Regel durch ein „Exklusiv-Oder", XOR) und anschließend wieder als Eingabe in das erste Register „hineingeschoben" werden (siehe Abbildung).

Solche linear rückgekoppelten Schieberegister (englisch: *linear feedback shift register*, LFSR) lassen sich mathematisch gut beschreiben und haben interessante Eigenschaften. So lässt sich ein *n*-stufiges LFSR durch ein so genanntes Rückkoppelungspolynom (auch: charakteristisches Polynom) beschreiben. Die Koeffizienten des Polynoms beschreiben die Rückkoppelungsstellen. Das Polynom rechnet über dem endlichen Zahlkörper $Z_2 = \{0, 1\}$. Das dreistufige LFSR aus der Abbildung hat das Rückkoppelungspolynom x^3+x^2+1.

Ein *n*-stufiges, linear rückgekoppeltes Schieberegister erzeugt eine Ausgabefolge mit einer maximalen Periode von 2^n-1, sofern es mit einem Startwert (Initialisierungsvektor) ungleich dem Null-Vektor belegt wird. Die maximale Periode wird erreicht, wenn das das Schieberegister beschreibende Rückkopplungspolynom irreduzibel ist (also nicht in das Produkt zweier Polynome zerlegt werden kann); ein solches charakteristisches Polynom wird auch „primitives Polynom" genannt. Das Rückkoppelungspolynom des dreistufigen LFSR aus der Abbildung ist irreduziebel; es erzeugt daher eine Binärfolge der Periode 2^3-1 = 7.

Das ist eine schöne Eigenschaft, lässt sich doch so eine quasi-zufällige Zahlenfolge erzeugen, deren Periode exponentiell mit der Länge *n* des Schieberegisters wächst. Für *n* = 10 hat die Ausgabe eine Periode von 1.023, mit *n* = 16 erreicht man eine Periodenlänge von 65.535, und bei einer Schieberegisterlänge von *n* = 32 dauert es fast 4,3 Milliarden Takte, bis sich die Binärfolge wiederholt.

Einsatz

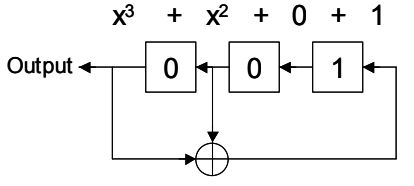
Geradezu auf der Hand liegt der Einsatz eines LFSR zur Erzeugung von pseudozufälligen Binärfolgen. Damit sie nicht vorhersagbar sind, müssen das Rückkoppelungspolynom (der „Schlüssel" des LFSR) und der Initialisierungsvektor (IV) geheim gehalten werden. Das ist allerdings schwierig, da sich das Polynom schon aus einer 2*n* bit langen Zufallsfolge errechnen lässt (s. u.).

Häufig wurden rückgekoppelte Schieberegister auch als Stromchiffre eingesetzt: Der pseudozufällige Binärstrom („Schlüsselstrom") wurde dazu mit den Bits des Datenstroms XOR-verknüpft.

Sicherheit

Ein *n*-stufiges linear rückgekoppeltes Schieberegister kann mathematisch als eine binäre Gleichung betrachtet werden, deren *n*+1-tes Bit sich aus den vorausgegangenen *n* Bits errechnet.
Kennt ein Angreifer 2*n* aufeinander folgende Ausgabebits des LFSR, kann er ein

Abbildung 1



lineares binäres Gleichungssystem aus *n* Gleichungen aufstellen. Die *n* Unbekannten des Gleichungssystems sind genau die Rückkoppelungsstellen des Schieberegisters (oder die Koeffizienten des charakteristischen Polynoms). Dieses Gleichungssystem lässt sich selbst für „große" *n* (>80) in wenigen Sekunden lösen und liefert den „Schlüssel" des LFSR, das Rückkoppelungspolynom.

Schutz vor einer solchen Analyse bieten nur Systeme, die verhindern, dass ein Angreifer Zugriff auf eine 2*n* bit lange Folge des Schlüsselstroms (oder der Pseudozufallsdaten) erhält. Das ist praktisch jedoch schwierig, denn wenn ein Angreifer den Klartext einer verschlüsselten Nachricht kennt, erhält er daraus durch XOR-Verknüpfung den Schlüsselstrom – oder er wartet ab, bis das System einen „leeren" Datenstrom (eine Folge von 0-Bits) verschlüsselt.

Daher arbeiten die meisten der heute noch zur Verschlüsselung eingesetzten Schieberegister-Algorithmen entweder mit einer nichtlinearen Verknüpfung mehrerer LFSR, wie z. B. der A5/1 (gebrochen 1997), der A5/2 bei GSM (gebrochen 2006) und der E0 bei Bluetooth, oder aber mit einer „Filterfunktion", die den Output aus der logischen Verknüpfung mehrerer Registerinhalte gewinnt, wie z. B. der Crypto-1 von Mifare Classic (gebrochen 2007).