Ãëàâà 15
Îáúåäèíåíèå áëî÷íûõ øèôðîâ

Ñóùåñòâóåò ìíîæåñòâî ñïîñîáîâ îáúåäèíÿòü áëî÷íûå àëãîðèòìû äëÿ ïîëó÷åíèÿ íîâûõ àëãîðèòìîâ. Ñòàíäàðòíûì ñïîñîáîì îáúåäèíåíèÿ áëî÷íûõ øèôðîâ ÿâëÿåòñÿ ÷åðåç òåðíèíàëüíûé àëãîðèòì. DES ÿâëÿåòñÿ áåçîïàñíûì àëãîðèòìîì, îí ïîäâåðãàëñÿ äîñòàòî÷íî ìíîãî àòàê, òàê ÷òî íà ìîìåíò íàïèñàíèÿ ýòîé ãëàâû íåèçâåñòíî íèêàêèõ ñïîñîáîâ âçëîìàòü åãî áûñòðåå, ÷åì ïåðåáîðîì âñåõ âîçìîæíûõ êëþ÷åé. Ïîýòîìó ìû ïðåäïîëàãàåì, ÷òî DES áåçîïàñåí. Ïîäðîáíîå îïèñàíèå DES ìîæíî íàéòè â [1075]. Ïîñêîëüêó DES ÿâëÿåòñÿ ñòàíäàðòîì, îí ïîääåðæèâàåòñÿ ðàçëè÷íûìè ïðîãðàììíûìè ïðîäóêòàìè è áèáëèîòåêàìè. Ïîýòîìó ïîëüçîâàòåëè DES íå çàâèñÿò îò ïðîèçâîëà îäíîãî ïîñòàâùèêà. Ýòî ïîçâîëÿåò èñïîëüçîâàòü DES â êà÷åñòâå êîìïîíåíòà äðóãîãî àëãîðèòìà ñ äîâåðèåì äëèííûì êëþ÷îì? Ýòî ïîçâîëÿåò âû ïîëó÷èòü ïðåèìóùåñòâà äëèííîãî êëþ÷à ñ äàðàíòèåé äâóõ äåñÿòèëåòèé êðèïòîàíàëèçà.

Îäíî èç ñïîñîáîâ îáúåäèíåíèÿ ÿâëÿþòñÿ **ìíîãîêðàòíîå øèôðîâàíèå** - äëÿ øèôðîâàíèÿ îäíîãî è òîãî æå áëîêà îòêðûòîãî òåêñòà äëãîðèòì øèôðîâàíèÿ èñïîëüçóåòñÿ íåñêîëüêî êëþ÷åé. Ïîñëåäíèé øàã íàçûâàåòñÿ îáúåäèíåíèåì èñõîäíûõ øèôðîâàíèé, íî èñïîëüçóåò ðàçëè÷íûå àëãîðèòìû. Ñóùåñòâóþò è äðóãèå ìåòîäû.

Ïîâòîðíîå øèôðîâàíèå áëîêà îòêðûòîãî òåêñòà îäíîì è òåì æå êëþ÷îì ñ ïîìîùüþ òîãî æå èëè äðóãîãî àëãîðèòìà íåðàçóìíî. Ïîâòîðíîå èñïîëüçîâàíèå òîãî æå àëãîðèòìà íå óâåëè÷èâàåò ñëîæíîñòü âñêðûòèÿ ðàçëè÷íûõ øèôðîâàíèé, íî èñïîëüçóåò ðàçëè÷íûå àëãîðèòìû. Ñóùåñòâóþò è äðóãèå ìåòîäû. (Íå çàáûâàéòå, ìû ïðåäïîëàãàåì, ÷òî àëãîðèòì, âëþ÷àÿ êîëè÷åñòâî øèôðîâàíèé, èçâåñòåí êðèïòîàíàëèòèêó.) Ïðè ðàçëè÷íûõ àëãîðèòìàõ ñëîæíîñòü âñêðûòèÿ ðàçíîé ñëîæíîñòè, à ìîæåò è îñòàòüñÿ íåèçìåííîé. Åñëè âû ñîáèðàåòåñü èñïîëüçîâàòü ìåòîäû, îïèñàííûå â ýòîé ãëàâå, óáåäèòåñü, ÷òî êëþ÷è äëÿ ïîñëåäîâàòåëüíûõ øèôðîâàíèé ðàçëè÷íû è íåçàâèñèìû.

15.1 Äâîéíîå øèôðîâàíèå

Íàèâíûì ñïîñîáîì ïîâûñèòü áåçîïàñíîñòü àëãîðèòìà ÿâëÿåòñÿ øèôðîâàíèå áëîêà âåùåñòâåííûì ÷èñëîì ðàçëè÷íûì èëè êëþ÷àìè. Ñíà÷àëà áëîê øèôðóåòñÿ ïåðâûì êëþ÷îì, à çàòåì ïîëó÷èâøèéñÿ øèôðîòåêñò øèôðóåòñÿ âòîðûì êëþ÷îì. Äâîéíîå øèôðîâàíèå ÿâëÿåòñÿ îáðàòíûì ïðîöåññîì.

$$C = E_{K_2}(E_{K_1}(P))$$

$$P = D_{K_1}(D_{K_2}(C))$$

Åñëè áëîê-øèôð èñïîëüçóåò ðóïï (ñì. ðàçäåë 11.3), òî âñåãäà ñóùåñòâóåò K_3, äëÿ êîòîðîãî

$$C = E_{K_2}(E_{K_1}(P)) = E_{K_3}(P)$$

Åñëè àëãîðèì íå îáðàçóåò ãðóïïó, òî ïðè ïîâòîðíîì èñ÷åðïûâàþùåãî ïîèñêà âçëîìàòü ïîëó÷àþùèéñÿ äâàæäû çàøèôðîâàííûé áëîê øèôðîòåêñòà íàìíîãî ñëîæíåå. Âìåñòî 2^n (ãäå n - äëèíà êëþ÷à â áèòàõ), ïîòðåáóåòñÿ 2^{2n} ïîïûòîê. Åñëè àëãîðèì èñïîëüçóåò 64-áèòîâûé êëþ÷, äëÿ îáíàðóæåíèÿ êëþ÷åé, êîòîðûå çàøèôðîâàí øèôðîòåêñò, ïîòðåáóåòñÿ 2^{128} ïîïûòîê.

Íî ïðè âñêðûòèè ñ èçâåñòíûì îòêðûòûì òåêñòîì ýòî íå òàê. Ìåòîä è Õåëëìàí [1075] ïðèäóìàëè ñïîñîá îáìåíÿòü ïàìÿòü íà âðåìÿ, êîòîðûé ïîçâîëÿåò âñêðûòü òàêóþ ñõåìó äâîéíîãî øèôðîâàíèÿ çà 2^{n+1} øèôðîâàíèé, à íå çà 2^{2n}. (Îíè ñïîëüçîâàëè ýòó ñõåìó ïðîòèâ DES, íî ðåçóëüòàò ìîæíî îáîáùèòü íà âñå áëî÷íûå àëãîðèòìû.) Ýòî âñêðûòèå íàçûâàåòñÿ "**âñòðå÷à ïîñðåäèíå**", ñ îáîíé ñòîðîíû âûïîëíÿåòñÿ øèôðîâàíèå à ñ äðóãîé - äåøèôðèðîâàíèå, ïîëó÷èâøèéñÿ ðåçóëüòàò ñðàâíèâàþòñÿ.

Â ýòîì âñêðûòèè êðèïòîàíàëèòèêó èçâåñòíû P_1, C_1, P_2 è C_2, òàêèå ÷òî

$$C_1 = E_{K_2}(E_{K_1}(P_1))$$

$$C_2 = E_{K_2}(E_{K_1}(P_2))$$

Äëÿ êàæäîãî âîçìîæíîãî K (èëè K_1, èëè K_2), êðèïòîàíàëèòèê ðàññ÷èòûâàåò $E_K(P_1)$ è ñîõðàíÿåò ðåçóëüòàò â ïàìÿòè. Ñîáðàâ âñå ðåçóëüòàòû, îí äëÿ êàæäîãî K âû÷èñëÿåò $D_K(C_1)$ è èùåò â ïàìÿòè òàêîé æå ðåçóëüòàò. Åñëè òàêîé ðåçóëüòàò îáíàðóæåí, òî âîçìîæíî, ÷òî òåêóùèé êëþ÷ - K_2, à êëþ÷ äëÿ ðåçóëüòàòà â ïàìÿòè - K_1. Çàòåì êðèïòîàíàëèòèê øèôðóåò P_1 ñ ïîìîùüþ K_1 è K_2. Åñëè îí ïîëó÷àåò C_2, òî îí ìîæåò äàðàíòèðîâàòü (ñ âåðîÿòíîñòüþ óñïåõà 1 ê 2^{2n-2m}, ãäå m - ðàçìåð áëîêà), ÷òî îí óçíàë è K_1, è K_2. Åñëè ýòî íå òàê, îí ïðîäîëæàåò ïîèñê. Ìàêñèìàëüíîå êîëè÷åñòâî ïîïûòîê øèôðóåò P_1 è P_2, ðàâíî $2*2^n$, èëè 2^{n+1}. Åñëè âåðîÿòíîñòü îøèáêè ñëèøêîì âåëèêà, îí ìîæåò èñïîëüçîâàòü òðåòèé áëîê øèôðîâàíèÿ, îò ýòîãî õâàòàåò, ÷òîáû óâåëè÷èòü âåðîÿòíîñòü óñïåõà 1 ê 2^{2n-3m}. Ñóùåñòâóþò è äðóãèå ñïîñîáû îïòèìèçàöèè [912].

Äëÿ òàêîãî âñêðûòèÿ íóæåí áîëüøîé îáúåì ïàìÿòè: 2^n áëîêîâ. Äëÿ 56-áèòîâîãî êëþ÷à íóæíî õðàíèòü 2^{56} 64-áèòîâûõ áëîêîâ, èëè 10^{17} áàéòîâ. Òàêîé îáúåì ïàìÿòè ïîêà åùå òðóäíî ñåãîäíÿøíåìó êîìïüþòåðó, íî ýòîãî õâàòàåò, ÷òîáû óáåäèòüñÿ íåïðèãîäíîñòè êðèïòîãðàôè â òîì, ÷òî äâîéíûì øèôðîâàíèåì ïîëüçîâàòüñÿ íåëüçÿ.

Ïðè 128-áèòîâîì êëþ÷å äëÿ õðàíåíèÿ ïðîìåæóòî÷íûõ ðåçóëüòàòîâ ïîòðåáóåòñÿ 10^{39} áàéòîâ. Åñëè ïðåäïîëîæèòü, ÷òî åñòü ñïîñîá õðàíèòü áèò èíôîðìàöèè, èñïîëüçóÿ åäèíñòâåííûé àòîì äëþ èíèÿ, óñòðîéñòâî ïàìÿòè, íóæíîå äëÿ âûïîëíåíèÿ òàêîãî âñêðûòèÿ, áóäåò ïðåäñòàâëÿòü ñîáîé äëþ èíèåâûé êóá ñ ðåáðîì, äëèíîé 1 êì. Êðîìå òîãî, âàì ïîíàäîáèòñÿ êóäà-òî åãî ïîñòàâèòü! Âñêðûòèå "âñòðå÷à ïîñðåäèíå" êàæåòñÿ íåâîçìîæíûì äëÿ êëþ÷åé òàêîãî ðàçìåðà.

Äðóãèì ñïîñîáîì äâîéíîãî øèôðîâàíèÿ, êîòîðûé èíîãäà íàçûâàþò **Davies-Price**, ÿâëÿåòñÿ âàðèàíòîì CBC [435].

$$C_i = E_{K_1}(P_1 \oplus E_{K_2}(C_{i-1}))$$
$$P_i = D_{K_1}(C_i) \oplus E_{K_2}(C_{i-1}))$$

Óòâåðæäàåòñÿ, ÷òî "ó ýòîãî ðåæèìà íåò íèêàêèõ îñîáûõ äîñòîèíñòâ", ê òîìó æå îí, ïî âèäèìîìó, òàê æå ÷óâñòâèòåëåí êî âñêðûòèþ "âñòðå÷à ïîñðåäíèå" êàê è äóãèå ðåæèìû äâîéíîãî øèôðîâàíèÿ.

15.2

Òðîéíîå øèôðîâàíèå ñâóõ êëþ÷àìè

Â áîëåå èíòåðåñíîì ìåòîäå, ïðåäëîæåííîì Òà÷ìåíîì â [1551], áëîê îáðàáàòûâàåòñÿ òðè ðàçà ñ ïîìîùüþ äâóõ êëþ÷åé: ïåðâûì êëþ÷îì, âòîðûì êëþ÷îì è ñíîâà ïåðâûì êëþ÷îì. Îí ïðåäëàãàåò, ÷òîáû ñíà÷àëà øèôðîâàëè ïåðâûì êëþ÷îì, çàòåì äøèôðîâàëè âòîðûì, è îêîí÷àòåëüíî øèôðîâàëè ïåðâûì êëþ÷îì. Ïîëó÷àòåëü ðàñøèôðîâûâàåò ïåðâûì êëþ÷îì, çàòåì øèôðóåò âòîðûì è, íàêîíåö, äåøèôðèðóåò ïåðâûì.

$$C = E_{K_1}(D_{K_2}(E_{K_1}(P)))$$
$$P = D_{K_1}(E_{K_2}(D_{K_1}(C)))$$

Èíîãäà òàêîé ðåæèì íàçûâàþò **øèôðîâàíèå-äåøèôðèðîâàíèå-øèôðîâàíèå** (encrypt-decrypt-encrypt, EDE) [55]. Åñëè áëîê-íûé àëãîðèòì èñïîëüçóåò *n*-áèòîâûé êëþ÷, òî äëèíà êëþ÷à îïèñàííîé ñõåìû ñîñòàâëÿåò 2*n* áèò. Ëþáîïûòíûé âàðèàíò ñõåìû øèôðîâàíèå-äåøèôðèðîâàíèå-øèôðîâàíèå áûë ðàçðàáîòàí â IBM äëÿ ñîâìåñòèìîñòè ñ ñóùåñòâóþùèìè ðåàëèçàöèÿìè àëãîðèòìà: çàäàíèå äâóõ îäèíàêîâûõ êëþ÷åé ýêâèâàëåíòíî îäèíàðíîìó øèôðîâàíèþ. ýòîì êëþ÷îì. Ñõåìà øèôðîâàíèå-äåøèôðèðîâàíèå-øèôðîâàíèå ñàìà ïî ñåáå íå îâëàäàåò íèêàêîé áåçîïàñíîñòüþ, íî ýòîò ðåæèì áûë èñïîëüçîâàí äëÿ óëó÷øåíèÿ àëãîðèòìà DES â ñòàíäàðòàõ X9.17 è ISO 8732 [55, 761].

K_1 è K_2 ÷åðåäóþòñÿ äëÿ ïðåîòâðàùåíèÿ îïèñàííîãî âûøå âñêðûòèÿ "âñòðå÷à ïîñðåäíèå". Åñëè $C = E_{K_1}(E_{K_1}(E_{K_1}(P)))$, òî êðèïòîàíàëèòèê äëÿ ëþáîãî âîçìîæíîãî K_1 ìîæåò çàðàíåå âû÷èñëèòü $E_{K_1}(E_{K_1}(P))$ è çàòåì âûïîëíèòü âñêðûòèå. Äëÿ ýòîãî ïîòðåáóåòñÿ òîëüêî 2^{n+2} øèôðîâàíèé.

Òðîéíîå øèôðîâàíèå ñ äâóìÿ êëþ÷àìè óñòîé÷èâî ê òàêîìó âñêðûòèþ. Íî Ìåðêë è Õåëëìàí ðàçðàáîòàëè äðóãîé ñïîñîá ðàçìåíà ïàìÿòè íà âðåìÿ, êîòîðûé ïîçâîëÿåò âçëîìùèêó ñ 2^{n-1} äåéñòâèé, èñïîëüçóÿ 2^n áëîêîâ ïàìÿòè [1075].

Äëÿ êàæäîãî âîçìîæíîãî K_2 ðàñøèôðóéòå 0 è ñîõðàíèòå ðåçóëüòàò. Çàòåì ðàñøèôðóéòå 0 äëÿ êàæäîãî âîçìîæíîãî K_1, ÷òîáû ïîëó÷èòü *P*. Âûïîëíèòå òðîéíîå øèôðîâàíèå *P*, ÷òîáû ïîëó÷èòü *C*, è çàòåì ðàñøèôðóéòå *C* êëþ÷îì K_1. Åñëè ïîëó÷åííûå çíà÷åíèå ñîâïàäàåò ñ çíà÷åíèåì (õðàíÿùåìñÿ â ïàìÿòè), ïîëó÷åííûé ïðè äâîéíîì øèôðîâàíèè 0 êëþ÷îì K_2, òî ïàðà K_1 K_2 ÿâëÿåòñÿ âîçìîæíûì ðåçóëüòàòîì ïîèñêà. Ïðîâåðüòå, òàê ëè ýòî. Åñëè íåò, ïðîäîëæàéòå ïîèñê.

Âûïîëíåíèå ýòîãî âñêðûòèÿ ñ âû÷èñëåíèåì îòêðûòûõ òåêñòîâ òðåáóåò îãðîìíîãî îáúåìà ïàìÿòè. Ïîíàäîáèòñÿ 2^n âðåìåíè è ïàìÿòè, à òàêæå 2^m âû÷èñëåíèé îòêðûòûõ òåêñòîâ. Âñêðûòèå íå î÷åíü ïðàêòè÷íî, íî âñå æå ÷óâñòâèòåëüíîñòü ê íåìó ÿâëÿåòñÿ ñëàáîñòüþ àëãîðèòìà.

Ïàóëü âàí Îîðñ÷îò (Paul van Oorschot) è Ìàéêë Âèíåð (Michael Wiener) ïðåäëîæèëè ýòî âñêðûòèå ê âñêðûòèþ ñ èçâåñòíûì îòêðûòûì òåêñòîì, äëÿ êîòîðîãî íóæíî *p* èçâåñòíûõ îòêðûòûõ òåêñòîâ. Â ïðèìåðå ïðåäïîëàãàåòñÿ, ÷òî èñïîëüçóåòñÿ ðåæèì EDE.

(1) Ïðåäïîëîæèòü ïðåâî ïðîìåæóòî÷íîå çíà÷åíèå *a*.

(2) Èñïîëüçóÿ èçâåñòíûé îòêðûòûé òåêñò, ñâÿçàííûé äëÿ êàæäîãî âîçìîæíîãî K_1 âòîðîå ïðîìåæóòî÷íîå çíà÷åíèå *b*, ïðè ïåðâîì ïðîìåæóòî÷íîì çíà÷åíèè, ðàâíîì *a*:

$b = D_{K_1}(C)$

ãäå *C* - ýòî øèôðîòåêñò, ïîëó÷åííûé ïî èçâåñòíîìó îòêðûòîìó òåêñòó.

(3) Äëÿ êàæäîãî âîçìîæíîãî K_2 íàéòè â òàáëèöå ýëåìåíòû ñ ñîâïàäàþùèì âòîðûì ïðîìåæóòî÷íûì çíà÷åíèå

b:

$b = E_{K_2}(a)$

(4) Âåðîÿòíîñòü óñïåõà ðàâíà *p/m*, ãäå *p* - ÷èñëî èçâåñòíûõ îòêðûòûõ òåêñòîâ, à *m* - ðàçìåð áëîêà. Åñëè ñîâïàäåíèÿ íå îáíàðóæåíû, âûáåðèòå äðóãîå *a* è íà÷íèòå ñíà÷àëà.

Âñêðûòèå òðåáóåò $2^{n+m}/p$ âðåìåíè è *p* - ïàìÿòè. Äëÿ DES ýòî ðàâíî $2^{120}/p$ [1558]. Äëÿ *p*, áîëüøèõ 256, ýòî âñêðûòèå áûñòðåå, ÷åì èñ÷åðïûâàþùèé ïîèñê.

Òðîéíîå øèôðîâàíèå ñ òðåìÿ êëþ÷àìè

Åñëè âû ñîáñòâåííûì èñïîëüçîâàòü òðîéíîå øèôðîâàíèå, ÿ ðåêîìåíäóþ òðè ðàçëè÷íûõ êëþ÷à. Îáùàÿ äëèíà êëþ÷à áîëüøå, íî õðàíåíèå êëþ÷à îáû÷íî íå ÿâëÿåòñÿ ïðîáëåìîé. Áèò äâóêâû.

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P)))$$
$$P = D_{K_1}(E_{K_2}(D_{K_3}(C)))$$

Äëÿ íàèëó÷øåãî âñêðûòèÿ ñðàçìåíî ïàìÿòè íà âðåìÿ, êîòîðûì ÿâëÿåòñÿ "âñòðå÷à ïîñåðåäèíå", ïîòðåáóåòñÿ 2^{2n} äåéñòâèé è 2^n áëîêîâ ïàìÿòè [1075]. Òðîéíîå øèôðîâàíèå ñ òðåìÿ íåçàâèñèìûìè êëþ÷àìè áåçîïàñíî íàñòîëüêî, íàñêîëüêî íà ïåðâûé âçãëÿä êàæåòñÿ áåçîïàñíûì äâîéíîå øèôðîâàíèå.

Òðîéíîå øèôðîâàíèå ñ ìèíèìàëüíûì êëþ÷îì (TEMK)

Ñóùåñòâóåò áåçîïàñíûé ñïîñîá èñïîëüçîâàòü òðîéíîå øèôðîâàíèå ñ äâóìÿ êëþ÷àìè, ïðîòèâîñòîÿùèé îïèñàííîìó âûøå âñêðûòèþ è íàçûâàåìûé Òðîéíûì øèôðîâàíèåì ñ ìèíèìàëüíûì êëþ÷îì (Triple Encryption with Minimum Key, TEMK) [858]. Ôîêóñ â òîì, ÷òîáû ïîëó÷èòü òðè êëþ÷à èç: X_1 è X_2.

$$K_1 = E_{X_1}(D_{X_2}(E_{X_1}(T_1)))$$
$$K_2 = E_{X_1}(D_{X_2}(E_{X_1}(T_2)))$$
$$K_3 = E_{X_1}(D_{X_2}(E_{X_1}(T_3)))$$

T_1, T_2 è T_3 ïðåäñòàâëÿò ñîáé êîíñòàíòû, êîòîðûå íåîáõîäèìî ðàíåå çàäàòü â ñåêðåòå. Ýòà ñõåìà äàðàíòèðóåò, ÷òî äëÿ ëþáîé êîíêðåòíîé ïàðû êëþ÷åé íàèëó÷øèì áóäåò âñêðûòèå ñ èçâåñòíûì îòêðûòûì òåêñòîì.

Ðåæèì òðîéíîãî øèôðîâàíèÿ

Íåäîñòàòî÷íî ïðîñòî îïðåäåëèòü òðîéíîå øèôðîâàíèå, íóæíî âûáðàòü îäèí èç ñïîñîáîâ åãî èñïîëüçîâàíèÿ. Ðåøåíèå çàâèñèò îò òðåáóåìûõ áåçîïàñíîñòè è ýôôåêòèâíîñòè. Âîò äâà âîçìîæíûõ ðåæèìà òðîéíîãî øèôðîâàíèÿ:

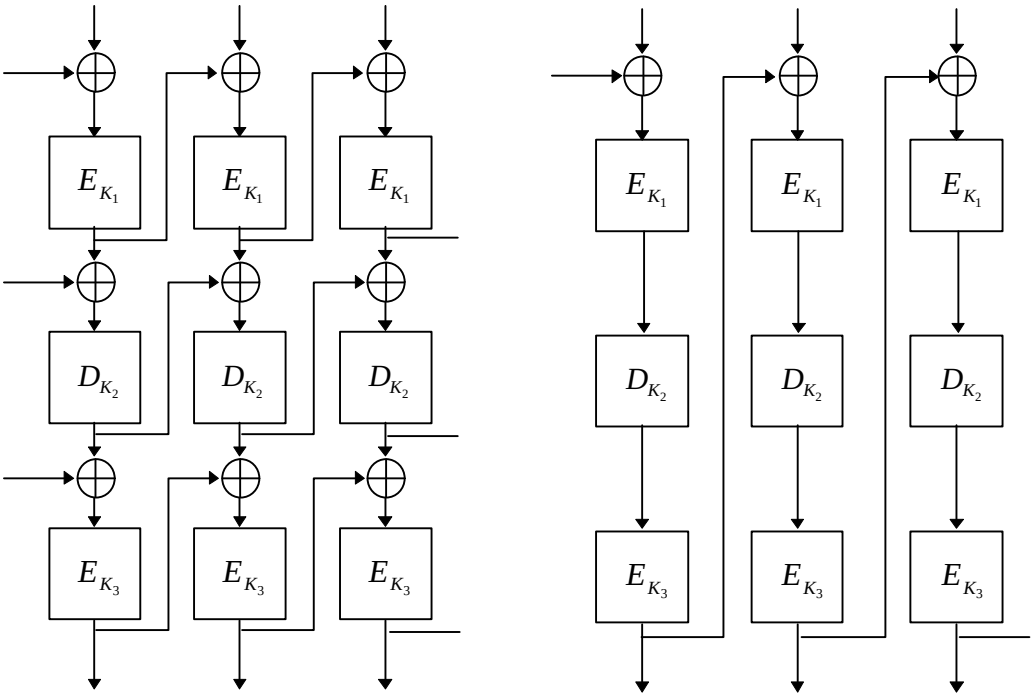
Âíóòðåííèé CBC: Ôàéë òðè ðàçà øèôðóåòñÿ â ðåæèìå CBC (ñì. 14tha). Äëÿ ýòîãî íóæíî òðè ðàçëè÷íûõ IV.

$$C_i = E_{K_3}(S_i \oplus C_{i-1}); S_i = D_{K_2}(T_i \oplus S_{i-1}); T_i = E_{K_1}(P_i \oplus T_{i-1})$$
$$P_i = T_{i-1} \oplus D_{K_1}(T_i); T_i = S_{i-1} \oplus E_{K_2}(S_i); S_i = C_{i-1} \oplus D_{K_3}(C_i)$$

C_0, S_0 è T_0 ÿâëÿþòñÿ IV.

Âíåøíèé CBC: Ôàéë òðîêðàòíî øèôðóåòñÿ â ðåæèìå CBC (ñì. 14thb). Äëÿ ýòîãî íóæåí îäèí IV.

$$C_i = E_{K_3}(D_{K_2}(E_{K_1}(P_i \oplus C_{i-1})))$$
$$P_i = C_{i-1} \oplus D_{K_1}(E_{K_2}(D_{K_3}(C_i)))$$



(à) Âíóòðåííèé CBC (b) Âíåøíèé CBC

Ðèñ. 15-1. Òðîéíîå øèôðîâàíèå â ðåæèìå CBC.

Äëÿ îáîèõ ðåæèìîâ íóæíî áîëüøå ðåñóðñîâ, ÷åì äëÿ îäíîêðàòíîãî øèôðîâàíèÿ: áîëüøå àïïàðàòóðû èëè áîëüøå âðåìåíè. Îäíàêî ïðè òðåõ øèôðóþùèõ ìèêðîñõåìàõ ïðîèçâîäèòåëüíîñòü âíóòðåííåãî CBC íå ìåíüøå, ÷åì ïðè îäíîêðàòíîì øèôðîâàíèè. Òàê êàê òðè øèôðîâàíèÿ CBC íåçàâèñèìû, òðè ìèêðîñõåìû ìîãóò áûòü çàãðóæåíû ïîñòîÿííî, ïîäàâàÿ ñâîé âûõîä ñåáå íà âõîä.

Íàïðîòèâ âî âíåøíåì CBC îáðàòíàÿ ñâÿçü íàõîäèòñÿ íàðóæå ïî îòíîøåíèþ ê òðåì øèôðîâàíèÿì. Ýòî îçíà÷àåò, ÷òî äàæå ñ òðåìÿ ìèêðîñõåìàìè ïðîèçâîäèòåëüíîñòü áóäåò ðàâíà òîëüêî îäíîé òðåòè ïðîèçâîäèòåëüíîñòè ïðè îäíîêðàòíîì øèôðîâàíèè. ×òîáû ïîëó÷èòü òó æå ïðîèçâîäèòåëüíîñòü äëÿ âíåøíåãî CBC, ïîòðåáóåòñÿ ÷åòâåðîâàíèå IV (ñì. ðàçäåë 9.12):

$$C_i = E_{K_3}(D_{K_2}(E_{K_1}(P_i \oplus C_{i-3})))$$

Â ýòîì ñëó÷àå C_0, C_{-1} è C_{-2} ÿâëÿþòñÿ IV. Ýòî íå ïîìåøàò ïðè ïðîãðàììíîé ðåàëèçàöèè, ðàçäåë òîëüêî ïðè èñïîëüçîâàíèè ïàðàëëåëüíîãî êîìïüþòåðà.

Ê ñîæàëåíèþ ìåíåå ñëîæíûé ðåæèì ÿâëÿåòñÿ òàêæå è ìåíåå áåçîïàñíûì. Áèòàì ïðîàíàëèçèðîâàë ðàçëè÷íûå ðåæèìû ïî îòíîøåíèþ ê äëÿôåðåíöèàëüíîìó êðèïòàíàëèçó è îáíàðóæèë, ÷òî áåçîïàñíîñòü âíóòðåííåãî CBC ïî ñðàâíåíèþ ñ îäíîêðàòíûì øèôðîâàíèåì óâåëè÷èâàåòñÿ íåçíà÷èòåëüíî. Åñëè ðàññìàòðèâàòü òðîéíîå øèôðîâàíèå êàê äâîéíûé áîëüøîé àëãîðèòì, òî âíóòðåííåå îáðàòíûå ñâÿçè ïîçâîëÿþò âåäóùèì âíåøíþþ è èçâåñòíóþ èíôîðìàöèþ âíóòðè àëãîðèòìà, ÷òî îáëåã÷àåò êðèïòîàíàëèç. Äëÿ äèôôåðåíöèàëüíûõ âñêðûòèé íóæíî îãðîìíîå êîëè÷åñòâî âûáðàííûõ øèôðîòåêſòîâ, ÷òî äàëåêî ýòè âñêðûòèÿ íå ñëèøêîì ïðàêòè÷íû, íî ýòèõ ðåçóëüòàòîâ äîëæíî õâàòèòü, ÷òîáû íàñòîÿùèì ïàðàíîèêàì ïîëüçîâàòåëå. Áîëåèç óñòîé÷èâîñòè äëãîðèòìîâ ê âñêðûòèÿì ãðóáîé ñèëîé è "âñòðå÷åé ïîñðåäèíå" ïîêàçàë, ÷òî îáà âàðèàíòà îäíàêîâî áåçîïàñíû [806].

Êðîìå ýòèõ ñóùåñòâóò è äðóãèå ðåæèìû. Ì îæíî çàøèôðîâàòü ôàéë îäíî ðàç â ðåæèìå ECB, çàòåì äâàæäû â CBC, èëè îäíî ðàç â CBC, îäíî â ECB è åùå ðàç â CBC, èëè äâàæäû â CBC è îäíî ðàç â ECB. Áèòàì ïîêàçàë, ÷òî ýòè âàðèàíòû íå áåçîïàñíû, ÷åì îäíîêðàòíûé DES, ïðîòèâ âñêðûòèÿ äèôôåðåíöèàëüíûì êðèïòîàíàëèçîì ñ âûáðàííûì îòêðûòûì òåêſòîì [162]. Î í íå îñòàâèë áîëüøèõ íàäåæä è äëÿ äðóãèõ âàðèàíòîâ. Åñëè âû ñîáèðàåòåñü ïðèìåíÿòü òðîéíîå øèôðîâàíèå, èñïîëüçóéòå âíåøíþþ îáðàòíóþ ñâÿçü.

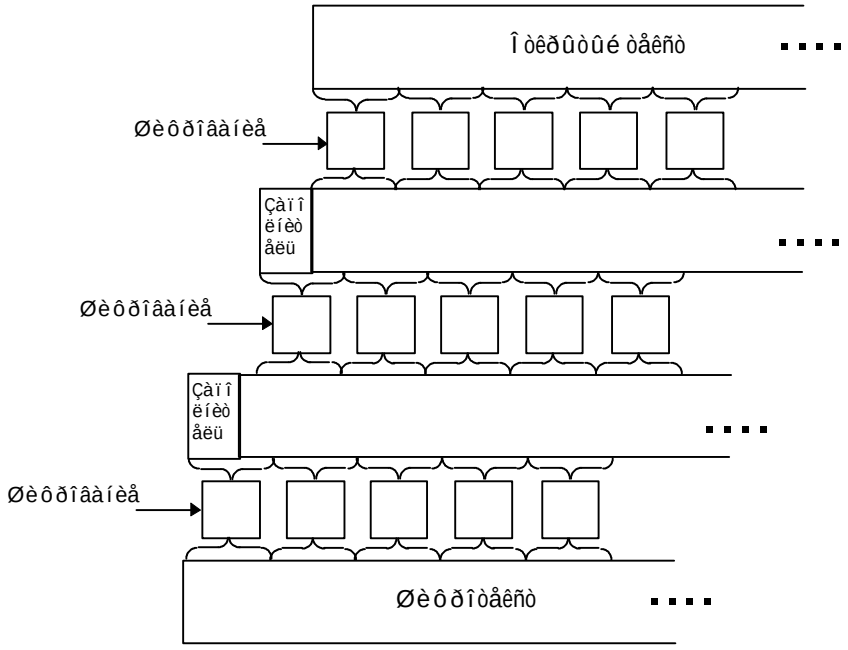
Âàðèàíòû òðîéíîãî øèôðîâàíèÿ

Ïðåæäå, ÷åì ïîÿâèëèñü äîêàçàòåëüſòâà òîãî, ÷òî DES íå îáðàçóåò ãðóïïó, äëÿ ìíîãîêðàòíîãî øèôðîâàíèÿ ïðåäëàãàëèñü ðàçëè÷íûå ñõåìû. Îäíèì èç ñïîñîáîâ îáåñïå÷èòü, ÷òî òðîéíîå øèôðîâàíèå íå âûðîäèòñÿ â îäíîêðàòíå, áûëî èçìåíåíèå ýôôåêòèâíîé äëèíû áëîêà. Ïðîñòûì ìåòîäîì ÿâëÿåòſ äîáàâëåíèå áèòàçàïîëíèòåëÿ. Ìåæó ïåðâûì è âòîðûì, à òàêæå ìåæó âòîðûì è òðåòüèì øèôðîâàíèÿìè òåñò äîïîëíÿåòſ

ñòðîêîé ñëó÷àéíûõ áèòîâ (ñì. Ðèñ. 15.2). Åñëè *PP* - ýòî ôóíêöèÿ äîïîëíåíèÿ, òî:

$$C = E_{K_3}(PP(E_{K_2}(PP(E_{K_1}(P)))))$$

Ýòî äîïîëíåíèå íå òîëüêî ðàçðóøàåò øàáëîíû, íî òàêæå îáåñïå÷èâàåò ïðåêðûòèå áëîêîâ øèôðîâàíèÿ, êàê êèðïè÷åé â ñòåíå. Ê äëèíå ñîîáùåíèÿ äîáàâëÿåòñÿ òîëüêî îäèí áëîê.



Ðèñ. 15-2. Òðîéíîå øèôðîâàíèå ñçàïîëíåíèåì.

Äðóãîé ìåòîä, ïðåäëîæåííûé Êàðëîì Ýëëèñîíîì (Carl Ellison), èñïîëüçóåò íåêîòîðóþ ôóíêöèþ íåçàâèñèìîé îò êëþ÷à ïðåîáðàçîâàíèÿ øèôðîâàíèÿ. Ïðåäñòàâëåíèå äîæíà ðàâíîâåðîÿòíî áûòü ñ áîëüøèì äîâåðèåì - 8 Êáàéò èëè îêòåò ýòîãî, ÷òî äëåàò ýôôåêòèâíûé ðàçìåð áëîêà äëÿ ýòîãî âàðèàíòà ðàâíû 8 Êáàéòàì. Ïðè óñëîâèè, ÷òî ïðåäñòàâëåíèå âûïîëíÿåòñÿ áûñòðî, ýòîò âàðèàíò íåìàëîâû ìåäëåííåå, ÷åì áàçîâûå òðîéíûå øèôðîâàíèå.

$$C = E_{K_3}(T(E_{K_2}(T(E_{K_1}(P)))))$$

T ñîáåðåò âõîäíûå áëîêè (äî 8 Êáàéò â äëèíó) è èñïîëüçóåò ãåíåðàòîð ïñåâäîñëó÷àéíûõ ÷èñåë äëÿ èõ ïåðåìåøèâàíèÿ. Èçìåíåíèå îäíîãî áèòà âõîäà ïðèâîäèò ê èçìåíåíèþ 8 áàéòîâ ðåçóëüòàòà ïðåîãî øèôðîâàíèÿ, ê èçìåíåíèþ äî 64 áàéòîâ ðåçóëüòàòà âòîðîãî øèôðîâàíèÿ è ê èçìåíåíèþ äî 512 áàéòîâ ðåçóëüòàòà òðåòüåãî øèôðîâàíèÿ. Åñëè êàæäûé áëîê íåçàâèñèìî ðàíäîìèçèðîâàí â ðåæèìå CBC, êàê áûëî ïðåäïîëîæåíî, òî èçìåíåíèå äâóõ áèòîâ âõîäà ñîðåò âñåãî ïðèâåäåò ê èçìåíåíèþ âñåãî 8-êèëîáàéòîâîãî áëîêà, äàæå åñëè ýòîò áëîê íå ÿâëÿåòñÿ ïåðâûì.

Ñàìûé ïîñëåäíèé âàðèàíò ýòîé ñõåìû îòâå÷àåò íà âîïðîñ îá èñïîëüçîâàíèè CBC, âûïîëíåííîé Áèòàìè, äîáàâëåíèå ïðîöåäóð îòáëåâàíèÿ, ÷òîáû çàìàñêèðîâàòü ñòðóêòóðó îðèãèíàëüíîãî òåêñòà. Ýòà ïðîöåäóðà ïðåäñòàâëÿåò ïîñëåäîâàòåëüíîñòü XOR ñ êðèïòîãðàôè÷åñêè áåçîïàñíûì ãåíåðàòîðîì ïñåâäîñëó÷àéíûõ ÷èñåë è íèæå îáîçíà÷åíà êàê *R*. *T* ìåøàåò êðèòèêàì èñïîëüçîâàòü *a priori*, êàêîé êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ ëþáîãî çàäàííîãî áàéòà âõîäà ïîñëåäîâàòåëüíîñòè øèôðîâàíèÿ. Âòîðîå øèôðîâàíèå îáîçíà÷åíî *nE* (øèôðîâàíèå ñ öèêëè÷åñêîì èñïîëüçîâàíèåì *n* ðàçëè÷íûõ êëþ÷åé):

$$C = E_{K_3}(R(T(nE_{K_2}(T(E_{K_1}(P))))))$$

Âñå øèôðîâàíèÿ âûïîëíÿþòñÿ â ðåæèìå ECB, èñïîëüçóåòñÿ íå ìåíüøå *n*+2 êëþ÷åé øèôðîâàíèÿ è êðèïòîãðàôè÷åñêè áåçîïàñíûé ãåíåðàòîð ïñåâäîñëó÷àéíûõ ÷èñåë.

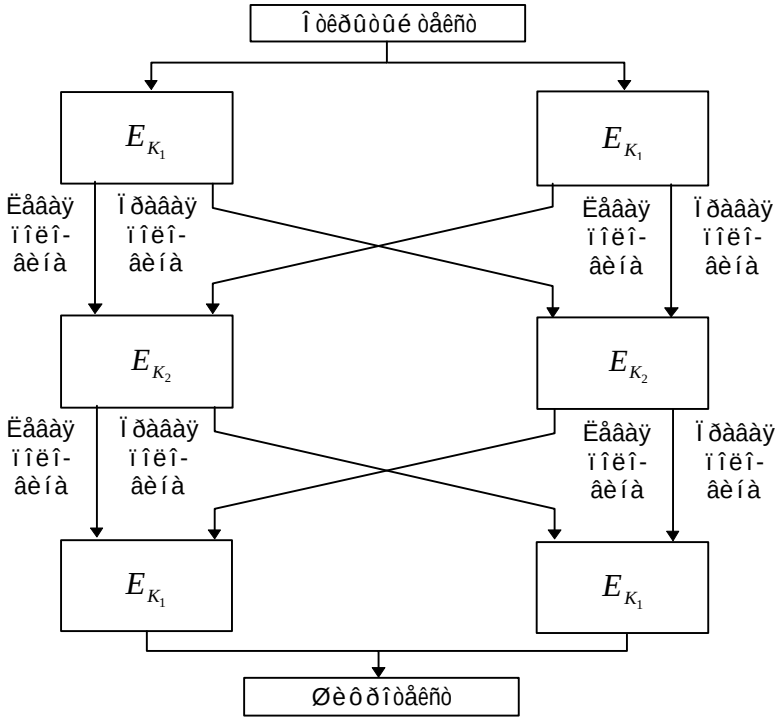
Ýòà ñõåìà áûëà ïðåäëîæåíà äëÿ èñïîëüçîâàíèÿ âìåñòå ñ DES, íî îíà ðàáîòàåò ñ ëþáûì áëî÷íûì àëãîðèòìîì. Ðåçóëüòàòû êðèïòîàíàëèçà òàêîé ñõåìû ìíå íåèçâåñòíû.

15.3 Óäâîåíèå äëèíû áëîêà

Â àêàäåìè÷åñêîì ñîîáùåñòâå äâîé ñîîðÿò íà òàì, äîñòàòî÷íà ëè 64-áèòîâàÿ äëèíà áëîêà. Ñ îäíîé ñòîðîíû 64-áèòîâûé áëîê îáåñïå÷èâàåò äëîóçè îòêðûòîãî òåêſòà òîëüêî â 8 áàéòàõ øèôðîâàíñòà. Ñ äðóãîé ñòîðîíû áîëåå äëèííûé áëîê çàðóáèýò áåçîïàñíóþ ìàñêèðîâêó ñòðóêòóðû, êðîìå òîãî, áîëüøå âîçìîæíîñòåé îøèáêè-

ñÿ.

Ñóùåñòâóþò ïðåäëîæåíèÿ óäâàèâàòü äëèíó áëîêà àëãîðèòìà ñ ïîìîùüþ ìíîãîêðàòíîãî øèôðîâàíèÿ [299]. Ïðåæäå, ÷åì ðàññìîòðèì âîçìîæíîñòü "âñòðå÷à ïîñåðåäèíå". Ñõåìà Äè÷àðäà Àóòáðèäæà (Richard Outerbridge) [300], ïîêàçàííàÿ íà 12-é, íå áëåñòÿùàÿ, ÷åì òðîéíîå øèôðîâàíèå ñ îäíîðîì áëîêîì è äâóìÿ êëþ÷àìè [859].



Ðèñ. 15-3. Óäâîåíèå äëèíû áëîêà.

Îäíàêî ÿ íå ðåêîìåíäóþ èñïîëüçîâàòü ïîäîáíûé ïðèåì. Î í íå áûñòðåå îáû÷íîãî òðîéíîãî øèôðîâàíèÿ: äëÿ øèôðîâàíèÿ äâóõ áëîêîâ äàííûõ âñå òàêæå íóæíî øåñòü øèôðîâàíèé. Õàðàêòåðèñòèêè îáû÷íîãî òðîéíîãî øèôðîâàíèÿ èçâåñòíû, à çà íîâûìè êîíñòðóêöèÿìè ÷àñòî ïðÿ÷óòñÿ íîâûå ïðîáëåìû.

15.4 Äðóãèå ñõåìû ìíîãîêðàòíîãî øèôðîâàíèÿ

Ïðîáëåìîé òðîéíîãî øèôðîâàíèÿ ñ äâóìÿ êëþ÷àìè ÿâëÿåòñÿ òî, ÷òî äëÿ óâåëè÷åíèÿ âäâîå ïðîñòðàíñòâà êëþ÷åé íóæíî âûïîëíÿòü òðè øèôðîâàíèÿ êàæäîãî äëîêà îòêðûòîãî òåêñòà. Ðàçâå íå çäîðîâî áûë áû íàéòè êàêîé-íèáóäü õèòðûé ñïîñîá îáúåäèíèòü äâà øèôðîâàíèÿ, êîòîðûå óäâîèëè áû ïðîñòðàíñòâî êëþ÷åé?

Äâîéíîé OFB/ñ÷åò÷èê

Ýòîò ìåòîä èñïîëüçóåò áëî÷íûé àëãîðèòì äëÿ ãåíåðàöèè äâóõ ïîòîêîâ êëþ÷åé, êîòîðûå èñïîëüçóþòñÿ äëÿ øèôðîâàíèÿ îòêðûòîãî òåêñòà.

$$S_i = E_{K_1}(S_{i-1} \oplus I_1); I_1 = I_1 + 1$$

$$T_i = E_{K_2}(T_{i-1} \oplus I_2); I_2 = I_2 + 1$$

$$C_i = P_i \oplus S_i \oplus T_i$$

S_i è T_i - âíóòðåííèå ïåðåìåííûå, à I_1 è I_2 - ñ÷åò÷èêè. Äâå êîïèè áëî÷íîãî àëãîðèòìà ðàáîòàþò â íåêîòîðîì ãèáðèäíîì ðåæèìå OFB/ñ÷åò÷èê, à îêðûòûé òåêñò, S_i è T_i îáúåäèíÿþòñÿ ñ ïîìîùüþ XOR. Êëþ÷è K_1 è K_2 íåçàâèñèìû. Ðåçóëüòàòû êðèïòîàíàëèçà ýòîãî âàðèàíòà ìíå íåèçâåñòíû.

ECB + OFB

Ýòîò ìåòîä áûë ðàçðàáîòàí äëÿ øèôðîâàíèÿ íåñêîëüêèõ ñîîáùåíèé ôèêñèðîâàííîé äëèíû, íàïðèìåð, áëîêîâ äiñêà [186, 188]. Èñïîëüçóþòñÿ äâà êëþ÷à: K_1 è K_2. Ñíà÷àëà äëÿ ãåíåðàöèè ìàñêè äëÿ áëîêà íóæíîé äëèíû èñïîëüçóåòñÿ âûðàáîòàííûé àëãîðèòì è êëþ÷. Ýòà ìàñêà áóäåò èñïîëüçîâàíà ïîâòîðíî äëÿ øèôðîâàíèÿ ñîîáùåíèé òåì æå êëþ÷àìè. Çàòåì âûïîëíÿþòñÿ XOR îòêðûòîãî òåêñòà ñîîáùåíèÿ è ìàñêè. Íàêîíåö ðåçóëüòàò XOR øèôðóåòñÿ ñ ïîìîùüþ âûðàáîòàííîãî àëãîðèòìà è êëþ÷à K_2 â ðåæèìå ECB.

Àíàëèç ýòîãî ìåòîäà ïðîâîäèëñÿ òîëüêî â òîé ðàáîòå, â êîòîðîé îí è áûë îïóáëèêîâàí. Ïîíÿòíî, ÷òî îí íå ñëèøêîì øèðîêî ìîæåò âûïîëíÿòüñÿ ECB è âîçìîæíî òàêæå ñèëåí, êàê è äâîéíîå ïðèìåíåíèå äëãîðåòíà. Åñòüòî, êðèïòîàíàëèòèê ìîæåò âûïîëíÿòü ïîèñê êëþ÷åé íåçàâèñèìî, åñëè îí ïîëó÷èò íåñêîëüêî îòêðûòûõ òåêñòîâ ôàéëîâ, çàøèôðîâàííûõ îäíèì êëþ÷îì.

×òîáû çàòðóäíèòü àíàëèç èäåíòè÷íûõ áëîêîâ â îäíèõ è òåõ æå ìåñòàõ ðàçëè÷íûõ ñîîáùåíèé, ìîæíî èñïîëüçîâàòü IV. Â îòëè÷èè îò èñïîëüçîâàíèÿ IV â äóãèõ ðåæèìàõ â äàííîì ñëó÷àå ïåðåä øèôðîâàíèåì ECB âûïîëíÿåòñÿ XOR êàæäîãî áëîêà ñîîáùåíèÿ ñ IV.

Ì ýòò Áëýç (Matt Blaze) ðàçðàáîòàë ýòîò ðåæèì äëÿ ñâîåé UNIX Cryptographic File System (CFS, êðèïòîãðàôè÷åñêàÿ ôàéëîâàÿ ñèñòåìà). Ýòî õîðîøèé ðåæèì, ïîñêîëüêó ñîîòíîñèòñÿ ÿâëÿåòñÿ òîëüêî îäíî øèôðîâàíèå â ðåæèìå ECB, ìàñêà ìîæåò áûòü ñãåíåðèðîâàíà òîëüêî îäèí ðàç è ñîõðàíåíà. Â CFS â êà÷åñòâå áëî÷íîãî àëãîðèòìà èñïîëüçóåòñÿ DES.

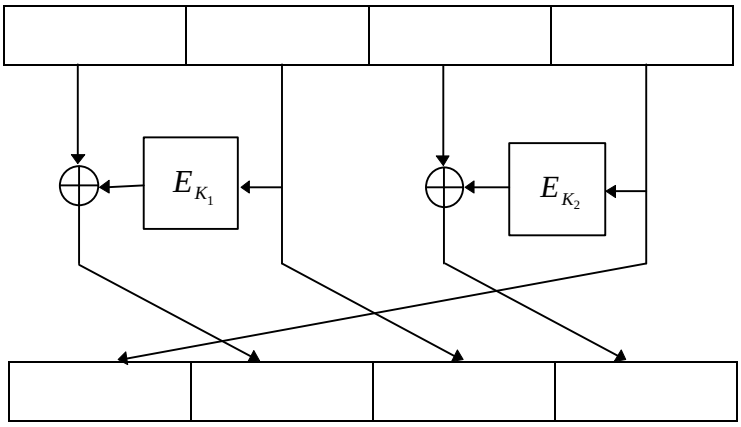
xDES[i]

Â [1644, 1645] DES èñïîëüçóåòñÿ êàê êîìïîíåíò ðÿäà áëî÷íûõ àëãîðèòìîâ ñóâëè÷åíûì ðàçìåðàìè êëþ÷åé è áëîêîâ. Ýòè ñõåìû íèêàê íå çàâèñÿò îò DES, è â íèõ ìîæåò èñïîëüçîâàòüñÿ ëþáîé áëî÷íûé àëãîðèòì.

Ïåðâûé, *x*DES[1], ïðåäñòàâëÿåò ñîáîé ïðîñòó ñõåìó Luby-Rackoff ñ áëî÷íûì øèôðîì â êà÷åñòâå áàçîâîé ôóíêöèè (ñì. ðàçäåë 14.11). Ðàçìåð áëîêà â äâà ðàçà áîëüøå ðàçìåðà áëîêà èñïîëüçóåìîãî áëî÷íîãîôèëüòðà, à ðàçìåð êëþ÷à â òðè ðàçà áîëüøå, ÷åì ó èñïîëüçóåìîãî áëî÷íîãî ôèëüòðà. Â êàæäîì èç 3 ýòàïîâ ïðåâðàùåíèÿ øèôðóåìûé áëî÷íûì àëãîðèòìîì è îäíèì èç êëþ÷åé, çàòåì âûïîëíÿåòñÿ XOR ðåçóëüòàòà è ëåâîé ïîëîâèíû, è ïîëîâèíû ïåðåñòàâëÿþòñÿ.

Ýòî áûñòðåå, ÷åì îáû÷íîå òðîéíîå øèôðîâàíèå, òàê êàê òðåáóåòñÿ øèôðîâàíèÿ è øèôðóåòñÿ áëîê, äëèíà êîòîðîãî â äâà ðàçà áîëüøå äëèíû áëîêà èñïîëüçóåìîãî áëî÷íîãî àëãîðèòìà. Íî ïðè ýòîì ñóùåñòâóåò ïðîñòîå âñêðûòèå "âñòðå÷à ïîñðåäèíå", êîòîðîå ïîçâîëÿåò íàéòè êëþ÷ ñ ïîìîùüþ òàáëèöû ðàçìåðîì 2^k, ãäå k - ýòî ðàçìåð êëþ÷à áëî÷íîãî àëãîðèòìà. Ïðåäàäÿ ïîëíîâèíà áëîêà îòêðûòîãî òåêñòà øèôðóåòñÿ ñ ïîìîùüþ âñåõ âîçìîæíûõ çíà÷åíèé K_1, âûïîëíÿåòñÿ XOR ñ ëåâîé ïîëîâèíîé îòêðûòîãî òåêñòà è ïîëó÷åííûå çíà÷åíèÿ ñîõðàíÿþòñÿ â òàáëèöå. Çàòåì ïðåâðàùåíèå øèôðîâàííîãî òåêñòà øèôðóåòñÿ ñ ïîìîùüþ âñåõ âîçìîæíûõ çíà÷åíèé K_3, è âûïîëíÿåòñÿ ïîèñê ñîâïàäåíèé â òàáëèöå. Ïðè ñîâïàäåíèè ïàðà êëþ÷åé K_1 è K_3 - âîçìîæíûé âàðèàíò ïðàâîãî êëþ÷à. Ïîñëå íåñêîëüêèõ ïîâòîðåíèé âñêðûòèÿ îñòàíåòñÿ òîëüêî îäèí êàíäèäàò. Òàêèì îáðàçîì, *x*DES[1] íà ÿâëÿåòñÿ èäåàëüíûì ðåøåíèåì. Äàæå õóæå, ñóùåñòâóåò âñêðûòèå ñ âû÷èñëèòåëüíîé ñëîæíîñòüþ, äîâîëüíî áëèçêîé ê *x*DES[1] íå íàìíîãî ñëîæíåå èñïîëüçóåìîãî â íåì áëî÷íîãî àëãîðèòìà [858].

Â *x*DES[2] ýòà èäåÿ ðàñøèðÿåòñÿ äî 5-ýòàïíîãî àëãîðèòìà, ðàçìåð áëîêà êîòîðîãî â 4 ðàçà, à ðàçìåð êëþ÷à â 10 ðàç ïðåâûøàþò ðàçìåðû áëîêà è êëþ÷à èñïîëüçóåìîãî áëî÷íîãî øèôðà. Íà 11th ïîêàçàí îäèí ýòàï *x*DES[2], êîòîðûé ïîâòîðÿåòñÿ äîñòàòî÷íîå êîëè÷åñòâî ðàç, ÷òîáû *x*DES[2] íå îòëè÷àëñÿ îò èäåàëüíîãî â íåì áëî÷íîãî àëãîðèòìà [858].



Ðèñ. 15-4. Îäèí ýòàï *x*DES[2].

Ê òîìó æå, ýòà ñõåìà áûòðåå, ÷åì òðîéíîå øèôðîâàíèå: äëÿ øèôðîâàíèÿ áëîêà, êîòîðûé â ÷åòûðå ðàçà áîëüøå áëîêà èñïîëüçóåìîãî áëî÷íîãî øèôðà, íóæíî 10 øèôðîâàíèé. Îäíàêî ýòîò ìåòîä ÷óâñòâèòåëåí ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó [858] è èñïîëüçîâàòü åãî íå ñòîèò. Òàêàÿ ñõåìà îñòàåòñÿ ÷óâñòâèòåëüíîé ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó, äàæå åñëè èñïîëüçóåòñÿ DES ñ íåçàâèñèìûì êëþ÷àìè ýòàïîâ.

Äëÿ $i \geq 3$ *x*DES[i] âåðîÿòíî ñëèøêîì âåëèê, ÷òîáû èñïîëüçîâàòü åãî â êà÷åñòâå áëî÷íîãî àëãîðèòìà. Íàïðèìåð, ðàçìåð áëîêà äëÿ *x*DES[3] â 6 ðàç áîëüøå, ÷åì ó ëåãàùåãî â îñíîâå áëî÷íîãî øèôðà, êëþ÷ â 21 ðàç äëèííåå, à äëÿ øèôðîâàíèÿ áëîêà, êîòîðûé â 6 ðàç äëèííåå áëîêà ëåãàùåãî â îñíîâå áëî÷íîãî øèôðà, íóæíî 21 øèôðîâàíèå.

Ýòî ìåäëåííåå, ÷åì òðîéíîå øèôðîâàíèå.

Ïðèìåðû øèôðîâàíèé

Åñëè òðîéíîå øèôðîâàíèå íåäîñòàòî÷íî áåçîïàñíî - ìîæåò áûòü, âàì íóæíî øèôðîâàòü êëþ÷è òðîéíîãî øèôðîâàíèÿ, èñïîëüçóÿ åùå áîëåå ñëîæíûé àëãîðèòì - òî êðàòíîñòü øèôðîâàíèÿ ìîæíî óâåëè÷èòü. Î÷åíü óñòîé÷èâî ê âñêðûòèþ "âñòðå÷à ïîñðåäèíå" ïðèêðàòíîå øèôðîâàíèå. (Àðãóìåíòû, àíàëîãè÷íûå ðàññìîòðåííûì äëÿ äâîéíîãî øèôðîâàíèÿ, ïîêàçûâàþò, ÷òî ÷åòûðåõêðàòíîå øèôðîâàíèå ïî ñðàâíåíèþ ñ òðîéíûì ëèøü íåçíà÷èòåëüíî ïîâûøàåò íàäåæíîñòü.)

$$C = E_{K_1}(D_{K_2}(E_{K_3}(D_{K_2}(E_{K_1}(P)))))$$

$$P = D_{K_1}(E_{K_2}(D_{K_3}(E_{K_2}(D_{K_1}(C)))))$$

Ýòà ñõåìà îáðàòíî ñîâìåñòèìà ñ òðîéíûì øèôðîâàíèåì, åñëè $K_1 = K_2$, è ñ îäíîêðàòíûì øèôðîâàíèåì, åñëè $K_1 = K_2 = K_3$. Êîíå÷íî, îíà áóäåò åùå íàäåæíåé, åñëè èñïîëüçîâàòü ïÿòü íåçàâèñèìûõ êëþ÷åé.

15.5 Óìåíüøåíèå äëèíû êëþ÷à â CDMF

Ýòîò ìåòîä áûë ðàçðàáîòàí IBM äëÿ ïðîäóêòà CDMF (Commercial Data Masking Facility, Êîìåð÷åñêå ñðåäñòâî ìàñêèðîâàíèÿ äàííûõ) (ñì. ðàçäåë 24.8), ÷òîáû ïðåäîòâðàòèòü 56-áèòîâûé êëþ÷ DES â 40-áèòîâûé, ðàçðåøåííûé äëÿ ýêñïîðòà [785]. Ïðåäïîëàãàåòñÿ, ÷òî ïåðâîíà÷àëüíûé êëþ÷ DES ñîäåðæèò áèòû ÷åòíîñòè.

(1) Îáíóëÿþòñÿ áèòû ÷åòíîñòè: áèòû 8, 16, 24, 32, 40, 48, 56, 64.

(2) Ðåçóëüòàò ýòàïà (1) øèôðóåòñÿ ñ ïîìîùüþ DES êëþ÷îì 0xc408b0540ba1e0ae, ðåçóëüòàò øèôðîâàíèÿ îáúåäèíÿåòñÿ ïîñðåäñòâîì XOR ñ ðåçóëüòàòîì ýòàïà (1).

(3) Â ðåçóëüòàòå ýòàïà (2) îáíóëÿþòñÿ ñëåäóþùèå áèòû: 1, 2, 3, 4, 8, 16, 17, 18, 19, 2.0, 2.4, 32, 33, 34, 35, 36, 40, 48, 49, 50, 51, 52, 56, 64.

(4) Ðåçóëüòàò ýòàïà (3) øèôðóåòñÿ ñ ïîìîùüþ DES êëþ÷îì 0xef2c041ce6382fe6. Ïîëó÷åííûé êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ ñîîáùåíèÿ.

Íå çàáûâàéòå, ÷òî ýòîò ìåòîä óêîðà÷èâàåò êëþ÷ è, ñëåäîâàòåëüíî, îñëàáëÿåò àëãîðèòì.

15.6 Îòáåëèâàíèå

Îòáåëèâàíèå (whitening) íàçûâàþòñÿ ñîîáùåíèÿ XOR ÷àñòè êëþ÷à ñ âõîäîì áëî÷íîãî àëãîðèòìà è XOR äóãîé ÷àñòè êëþ÷à ñ âûõîäîì áëî÷íîãî àëãîðèòìà. Âïåðâûå ýòî ìåòîä áûë ïðèìåíåí äëÿ âàðèàíòà DESX, ðàçðàáîòàííîãî RSA Data Security, Inc., à çàòåì (ïî-âèäèìîìó, íåçàâèñèìî) â Khufu è Khafre. (Ðèâåñò è äàë èì ýòî ìåòîäó, ýòî íåîáû÷íîå èñïîëüçîâàíèå ñëîâà.)

Ñìûñë ýòèõ äåéñòâèé â òîì, ÷òîáû ïîìåøàòü êðèòîàíàëèòèêó ïîëó÷èòü ïàðó "îòêðûòûé òåêñò/øèôðîòåêñò" äëÿ ëåæàùåãî â îñíîâå áëî÷íîãî àëãîðèòìà. Ìåòîä çàñòàâëÿåò êðèïòîàíàëèòèêà óãàäûâàòü íå òîëüêî êëþ÷ àëãîðèòìà, íî è îäíî èç çíà÷åíèé òáåëèâàíèÿ. Òàê êàê XOR âûïîëíÿåòñÿ è ïåðåä, è ïîñëå áëî÷íîãî àëãîðèòìà, ñ÷èòàåòñÿ, ÷òî ýòîò ìåòîä óñòîé÷èâ ïðîòèâ âñêðûòèÿ "âñòðå÷à ïîñðåäèíå".

$$C = K_3 \oplus E_{K_2}(P \oplus K_1)$$

$$P = K_1 \oplus D_{K_2}(C \oplus K_3)$$

Åñëè $K_1 = K_2$, òî äëÿ âñêðûòèÿ ãðóáîé ñèëîé ïîòðåáóåòñÿ $2^{n+m/p}$ äåéñòâèé, ãäå n - ðàçìåð êëþ÷à, m - ðàçìåð áëîêà, è p - êîëè÷åñòâî èçâåñòíûõ îòêðûòûõ òåêñòîâ. Åñëè K_1 è K_2 ðàçëè÷íû, òî äëÿ âñêðûòèÿ ãðóáîé ñèëîé ñ òðåìÿ èçâåñòíûìè òîêðûòûìè òåêñòàìè îòðåáóåòñÿ 2^{n+m+1} äåéñòâèé. Ïðîòèâ äèôôåðåíöèàëüíîãî è êëîéíîãî êðèïòîàíàëèçà, òàêèå ìåðû îáåñïå÷èâàþò çàùèòó òîëüêî äëÿ íåñêîëüêèõ áèòîâ êëþ÷à. Íî ñ âû÷èñëèòåëüíîé òî÷êè çðåíèÿ ýòî î÷åíü äåøåâûé ñïîñîá ïîâûñèòü áåçîïàñíîñòü áëî÷íîãî àëãîðèòìà è êëþ÷åé.

15.7 Ìíîãîêðàòíîå ïîñëåäîâàòåëüíîå èñïîëüçîâàíèå áëî÷íûõ àëãîðèòìîâ

À êàê íàñ÷åò øèôðîâàíèÿ ñíà÷àëà àëãîðèòìîì À è êëþ÷îì $\hat{E}_A$, à çàòåì åùå ðàç àëãîðèòìîì Â è êëþ÷îì $\hat{E}_A$? Ìîæåò áûòü ó Àëèñû è Âîáà ðàçëè÷íûå ïðåäïî÷òåíèÿ î òîì, êàêîé àëãîðèòì áîëåå áåçîïàñåí: Àëèñà õî÷åò ïîëüçîâàòüñÿ àëãîðèòìîì À, à Âîá - àëãîðèòìîì Â. Ýòîò ïðèì, èíîãäà íàçûâàåìûé **ïîñëåäîâàòåëüíûì èñïîëüçîâàíèåì** (cascading), ìîæíî ðàñïðîñòðàíèòü è íà áîëüøåå êîëè÷åñòâî àëãîðèòìîâ è êëþ÷åé.

Ïåññèìèñòû óòâåðæäàëè, ÷òî ñîâìåñòíîå èñïîëüçîâàíèå äâóõ àëãîðèòìîâ íå ãàðàíòèðóåò ïîâûøåíèÿ áåçîïàñíîñòè. Àëãîðèòì ìîãóò âçàèìîäåéſñòâîâàòü êàêèì-òî õèòðûì ñïîñîáîì, ÷òî íà ñàìîì äåëå äàæå *óìåíüøèò*. Äàæå òðîéíîå øèôðîâàíèå òðåìÿ ðàçëè÷íûìè àëãîðèòìàìè ìîæåò íå áûòü íàñòîëüêî áåçîïàñíûì, íàñêîëüêî

âàì ýòî êàæåòñÿ. Êðèïòîãðàôèÿ - äîñòàòî÷íî òåì íîå èñêóññòâî, åñëè âû íå ñîâñåì ïîíèìàåòå, ÷òî äåëàåò, òî ìîæåò ëåãêî ïîïàñòü â áåäó.

Äåéñòâèòåëüíîñòü íàìíîãî ñâîëåå. Óïîìÿíóòûå ïðåäïîñòðåæåíèÿ âåðíû, òîëüêî åñëè ðàçëè÷íûå êëþ÷è çàâèñÿò äðóã îò äðóãà. Åñëè âñå èñïîëüçóåìûå êëþ÷è íåçàâèñèìû, òî ñëîæíîñòü âçëîìà ïîñëåäíåãî èç ïðèâåäåííûõ àëãîðèòìîâ [1033]. Åñëè âòîðîé äëãîðåòì ÷óâñòâèòåëåí ê âñêðûòèþ ñ âûáðàííûì îòêðûòûì òåêñòîì, òî ïåðâûé äëãîðèòì îáåñ÷èòü ýòî âñêðûòèå è ïðè ïîñëåäîâàòåëüíîì èñïîëüçîâàíèè ñåëåêòèâíîãî øèôðîâàíèÿ ê âñêðûòèþ ñ èçâåñòíûì îòêðûòûì òåêñòîì. Òàêîå âîçìîæíî íåëåãêî îáúÿñíèòü âñêðûòèÿ íå îãðàíè÷åíèå âñêðûòèÿ òîëüêî äëãîðèòìàìè øèôðîâàíèÿ: åñëè âû ïîçâîëèòå êîìó-òî äðóãîìó îïðåäåëèòü ëþáîé èç àëãîðèòìîâ, äåëàþùèõ ÷òî-òî ñ âàøèì ñîîáùåíèåì äî øèôðîâàíèÿ, ñòèò óäîñòîâåðèòüñÿ, ÷òî âàøå øèôðîâàíèå óñòîé÷èâî ïî îòíîøåíèþ ê âñêðûòèþ ñ âûáðàííûì îòêðûòûì òåêñòîì. (Îáðàòèòå âíèìàíèå, ÷òî íàéäåíèå ÷àñòè èñïîëüçóåìûì äëãîðèòìîì äëÿ ñæàòèÿ è îïòèôîâêè ðå÷è äî ìîäåëèðîâàíèÿ, ïðèìåíÿåìûì ïåðåä ëþáûì àëãîðèòìîì øèôðîâàíèÿ, ÿâëÿåòñÿ CELP, ðàçðàáîòàííûé NSA.)

Ýòî ìîæíî ñîîðìóëèðîâàòü è èíà÷å: Ïðè èñïîëüçîâàíèè âñêðûòèÿ ñ âûáðàííûì îòêðûòûì òåêñòîì ïîñëåäîâàòåëüíîñòü øèôðîâ âçëîìàòü íå ëåã÷å, ÷åì ëþáîé èç øèôðîâ ïîñëåäîâàòåëüíîñòè [858]. Ðÿä ðåçóëüòàòîâ ïîêàçàë, ÷òî ïîñëåäîâàòåëüíûå øèôðû âçëîìàòü íå ëåã÷å, ÷åì ëþáîé èç øèôðîâ ïîñëåäîâàòåëüíîñòè, íî â îñíîâå ýòèõ ðåçóëüòàòîâ ëåæàò íåîòðóå íåñîîòâåòñòâèÿ óñòîé÷èâî ïî îòíøåíèþ ê âñêðûòèþ ñ âûáðàííûì îòêðûòûì òåêñòîì. Òîëüêî åñëè àëãîðèòì îáëàäàåò ñèëüíîé ñòîéêîñòüþ, êàê â ñëó÷àå êàñêàäíûõ ïîòîêîâûõ øèôðîâ (èëè áëî÷íûõ øèôðîâ â ðåæèìå OFB), íàäåæíîñòü èõ ïîñëåäîâàòåëüíîñòè íå ìåíüøå, ÷åì ó ñèëüíåéøåãî èç èñïîëüçóåìûõ àëãîðèòìîâ.

Åñëè Àëèñà è Áîá íå äîâåðÿò àëãîðèòìàì äðóãà, îíè ìîãóò èñïîëüçîâàòü èõ ïîñëåäîâàòåëüíî. Äëÿ ïîòîêîâûõ àëãîðèòìîâ èõ ïîðÿäîê íå èìååò çíà÷åíèÿ. Ïðè èñïîëüçîâàíèè áëî÷íûõ àëãîðèòìîâ Àëèñà ìîæåò ñíà÷àëà èñïîëüçîâàòü àëãîðèòì A, à çàòåì àëãîðèòì B. Áîá, êîòîðûé áîëüøå äîâåðÿåò àëãîðèòìó B, ìîæåò èñïîëüçîâàòü àëãîðèòì B ïåðåä àëãîðèòìîì A. Ìåæäó àëãîðèòìàìè îíè ìîãóò âñòàâëÿòü õîðîøèé ïîòîêîâûé øèôð. Ýòî íå ïðè÷èíèò âðåäà è ìîæåò çíà÷èòåëüíî ïîâûñèòü áåçîïàñíîñòü.

Íå çàáóäüòå, ÷òî êëþ÷è äëÿ êàæäîãî àëãîðèòìà ïîñëåäîâàòåëüíîñòè äîëæíû áûòü íåçàâèñèìûìè. Åñëè àëãîðèòì A èñïîëüçóåò 64-áèòîâûé êëþ÷, à àëãîðèòì B - 128-áèòîâûé êëþ÷, òî ïîëó÷åâøàÿñÿ ïîñëåäîâàòåëüíîñòü äîëæíà èñïîëüçîâàòü 192-áèòîâûé êëþ÷. Ïðè èñïîëüçîâàíèè çàâèñèìûõ êëþ÷åé ó ïåññèìèñòîâ ãîðàçäî áîëüøå øàíñîâ îêàçàòüñÿ ïðàâûì.

15.8 Îáúåäèíåíèå íåñêîëüêèõ áëî÷íûõ àëãîðèòìîâ

Âîò äðóãîé ñïîñîá îáúåäèíèòü íåñêîëüêî áëî÷íûõ àëãîðèòìîâ, áåçîïàñíîñòü êîòîðîãî ãàðàíòèðîâàíî áóäåò ïî êðàéíåé ìåðå íà ìåíüøå, ÷åì áåçîïàñíîñòü îäíîãî àëãîðèòìà. Äëÿ ââóõ àëãîðèòìîâ (è ââóõ íåçàâèñèìûõ êëþ÷åé):

(1) Ãåíåðèðóåòñÿ ñòðîêà ñëó÷àéíûõ áèòîâ R òîãî æå ðàçìåðà, ÷òî è ñîîáùåíèå I.

(2) R øèôðóåòñÿ ïåðâûì àëãîðèòìîì.

(3) $I \oplus R$ øèôðóåòñÿ âòîðûì àëãîðèòìîì.

(4) Øèôðîâêè ñîîáùåíèÿ ÿâëÿþòñÿ îáúåäèíåíèåì ðåçóëüòàòîâ ýòàïîâ (2) è (3).

Ïðè óñëîâèè, ÷òî ñòðîêà ñëó÷àéíûõ áèòîâ äåéſòâèòåëüíî ñëó÷àéíà, ýòî ìåòîä øèôðóåò M ñ ïîìîùüþ îäíîðàçîâîãî äëèíîòà, à çàòåì ñîäåðæèìîå áëîêîâ è ïîëó÷åâøåãîñÿ ñîîáùåíèå øèôðóþòñÿ êàæäûì èç äâóõ àëãîðèòìîâ. Òàê êàê è îí, è äðóãîå íåíåõîäèìî äëÿ âîññòàíîâëåíèÿ M, êðèòè÷åñêèé ïðèâàòíûé êëþ÷ äîëæåí áûòü àëãîðèòìà. Íåäîñòàòêîì ÿâëÿåòñÿ óäâîåíèå ðàçìåðà øèôðîâêè ïî ñðàâíåíèþ ñ îòêðûòûì òåêñòîì.

Ýòîò ìåòîä ìîæíî ðàñøèðèòü äëÿ íåñêîëüêèõ àëãîðèòìîâ, íî äîáàâëåíèå êàæäîãî àëãîðèòìà óâåëè÷èâàåò øèôðîâêè. Ñàìà ïî ñåáå èäåÿ õîðîøà, íî, êàê ìíå êàæåòñÿ, íå î÷åíü ïðàêòè÷íà.

Ãëàâà 16
Ãåíåðàòîðû ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé è ïîòîêîâûå øèôðû

16.1 Ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû

Ëèíåéíûì êîíãðóýíòíûì ãåíåðàòîðîì ÿâëÿþòñÿ ãåíåðàòîðû ñëåäóþùåé ôîðìû

$X_n = (aX_{n-1} + b) \bmod m$

â êîòîðûõ X_n - ýòî n-ûé ÷ëåí ïîñëåäîâàòåëüíîñòè, à X_{n-1} - ïðåäûäóùèé ÷ëåí ïîñëåäîâàòåëüíîñòè. Ïåðåìåííûå a, b è m - ïîñòîÿííûå: a - **ìíîæèòåëü**, b - **èíêðåìåíò**, è m - ìîäóëü. Êëþ÷îì, èëè çàòðàâêîé, ñëóæèò çíà÷åíèå X_0.

Ïåðâîíà÷àëüíî ãåíåðàòîðà íå áîëüøå, ÷åì m. Åñëè a, b è m âûáðàíû ïðàâèëüíî, òî ãåíåðàòîð áóäåò **ãåíåðàòîðîì ñ ìàêñèìàëüíûì ïåðèîäîì** (èíîãäà íàçûâàåìûì ìàêñèìàëüíîé äëèíîé), è åãî ïåðèîä áóäåò ðàâåí m. (Íàïðèìåð, b äîëæíî áûòü âçàèìíî ïðîñòûì ñ m.) Ïîäðîáíûå îïèñàíèå âûâîäà êîíñòàíò äëÿ ïîëó÷åíèÿ ìàêñèìàëüíîãî ïåðèîäà ìîæíî íàéòè â [863, 942]. Åùå îäíîé õîðîøåé ñòàòüåé ïî ëèíåéíûì êîíãðóýíòíûì ãåíåðàòîðàì è èõ òåîðèè ÿâëÿåòñÿ [1446].

Â 15-é, âçÿòîé èç [1272,], ïåðå÷èñëÿþòñÿ õîðîøèå êîíñòàíòû ëèíåéíûõ êîíãðóýíòíûõ ãåíåðàòîðîâ. Âñå îíè îáåñïå÷èâàþò ãåíåðàòîðû ñ ìàêñèìàëüíûì ïåðèîäîì è, ÷òî äàæå áîëåå âàæíî, óäîâëåòâîðÿþò ñïåêòðàëüíîìó òåñòó íà ñëó÷àéíîñòü äëÿ ðàçìåðíîñòåé 2, 3, 4, 5 è 6 [385, 863]. Òàáëèöà îõâàòûâàåò ïî ìàêñèìàëüíîìó ïðîèçâåäåíèþ, êîòîðîå íå âûçûâàåò ïåðåïîëíåíèÿ â ñëîâå óêàçàííîé äëèíû.

Ïðèìóùåñòâî ëèíåéíûõ êîíãðóýíòíûõ ãåíåðàòîðîâ ÿâëÿåòñÿ èõ áûñòðîòà çà ñ÷åò ìàëîãî êîëè÷åñòâà îïåðàöèé íà áèò.

Ê íåñ÷àñòüþ ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû íåüçÿ èñïîëüçîâàòü â êðèïòîãðàôèè, òàê êàê îíè ïðåäñêàçóåìû. Âïåðâûå ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû áûëè âçëîìàíû Äæèìîì Ðèäñîì (Jim Reeds) [1294, 1295, 1296], à çàòåì Äæîàí Áîÿð (Joan Boyar) [1251]. Åé óäàëîñü òàêæå âñêðûòü êâàäðàòè÷íûå ãåíåðàòîðû:

$Xn = (aX_{n-1}^2 + bX_{n-1} + c) \bmod m$

è êóáè÷åñêèå ãåíåðàòîðû:

$Xn = (aX_{n-1}^3 + bX_{n-1}^2 + c\,X_{n-1} + d) \bmod m$

Äðóãèå èññëåäîâàòåëè ðàñøèðèëè èäåè Áîÿð, ðàçðàáîòàâ ñïîñîáû âñêðûòèÿ ëþáîãî ïîëèíîìèàëüíîãî ãåíåðàòîðà [923, 899, 900]. Áûëè âçëîìàíû è óñå÷åíû ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû [581, 705, 580], è óñå÷åíû ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû ñ íåèçâåñòíûìè ïàðàìåòðàìè [1500, 212]. Òàêèì îáðàçîì áûëà äîêàçàíà áåñïîëåçíîñòü êîíãðóýíòíûõ ãåíåðàòîðîâ äëÿ êðèïòîãðàôèè.

Òàáë. 16-1.
Êîíñòàíòû äëÿ ëèíåéíûõ êîíãðóýíòíûõ ãåíåðàòîðîâ

Ïåðèîäè÷íîñòü ïðè	a	b	m
2^{20}	106	1283	6075
2^{21}	211	1663	7875
2^{22}	421	1663	7875
2^{23}	430	2531	11979
	936	1399	6655
	1366	1283	6075
2^{24}	171	11213	53125
	859	2531	11979
	419	6173	29282
	967	3041	14406
2^{25}	141	28411	134456
	625	6571	31104
	1541	2957	14000
	1741	2731	12960
	1291	4621	21870
	205	29573	139968
2^{26}	421	17117	81000
	1255	6173	29282

	281	28411	134456
2^{27}	1093	18257	86436
	421	54773	259200
	1021	24631	116640
	1021	25673	121500
2^{28}	1277	24749	117128
	741	66037	312500
	2041	25673	121500
2^{29}	2311	25367	120050
	1807	45289	214326
	1597	51749	244944
	1861	49297	233280
	2661	36979	175000
	4081	25673	121500
	3661	30809	145800
2^{30}	3877	29573	139968
	3613	45289	214326
	1366	150889	714025
2^{31}	8121	28411	134456
	4561	51349	243000
	7141	54773	259200
2^{32}	9301	49297	233280
	4096	150889	714025
2^{33}	2416	374441	1771875
2^{34}	17221	107839	510300
	36261	66037	312500
2^{35}	84589	45989	217728

Îäíàêî, ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû ñîõðàíÿþò ñâîþ ïîëåçíîñòü äëÿ íåêîòîðûõ çàäà÷ïðèëîæåíèé, íàïðèìåð, äëÿ ìîäåëèðîâàíèÿ. Îíè ýôôåêòèâíû è â áîëüøèíñòâå èñïîëüçóåìûõ ýìïèðè÷åñêèõ òåñòàõ äåìîíñòðèðóþò õîðîøèå ñòàòèñòè÷åñêèå õàðàêòåðèñòèêè. Âàæíóþ èíôîðìàöèþ î ëèíåéíûõ êîíãðóýíòíûõ ãåíåðàòîðàõ è èõ òåîðèè ìîæíî íàéòè â [942].

Îáúåäèíåíèå ëèíåéíûõ êîíãðóýíòíûõ ãåíåðàòîðîâ

Áûë ïðåäïðèíÿò ðÿä ïîïûòîê îáúåäèíåíèÿ ëèíåéíûõ êîíãðóýíòíûõ ãåíåðàòîðîâ [1595, 941]. Êðèòåðèåì îöåíêè êà÷åñòâà ïîëó÷åííûõ ðåçóëüòàòîâ íå ïîâûøàåòñÿ, íî îíè îáëàäàþò áîëåå äëèííûì ïåðèîäîì è ëó÷øèì õàðàêòåðèñòèêàì â íåêîòîðûõ ñòàòèñòè÷åñêèõ òåñòàõ. Äëÿ 32-áèòîâûõ êîìïüþòåðîâ ìîæíî èñïîëüçîâàòü ñëåäóþùèé ãåíåðàòîð [941]:

```
static long sl = 1 ; /* "long" äîëæíî áûòü 32-áèòîâûì öåëûì. */ static long s2 = 1 ;

#define MODMULT(a,b,c,m,s) q = s/a; s = b*(s-a*q) - c*q; if (s<0) s+=m ;
/* MODMIJLT(a,b,c,nl,s) ðàññ÷èòûâàåò s*b mod m ïðè óñëîâèè, ÷òî m=a*b+c è 0 <= c < m. */

/* combinedLCG âîçâðàùàåò äâéñòâèòåëüíîå ïñåâäîñëó÷àéíîå çíà÷åíèå â äèàïàçîíå
* (0,1). Îíà îáúåäèíÿåò ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû ñ ïåðèîäàìè
* 2^31-85 è 2^31-249, è åå ïåðèîä ðàâåí ïðîèçâåäåíèþ ýòèõ âåëè÷èí. */

double combinedLCG ( void )
{
     long q ;
     long z ;
     MODMULT ( 53668, 40014, 12211, 2147483563L, s1 )
     MODMULT ( 52774, 40692, 3791, 2147483399L, s2 )
     z = s1 - s2 ;
     if ( z < 1 )
            z += 2147483562 ;
     return z * 4.656613e-10 ;
}

/* Â îáùåì ñëó÷àå ïåðåä èñïîëüçîâàíèåì combinedLCG âûçûâàåòñÿ initLCG. */
void initLCG( long InitS1, long InitS2 )
{
     sl = InitS1;
     s2 = InitS2;
}
```

Ýòîò ãåíåðàòîð ðàáîòàåò ïðè óñëîâèè, ÷òî êîìïüþòåð ìîæåò ïðåäñòàâèòü âñå öåëûå ÷èñëà ìåæäó $-2^{31}+85$ è $2^{31}-249$. Ïåðâîíà÷àëüíûå s_1 è s_2 ãëîáàëüíû è ñîäåðæàò òåêóùåå ñîñòîÿíèå ãåíåðàòîðà. Ïåðåä ïåðâûì âûçîâîì èõ íåîáõîäèìî ïðîèíèöèàëèçèðîâàòü. Äëÿ ïåðâîíà÷àëüíîé s_1 íà÷åëüíîå çíà÷åíèå äîëæíî ëåæàòü â äèàïàçîíå ìåæäó 1

è 2147483562, äëÿ ïåðâîíà÷íîé s_2 - ìåæäó 1 è 2147483398. Ïåðèîä ãåíåðàòîðà áëèçîê ê 10^{18}.

Íà 16-áèòîâîì êîìïüþòåðå èñïîëüçóéòå äóãîé ãåíåðàòîð:

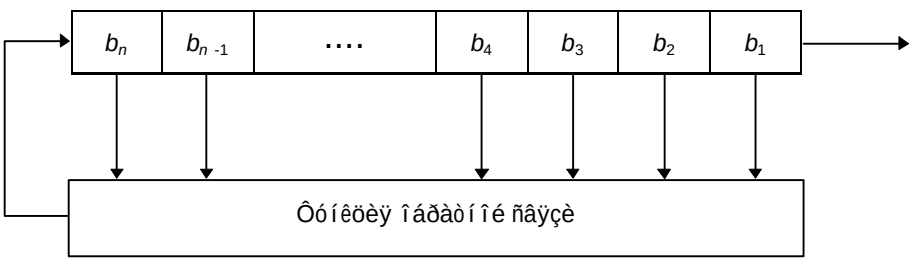
```
static int sl = 1 ; /* "int" äîëæíî áûòü 16-áèòîâûì öåëûì. */
static int s2 = 1 ;
static int s3 = 1 ;

#define MODMULT(a,b,c,m,s) q = s/a; s = b*(s-a*q) - c*q; if (s<0) s+=m ;
/* combinedLCG âû÷èñëÿåò ïñåâäîñëó÷àéíûå çíà÷åíèå â äèàïàçîíå
* (0,1). Îíà îáúåäèíÿåò ëèíåéíûå êîíãðóýíòíûå ãåíåðàòîðû ñ ïåðèîäàìè 2^15-405,
* 2^15-1041 è 2^15-1111, è åå ïåðèîä ðàâåí ïðîèçâåäåíèþ ýòèõ òðåõ ïðîñòûõ ÷èñåë. */

double combinedLCG ( void )
{
     long q ;
     long z ;

     MODMULT ( 206, 157, 21, 32363, sl )
     MODMULT ( 217, 146, 45, 31727, s2 )
     MODMULT ( 222, 142, 133, 31657, s3 )
     z = s1 - s2 ;
     if ( z < 1 )
             z -= 32362 ;
     z += s3 ;
     if ( z < 1 )
             z += 32362 ;
     return z * 3.0899e-5 ;

}

/* Â îáùåì ñëó÷àå ïåðåä èñïîëüçîâàíèåì combinedLCG âûçûâàåòñÿ initLCG. */
void initLCG( long InitS1, long InitS2, long InitS3)
{
     sl = InitS1;
     s2 = InitS2;
     s3 = InitS3;
}
```

Ýòîò ãåíåðàòîð ðàáîòàåò ïðè óñëîâèè, ÷òî êîìïüþòåð ìîæåò ïðåäñòàâèòü âñå öåëûå ÷èñëà ìåæäó -32363 è 32363. Ïåðâîíà÷àëüíûå s_1, s_2 è s_3 ãëîáàëüíû è ñîäåðæàò òåóùåå ñîñòîÿíèå ãåíåðàòîðà. Ïåðåä ïåðâûì âûçîâîì èõ íåîáõîäèìî ïðîèíèöèàëèçèðîâàòü. Äëÿ ïåðâîíà÷àëüíîé s_1 íà÷àëüíîå çíà÷åíèå äîëæíî ëåæàòü â äèàïàçîíå ìåæäó 1 è 32362, äëÿ ïåðâîíà÷àëüíîé s_2 - ìåæäó 1 è 31726, äëÿ ïåðâîíà÷àëüíîé s_3 - ìåæäó 1 è 31656. Ïåðèîä ãåíåðàòîðà ðàâåí $1.6*10^{13}$. Äëÿ îáîèõ ãåíåðàòîðîâ êîíñòàíòà *b* ðàâíà 0.

16.2 Ñãåíåðèðîâàííàÿ ðåãèñòðû ñ ëèíåéíîé îáðàòíîé ñâÿçüþ

Ïîñëåäîâàòåëüíîñòè ñãåíåðèðîâàííûõ ðåãiñòðîâ èñïîëüçóþòñÿ êàê â êðèïòîãðàôèè, òàê è â òåîðèè êîäèðîâàíèÿ. Èõ òåîðèÿ ïðåêðàñíî ïðîðàáîòàíà, ïîòîêîâûå øèôðû íà áàçå ñãåíåðèðîâàííûõ ðåãiñòðîâ ÿâëÿëèñü ðàáî÷åé ëîøàäêîé âîåííîé êðèïòîãðàôèè çàäîëãî äî ïîÿâëåíèÿ ýëåêòðîíèêè.

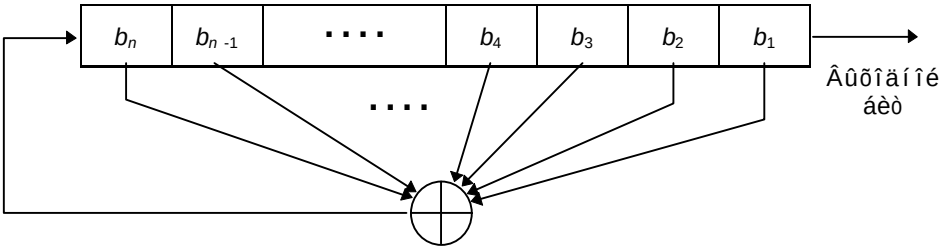
Ñãåíåðèðîâàííûé ðåãiñòð ñ îáðàòíîé ñâÿçüþ ñîñòîèò èç äâóõ ÷àñòåé: ñãåíåðèðîâàííîãî ðåãiñòðà è **ôóíêöèè îáðàòíîé ñâÿçè** (ñì. 15th). Ñãåíåðèðîâàííûé ðåãiñòð ïðåäñòàâëÿåò ñîáîé ïîñëåäîâàòåëüíîñòü áèòîâ. (Êîëè÷åñòâî áèòîâ îïðåäåëÿåòñÿ **äëèíîé** ñãåíåðèðîâàííîãî ðåãiñòðà. Åñëè äëèíà ðàâíà *n* áèòàì, òî ðåãiñòð íàçûâàåòñÿ *n*-áèòîâûì ñãåíåðèðîâàííûì ðåãiñòðîì.) Âñÿêèé ðàç, êîãäà íóæíî èçëåâ÷ü áèò, âñå áèòû ñãåíåðèðîâàííîãî ðåãiñòðà ñãåíåðàþòñÿ âïðàâî íà 1 ïîçèöèþ. Íîâûé êðàéíèé ëåâûé áèò ÿâëÿåòñÿ ôóíêöèåé âñåõ îñòàëüíûõ áèòîâ ðåãiñòðà. Íà âûõîäå ñãåíåðèðîâàííîãî ðåãiñòðà îêàçûâàåòñÿ îäèí, îáû÷íî ìëàäøèé çíà÷àùèé, áèò. **Ïðèìåíåíèå** ñãåíåðèðîâàííîãî ðåãiñòðà íàçûâàåòñÿ äëèíà ïîëó÷àåìîé ïîñëåäîâàòåëüíîñòè äî íà÷àëà åå ïîâòîðåíèÿ.



Ðèñ. 16-1. Ñãåíåðèðîâàííûé ðåãiñòð ñ îáðàòíîé ñâÿçüþ

Êðèïòîãðàôè íàâåëèñü ïîòîêîâûå øèôðû íà áàçå ñãåíåðèðîâàííûõ ðåãiñòðîâ: îíè ëåãêî ðåàëèçîâûâàëèñü ñ ïîìîùüþ öèôðîâîé àïïàðàòóðû. ß ëèøü ñëåãêà çàòðóäíèë ìàòìàòè÷åñêóþ òåîðèþ. Â 1965 ãîäó Ýðíñò Ñåëìåð (Ernst Selmer), ãëàâíûé êðèïòîãðàô íîðâåæñêîãî ïðàâèòåëüñòâà, ðàçðàáîòàë òåîðåòè÷åñêóþ ìîäåëü ïîñëåäîâàòåëüíîñòè ñãåíåðèðîâàííûõ ðåãiñòðîâ [1411]. Ñîëîìîí Âîëîìà (Solomon Golomb), ìàòìàòèê NSA, íàïèñàë êíèãó, èçëàãàþùèå åíåêîòîðûå ñâîè ðåçóëüòàòû è ðåçóëüòàòû Ñåëìåðà [643]. Ñì. òàêæå [970, 971, 1647].

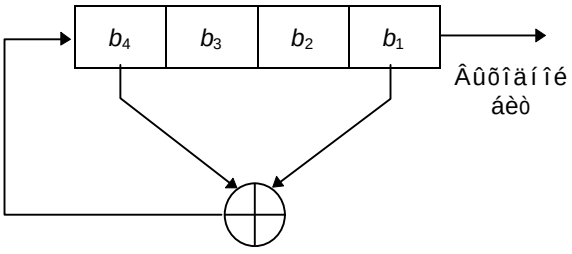
Ïðîñòåéøèì âèäîì ñäâèãîâîãî ðåãèñòðà ñ îáðàòíîé ñâÿçüþ ÿâëÿåòñÿ **ëèíåéíûé ñäâèãîâûé ðåãèñòð ñ îáðàòíîé ñâÿçüþ** (linear feedback shift register, èëè LFSR) (ñì. 14th). Îáðàòíàÿ ñâÿçü ïðåäñòàâëÿåò ñîáîé ïðîñòî XOR íåêîòîðûõ áèòîâ ðåãèñòðà, ïåðå÷íü ýòèõ áèòîâ íàçûâàåòñÿ **îòâîäíîé ïîñëåäîâàòåëüíîñòüþ** (tap sequence). Èíîãäà òàêîé ðåãèñòð íàçûâàåòñÿ **êîíôèãóðàöèåé Ôèáîíà÷è**. Èç-çà ïðîñòîòû ïîñëåäîâàòåëüíîñòè îáðàòíîé ñâÿçè äëÿ àíàëèçà LFSR ìîæíî èñïîëüçîâàòü äîâîëüíî ðàçâèòóþ ìàòåìàòè÷åñêóþ òåîðèþ, óáåæäàÿ ñåáÿ, ÷òî ýòè ïîñëåäîâàòåëüíîñòè äîñòàòî÷íî ñëó÷àéíû, ÷òîáû áûòü áåçîïàñíûì. LFSR ÷àùå äóãèõ ñäâèãîâûõ ðåãèñòðîâ èñïîëüçóþòñÿ â êðèïòîãðàôèè.



Ðèñ. 16-2. Ñäâèãîâûé ðåãèñòð ñ ëèíåéíîé îáðàòíîé ñâÿçüþ.

Íà 13-é ïîêàçàí 4-áèòîâûé LFSR ñ îòâîäîì îò ïåðâîãî è ÷åòâåðòîãî áèòîâ. Åñëè åãî ïðîèíèöèàëèçèðîâàòü çíà÷åíèåì 1111, òî äî ïîâòîðåíèÿ ðåãèñòð áóäåò ïðèíèìàòü ñëåäóþùèå âíóòðåííèå ñîñòîÿíèÿ:

1 1 1 1
0 1 1 1
1 0 1 1
0 1 0 1
1 0 1 0
1 1 0 1
0 1 1 0
0 0 1 1
1 0 0 1
0 1 0 0
0 0 1 0
0 0 0 1
1 0 0 0
1 1 0 0
1 1 1 0



Ðèñ. 16-3. 4-áèòîâûé LFSR.

Âûõîäíîé ïîñëåäîâàòåëüíîñòüþ áóäåò ñòðîêà ìëàäøèõ çíà÷àùèõ áèòîâ:

1 1 1 1 0 1 0 1 1 0 0 1 0 0 0. . . .

n-áèòîâûé LFSR ìîæåò íàõîäèòüñÿ â îäíîì èç 2^n-1 âîçìîæíûõ ñîñòîÿíèé. Ýòî îçíà÷àåò, ÷òî òåðåòè÷åñêè òàêîé ðåãèñòð ìîæåò åäíåðèðîâàòü ïñåâäîñëó÷àéíóþ ïîñëåäîâàòåëüíîñòü ñ ïåðèîäîì 2^n-1 áèòîâ. (×èñëî âîçìîæíûõ ñîñòîÿíèé è ïåðèîä ðàâíû 2^n-1, ïîòîìó ÷òî çàïîëíåíèå LFSR íóëåâûìè, ïðèâåäåò ê òîìó, ÷òî ñäâèãîâûé ðåãèñòð áóäåò âûäàâàòü áåñêîíå÷íóþ ïîñëåäîâàòåëüíîñòü íóëåé, ÷òî àáñîëþòíî áåñïîëåçíî.) Òîëüêî ïðè îïðåäåëåííûõ îòâîäíûõ ïîñëåäîâàòåëüíîñòÿõ LFSR öèêëè÷åñêè ïðîéäåò ÷åðåç âñå 2^n-1 âîçìîæíûõ ñîñòîÿíèé, òàêèå

LFSR ÿâëÿþòñÿ LFSR ñ ìàêñèìàëüíûì ïåðèîäîì. Ïîëó÷èâøèéñÿ ðåçóëüòàò íàçûâàåòñÿ **Ìíîãî÷ëåíîì ïîëíîãî ïåðèîäà**.

Äëÿ òîãî, ÷òîáû êîíêðåòíûé LFSR èìåë ìàêñèìàëüíûé ïåðèîä, ìíîãî÷ëåí, îáðàçîâàííûé èç îòâîäíîé ïîñëåäîâàòåëüíîñòè è êîíñòàíòû 1, äîëæåí áûòü ïðèìèòèâíûì ïî ìîäóëþ 2. **Ñòåïåíü** ìíîãî÷ëåíà ÿâëÿåòñÿ äëèíîé ñäâèãîâîãî ðåãèñòðà. Ïðèìèòèâíûé ìíîãî÷ëåí ñòåïåíè n - ýòî íåïðèâîäèìûé ìíîãî÷ëåí, êîòîðûé ÿâëÿåòñÿ äåëèòåëåì $x^{2^{n-1}}+1$, íî íå ÿâëÿåòñÿ äåëèòåëåì x^d+1 äëÿ âñåõ d, ÿâëÿþùèõñÿ äåëèòåëÿìè 2^n-1 (ñì. ðàçäåë 11.3). Ñîîòâåòñòâóþùàÿ ìàòåìàòè÷åñêàÿ òåîðèÿ îïèñàíà â [643, 1649, 1648].

Â îáùåì ñëó÷àå íå ñóùåñòâóåò ïðîñòîãî ñïîñîáà ãåíåðèðîâàòü ïðèìèòèâíûå ìíîãî÷ëåíû äàííîé ñòåïåíè ïî ìîäóëþ 2. Ïðîùå âñåãî âûáðàòü ìíîãî÷ëåí ñëó÷àéíûì îáðàçîì è ïðîâåðÿòü, íå ÿâëÿåòñÿ ëè îí ïðèìèòèâíûì. Ýòî íåëåãêî - è ÷ì-òî ïîõîæå íà ïðîâåðêó, íå ÿâëÿåòñÿ ëè ïðîñòûì ñëó÷àéíî âûáðàííûå ÷èñëî - íî ìíîãèå ìàòåìàòè÷åñêèå ïàêåòû ïðîãðàìì óìåþò ðåøàòü òàêóþ çàäà÷ó. Ðÿä ìåòîäîâ ïðèâåäåí â [970, 971].

Íåêîòîðûå, íî, êîíå÷íî æå, íå âñå, ìíîãî÷ëåíû ðàçëè÷íûõ ñòåïåíåé, ïðèìèòèâíûå ïî ìîäóëþ 2, ïðèâåäåíû â 14-é [1583, 643, 1649, 1648, 1272, 691]. Íàïðèìåð, çàïèñü (32, 7, 5, 3, 2, 1, 0) îçíà÷àåò, ÷òî ñëåäóþùåé ìíîãî÷ëåí ïðèìèòèâåí ïî ìîäóëþ 2:

$$x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$$

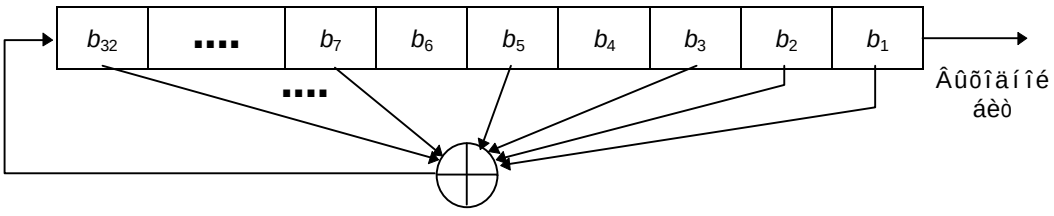
Ýòî ìîæíî ëåãêî îáîáùèòü äëÿ LFSR ñ ìàêñèìàëüíûì ïåðèîäîì. Ïåðâûì ÷èñëîì ÿâëÿåòñÿ äëèíà LFSR. Ïîñëåäíåå ÷èñëî âñåãäà ðàâíî 0, è åãî ìîæíî îïóñòèòü. Âñå ÷èñëà, çà èñêëþ÷åíèåì 0, çàäàþò îòâîäóþ ïîñëåäîâàòåëüíîñòü, îòñ÷èòûâàåìóþ îò ëåâîãî êðàÿ ñäâèãîâîãî ðåãèñòðà. Òî åñòü, ÷ëåíû ìíîãî÷ëåíà ñ ìåíüøåé ñòåïåíüþ ñîîòâåòñòâóþò ïîçèöèÿì áèòæâ ê ïðàâîìó êðàþ ðåãèñòðà.

Ïðîâîëæàÿ ïðèìåð, çàïèñü (32, 7, 5, 3, 2, 1, 0) îçíà÷àåò, ÷òî äëÿ âçÿòîãî 32-áèòîâîãî ñäâèãîâîãî ðåãèñòðà íîâûé áèò íîâûé áèò ãåíåðèðóåòñÿ ñ ïîìîùüþ XOR òðèäöàòè âòîðîãî, ñåäüìîãî, ïÿòîãî, òðåòüåãî, âòîðîãî è ïåðâîãî áèòîâ (ñì. 12th), ïîëó÷àþùèéñÿ LFSR áóäåò èìåòü ìàêñèìàëüíóþ äëèíó, öèêëè÷åñêè ïðîõîäÿ äî ïîâòîðåíèÿ ÷åðåç 2^{32}-1 çíà÷åíèé.

Êîä äëÿ ýòîãî LFSR íà ÿçûêå C âûãëÿäèò ñëåäóþùèì îáðàçîì:

```
int LFSR ( ) {
     static unsigned long ShiftRegister = 1;
     /* Âñå, êðîìå 0. */
     ShiftRegister = ((((ShiftRegister >> 31)
            ^(ShiftRegister >> 6)
            ^(ShiftRegister >> 4)
            ^(ShiftRegister >> 2)
            ^(ShiftRegister >> 1)
            ^ShiftRegister))
            & 0x00000001)
            <<31)
            | (ShiftRegister >> 1) ;
     return ShiftRegister & 0x00000001;
}
```

Åñëè ñäâèãîâûé ðåãèñòð äëèíîåé êîìïüþòåðíîãî ñëîâà, êîä óñëîæíÿåòñÿ, íî íå íàìíîãî.



Ðèñ. 16-4. 32-áèòîâûé LFSR ñ ìàêñèìàëüíîé äëèíîé.

Òàáë. 16-2.
Íåêîòîðûå ïðèìèòèâíûå ìíîãî÷ëåíû ïî ìîäóëþ 2

(1, 0)	(7, 3, 0)	(14, 5, 3, 1, 0)	(18, 5, 2, 1, 0)
(2, 1, 0)	(8, 4, 3, 2, 0)	(15, 1, 0)	(19, 5, 2, 1, 0)
(3, 1, 0)	(9, 4, 0)	(16, 5, 3.2, 0)	(20, 3, 0)
(4, 1, 0)	(10, 3, 0)	(17, 3, 0)	(21, 2, 0)
(5, 2, 0)	(11, 2, 0)	(17, 5, 0)	(22, 1, 0)
(6, 1, 0)	(12, 6, 4, 1, 0)	(17, 6, 0)	(23, 5, 0)
(7, 1, 0)	(13, 4, 3, 1, 0)	(18, 7, 0)	(24, 4, 3, 1, 0)

(25, 3, 0)
(26, 6, 2, 1, 0)
(27, 5, 2, 1, 0)
(28, 3, 0)
(29, 2, 0)
(30, 6, 4, 1.0)
(31, 3, 0)
(31, 6, 0)
(31, 7, 0)
(31, 13, 0)
(32, 7, 6, 2, 0)
(32, 7, 5, 3, 2, 1, 0)
(33, 13, 0)
(33, 16, 4, 1, 0)
(34, 8, 4, 3, 0)
(34, 7, 6, 5, 2, 1, 0)
(35, 2, 0)
(135, 11, 0)
(135, 16, 0)
(135, 22, 0)
(136, 8, 3, 2, 0)
(137, 21, 0)
(138, 8, 7, 1, 0)
(139, 8, 5, 3, 0)
(140, 29, 0)
(141, 13, 6, 1, 0)
(142, 21, 0)
(143, 5, 3, 2, 0)
(144, 7, 4, 2, 0)
(145, 52, 0)
(145, 69, 0)
(146, 5, 3, 2, 0)
(147, 11, 4, 2, 0)
(148, 27, 0)
(149, 10, 9, 7, 0)
(150, 53, 0)
(151, 3, 0)
(151, 9, 0)
(151, 15, 0)
(151, 31, 0)
(151, 39, 0)
(151, 43, 0)
(151, 46, 0)
(151, 51, 0)
(151, 63, 0)
(151, 66, 0)
(151, 67, 0)
(151, 70, 0)
(36, 11, 0)
(36, 6, 5, 4, 2, 1, 0)
(37, 6, 4, 1, 0)
(37, 5, 4, 3, 2, 1, 0)
(38, 6, 5, 1, 0)
(39, 4, 0)
(40, 5, 4, 3, 0)
(41, 3, 0)
(42, 7, 4, 3, 0)
(42, 5, 4, 3, 2, 1, 0)
(43, 6, 4, 3, 0)
(44, 6, 5, 2, 0)
(45, 4, 3, 1, 0)
(46, 8, 7, 6, 0)
(46, 8, 5, 3, 2, 1, 0)
(47, 5, 0)
(48, 9, 7, 4, 0)
(48, 7, 5, 4, 2, 1, 0)
(49, 9, 0)
(49, 6, 5, 4, 0)
(50, 4, 3, 2, 0)
(51, 6, 3, 1, 0)
(52, 3, 0)
(53, 6, 2, 1, 0)
(54, 8, 6, 3, 0)
(54, 6, 5, 4, 3, 2, 0)
(55, 24, 0)
(55, 6, 2, 1, 0)
(56, 7, 4, 2, 0)
(57, 7, 0)
(57, 5, 3, 2, 0)
(58, 19.0)
(58, 6, 5, 1, 0)
(59, 7, 4, 2, 0)
(59, 6, 5, 4, 3, 1, 0)
(60, 1, 0)
(61, 5, 2, 1, 0)
(62, 6, 5, 3, 0)
(63, 1, 0)
(64, 4, 3, 1, 0)
(65, 18, 0)
(65, 4, 3, 1, 0)
(66, 9, 8, 6, 0)
(66, 8, 6, 5, 3, 2, 0)
(67, 5, 2, 1, 0)
(152, 6, 3, 2, 0)
(153, 1, 0)
(153, 8, 0)
(154, 9, 5, 1, 0)
(155, 7, 5, 4, 0)
(156, 9, 5, 3, 0)
(157, 6, 5, 2, 0)
(158, 8, 6, 5, 0)
(159, 31, 0)
(159, 34, 0)
(159, 40, 0)
(160, 5, 3, 2, 0)
(161, 18, 0)
(161, 39, 0)
(161, 60, 0)
(162, 8, 7, 4, 0)
(163, 7, 6, 3, 0)
(164, 12, 6, 5, 0)
(165, 9, 8, 3, 0)
(166, 10, 3, 2, 0)
(167, 6, 0)
(170, 23, 0)
(172, 2, 0)
(174, 13, 0)
(175, 6, 0)
(175, 16, 0)
(175, 18, 0)
(175, 57, 0)
(177, 8, 0)
(177, 22, 0)
(1 77, 88, 0)
(68, 9, 0)
(68, 7, 5, 1, 0)
(69, 6, 5, 2, 0)
(70, 5, 3, 1, 0)
(71, 6, 0)
(71, 5, 3, 1, 0)
(72, 10, 9, 3, 0)
(72, 6, 4, 3, 2, 1, 0)
(73, 25, 0)
(73, 4, 3, 2, 0)
(74, 7, 4, 3, 0)
(75, 6, 3, 1, 0)
(76, 5, 4, 2, 0)
(77, 6, 5, 2, 0)
(78, 7, 2, 1, 0)
(79, 9, 0)
(79, 4, 3, 2, 0)
(80, 9, 4, 2, 0)
(80, 7, 5, 3, 2, 1, 0)
(81, 4, 0)
(82, 9, 6, 4, 0)
(82, 8, 7, 6, 1, 0)
(83, 7, 4, 2, 0)
(84, 13, 0)
(84, 8, 7, 5, 3, 1, 0)
(85, 8, 2, 1, 0)
(86, 6, 5, 2, 0)
(87, 13, 0)
(87, 7, 5, 1, 0)
(88, 11, 9, 8, 0)
(88, 8, 5, 4, 3, 1, 0)
(89, 38, 0)
(89, 51, 0)
(89, 6, 5, 3, 0)
(90, 5, 3, 2, 0)
(91, 8, 5, 1, 0)
(91, 7, 6, 5, 3, 2, 0)
(92, 6, 5, 2, 0)
(93, 2, 0)
(94, 21, 0)
(94, 6, 5, 1, 0)
(95, 11, 0)
(95, 6, 5, 4, 2, 1, 0)
(96, 10, 9, 6, 0)
(96, 7, 6, 4, 3, 2, 0)
(178, 87, 0)
(183, 56, 0)
(194, 87, 0)
(198, 65, 0)
(201, 14, 0)
(201, 17, 0)
(201, 59, 0)
(201, 79, 0)
(202, 55, 0)
(207, 43, 0)
(212, 105, 0)
(218, 11, 0)
(218, 15, 0)
(218, 71, 0)
(218.83, 0)
(225, 32, 0)
(225, 74, 0)
(225, 88, 0)
(225, 97, 0)
(225, 109, 0)
(231, 26, 0)
(231, 34, 0)
(234, 31, 0)
(234, 103, 0)
(236, 5, 0)
(250, 103, 0)
(255, 52, 0)
(255, 56, 0)
(255, 82, 0)
(258, 83, 0)
(266, 47, 0)
(97, 6, 0)
(98, 11, 0)
(98, 7, 4, 3, 1, 0)
(99, 7, 5, 4, 0)
(100, 37, 0)
(100, 8, 7, 2, 0)
(101, 7, 6, 1, 0)
(102, 6, 5, 3, 0)
(103, 9, 9)
(104, 11, 10, 1, 0)
(105, 16, 0)
(106, 15, 0)
(107, 9, 7, 4, 0)
(108, 31, 0)
(109, 5, 4, 2.0)
(110, 6, 4, 1, 0)
(111, 10, 0)
(111, 49, 0)
(113, 9, 0)
(113, 15, 0)
(113, 30, 0)
(114, 11, 2, 1, 0)
(115, 8, 7, 5, 0)
(116, 6, 5, 2, 0)
(117, 5, 2, 1, 0)
(118, 33, 0)
(119, 8, 0)
(119, 45, 0)
(120, 9, 6, 2, 0)
(121, 18, 0)
(122, 6, 2, 1, 0)
(123, 2, 0)
(124, 37, 0)
(125, 7, 6, 5, 0)
(126, 7, 4, 2, 0)
(127, 1, 0)
(127, 7, 0)
(127, 63, 0)
(128, 7, 2, 1, 0)
(129, 5, 0)
(130, 3, 0)
(131, 8, 3, 2, 0)
(132, 29, 0)
(133, 9, 8, 2, 0)
(134, 57, 0)
(270, 133, 0)
(282, 35, 0)
(282, 43, 0)

(286, 69, 0)	(378, 43, 0)	(521, 168, 0)	(2281, 915, 0)
(286, 73, 0)	(378, 107, 0)	(607, 105, 0)	(2281, 1029, 0)
(294, 61, 0)	(390, 89, 0)	(607, 147, 0)	(3217, 67, 0)
(322, 67, 0)	(462, 73, 0)	(607, 273, 0)	(3217, 576, 0)
(333, 2, 0)	(521, 32, 0)	(1279, 216, 0)	(4423, 271, 0)
(350, 53, 0)	(521, 48, 0)	(1279, 418, 0)	(9689, 84, 0)
(366, 29, 0)	(521, 158, 0)	(2281, 715, 0)	

Îáðàòèòå âíèìàíèå, ÷òî ó âñåõ ýëåìåíòîâ òàáëèöû íå÷åòíûå ÷èñëî êîýôôèöèåíòîâ. ß ïðèâåë òàêóþ äëèííóþ òàáëèöó, òàê êàê LSR ÷àñòî èñïîëüçóþòñÿ äëÿ êðèïòîãðàôèè ñ ïîòîêîâûì øèôðîâàíèå, è ÿ õîòåë, ÷òîáû ðàçíûå ëþäè ìîãëè ïîäîáðàòü ðàçëè÷íûå ïðèìèòèâíûå ìíîãî÷ëåíû. Åñëè $p(x)$ ïðèìèòèâåí, òî ïðèìèòèâåí è $x^n p(1/x)$, ïîýòîìó êàæäûé ýëåìåíò òàáëèöû íà ñàìîì äåëå îïðåäåëÿåò äâà ïðèìèòèâíûõ ìíîãî÷ëåíà.

Íàïðèìåð, åñëè $(a, b, 0)$ ïðèìèòèâåí, òî ïðèìèòèâåí è $(a, a - b, 0)$. Åñëè ïðèìèòèâåí $(a, b, c, d, 0)$, òî ïðèìèòèâåí è $(a, a - d, a - c, a - b, 0)$. Ìàòåìàòè÷åñêè:

åñëè ïðèìèòèâåí $x^a + x^b + 1$, òî ïðèìèòèâåí è $x^a + x^{a-b} + 1$

åñëè ïðèìèòèâåí $x^a + x^b + x^c + x^d + 1$, òî ïðèìèòèâåí è $x^a + x^{a-d} + x^{a-c} + x^{a-b} + 1$

Áûñòðåå âñåãî ïðîâåðèòü ïðèìèòèâíûå òðåõ÷ëåíû, òàê êàê äëÿ ãåíåðàöèè íîâîãî áèòà òóæíî âûïîëíÿòü XOR òîëüêî äâóõ áèòîâ ñäâèãîâîãî ðåãèñòðà. Äåéñòâèòåëüíî, âñå ìíîãî÷ëåíû îáðàòíûå â 14-é, ÿâëÿþñü **ðàçðåæåííûìè**, òî åñòü, ó íèõ íåìíîãî êîýôôèöèåíòîâ. Ðàçðåæåííîñòü âñåãäà ïðåäñòàâëÿò ñîâîê èñòî÷íèêè ñëàáîñòè, êîòîðîé èíîãäà äîñòàòî÷íî äëÿ âñêðûòèÿ àëãîðèòìà. Äëÿ êðèïòîãðàôè÷åñêèõ àëãîðèòìîâ ãîðàçäî ëó÷øå èñïîëüçîâàòü **ïëîòíûå** ïðèìèòèâíûå ìíîãî÷ëåíû, òà, ó êîòîðûõ ìíîãî êîýôôèöèåíòîâ. Ïðèìåíÿÿ ïîíÿòíûå ìíîãî÷ëåíû, îñîáåííî â êà÷åñòâå ÷àñòè êëþ÷à, ìîæíî èñïîëüçîâàòü çíà÷èòåëüíî áîëåå êîðîòêèå LFSR.

Ãåíåðèðîâàòü ïëîòíûå ïðèìèòèâíûå ìíîãî÷ëåíû ïî ìîäóëþ 2 íåëåãêî. Â îáùåì ñëó÷àå äëÿ ãåíåðàöèè ïðèìèòèâíûõ ìíîãî÷ëåíîâ ñòåïåíè *k* íóæíî çíàòü ðàçëîæåíèå íà ìíîæèòåëè ÷èñëà 2^k-1. Ïðèìèòèâíûå ìíîãî÷ëåíû ìîæíî íàéòè â ñëåäóþ ùèõ òðóäàõ: [652, 1285, 1287].

Ñàìè ïî ñåáå LFSR ÿâëÿþñü õîðîøèìè ãåíåðàòîðàìè ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé, íî îíè îáëàäàþò íåêîòîðûìè íæåëàòåëüíûìè íåëó÷àéíûìè ñâîéñòâàìè. Ïîñëåäîâàòåëüíûå áèòû ëèíåéíû, ÷òî äåëàåò èõ áåñïîëåçíûìè äëÿ øèôðîâàíèÿ. Äëÿ LFSR äëèíû *n* âîóòðåííåå ñîñòîÿíèå ïðåäñòàâëÿåò ñîáîé ïðåäûäóùèå *n* âûõîäíûõ áèòîâ ãåíåðàòîðà. Äàæå åñëè ñòåïåíü ïîëíîãî÷ëåíà îêàçûâàåòñÿ ïîëíîé, îíà ìîæåò áûòü îïðåäåëåíà ïî 2*n* âûõîäíûì áèòàì ãåíåðàòîðà ñ ïîìîùüþ âûñîêî ýôôåêòèâíîãî àëãîðèòìà Berlekamp-Massey [1082,1083]: ñì. ðàçäåë 16.3.

Êðîìå òîãî, áîëüøèå ñëó÷àéíûå ÷èñëà, ãåíåðèðóåìûå ñ èñïîëüçîâàíèåì èäóùèõ ïîäðÿä áèòîâ ýòîé ïîñëåäîâàòåëüíîñòè, ñëëüíî êîððåëèðîâàííû è äëÿ íåêîòîðûõ òèïîâ ïðèëîæåíèé âîâñå íå ÿâëÿþòñÿ ñëó÷àéíûìè. Íåñìîòðÿ íà ýòî LFSR ÷àñòî èñïîëüçóþòñÿ äëÿ ñîçäàíèÿ àëãîðèòìîâ øèôðîâàíèÿ.

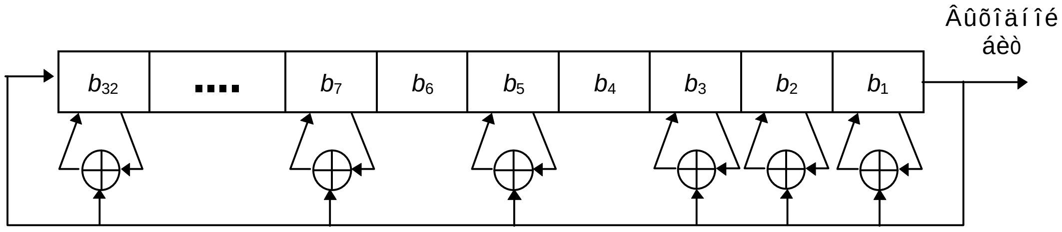
Ïðîãðàììíàÿ ðåàëèçàöèÿ LFSR

Ïðîãðàììíûå ðåàëèçàöèè LFSR ìåäëåííû è áûñòðåå ðàáîòàþò, åñëè îíè íàïèñàíû íà àññåìáëåðå, à íå íà C. Îäíàêî èç ðåøåíèé ÿâëÿþòñÿ èñïîëüçîâàíèå ïàðàëëåëüíî 16 LFSR (èëè 32, â çàâèñèìîñòè îò äëèíû ñëîâà âàøåãî êîìïüþòåðà). Â ýòîé ñõåìå èñïîëüçóåòñÿ ìàññèâ ñëîâ, ðàçìåð êîòîðîãî ðàâåí äëèíå LFSR, à êàæäûé áèò ñëîâà ìàññèâà îòíîñèòñÿ ê ñâîåìó LFSR. Ïðè óñëîâèè, ÷òî èñïîëüçóþòñÿ îäèíàêîâûå ìíîãî÷ëåíû îáðàòíîé ñâÿçè, ýòî ìîæåò äàòü çàìåòíûé âûèãðûø ïðîèçâîäèòåëüíîñòè. Âîîáùå, ëó÷øèì ñïîñîáîì îáîéòèñü ðåãèñòðû ÿâëÿþòñÿ ñòàíäàðòíûì ïðèåìîì [901].

Ñõåìó îáðàòíîé ñâÿçè LFSR ìîæíî ìîäèôèöèðîâàòü. Ïîëó÷àþùèéñÿ äâîè÷íûé áóäåò êðèòîãðàôè÷åñêè áîëåå íàäåæíûì, íî îí âñå åùå áóäåò îáëàäàòü ìàêñèìàëüíûì ïåðèîäîì [1272]. Âìåñòî èñïîëüçîâàíèÿ äëÿ ãåíåðàöèè íîâîãî êðàéíåãî ëåâîãî áèòà áèòîâ îòâîäèòå ïîñëåäîâàòåëüíîñòè ìíîãî÷ëåíà îáðàòíîé âûïîëíÿþòñÿ XOR êàæäîãî áèòà îòâîäíîé ïîñëåäîâàòåëüíîñòè ñ âûõîäîì ãåíåðàòîðà è çàìåíà åãî ðåçóëüòàòîì ýòîãî äåéñòâèÿ, çàòåì ðåçóëüòàò ãåíåðàòîðà ñòàíîâèòñÿ íîâûì êðàéíèì ëåâûì áèòîì (ñì. 11th). Èíîãäà ýòó ìîäèôèêàöèþ íàçûâàþò **êîíôèãóðàöèåé Ãàëóà**. Íà ÿçûêå C ýòî âûãëÿäèò ñëåäóþùèì îáðàçîì:

```
#define mask 0x80000057

static unsigned long ShiftRegister=1;
void seed_LFSR (unsigned long seed)
{
     if (seed == 0) /* âî èçáåæàíèå áåäû */
            seed = 1 ;
     ShiftRegister = seed;
}

int modified_LFSR (void)
```

```
{
      if (ShiftRegister & 0x00000001) {
            ShiftRegister = (ShiftRegister ^ mask >> 1) | 0x8000000 ;
      return 1;
      } else {
            ShiftRegister >>= 1;
            return 0;
      }
}
```



Ðèñ. 16-5. LFSR Ãàëóà.

Âûèãðûø ñîñòîèò â òîì, ÷òî âñå XOR ìîæíî ñäåëàòü çà îäíó îïåðàöèþ. Ýòà ñõåìà òàêæå ìîæåò áûò ðàñïàðàëëåëåíà, à ïîëèíîìû ðàçëè÷íûõ îáðàòíûõ ñâÿçåé ìîãóò áûòü ðàçëè÷íû. Òàêàÿ êîíôèãóðàöèÿ Ãàëóà ìîæåò äàòü âûèãðûø è ïðè àïïàðàòíîé ðåàëèçàöèè, îñîáåííî â âèäå ÑÁÈÑ. Âîîáùå, ïðè èñïîëüçîâàíèè àïïàðàòóðû, êîòîðàÿ õîðîøî âûïîëíÿåò ñäâèãè ïðèìåíÿéòå êîíôèãóðàöèþ Ôèáîíà÷è, åñëè åñòü âîçìîæíîñòü èñïîëüçîâàòü ïàðàëëåëèçì, ïðèìåíÿéòå êîíôèãóðàöèþ Ãàëóà.

16.3 Ïðîåêòèðîâàíèå è àíàëèç ïîòîêîâûõ øèôðîâ

Áîëüøèíñòâî ðåàëüíûõ ïîòîêîâûõ øèôðîâ îñíîâàíû íà LFSR. Äàæå â ïåðâûå äíè ýëåêòðîíèêè ïîñòðîèòü èõ áûëî íåñëîæíî. Ñäâèãîâûé ðåãèñòð íå ïðåäñòàâëÿåò èç ñåáÿ íè÷åãî áîëüøåãî, ÷åì ìàññèâ áèòîâ, à ïîñëåäîâàòåëüíîñòü îáðàòíîé ñâÿçè - íàáîð âåíòèëåé XOR. Äàæå ïðè èñïîëüçîâàíèè ÑÁÈÑ ïîòîêîâûé øèôð íà áàçå LFSR îáåñïå÷èâàåò íåìàëóþ áåçîïàñíîñòü ñ ïîìîùüþ íåñêîëüêèõ ëîãè÷åñêèõ âåíòèëåé.

Ïðîáëåìà LFSR ñîñòîèò â òîì, ÷òî èõ ïðîãðàììíàÿ ðåàëèçàöèÿ î÷åíü íåýôôåêòèâíà. Âàì ïðèõîäèòñÿ èçáåãàòü ðàçðåæåííûõ ìíîãî÷ëåíîâ îáðàòíîé ñâÿçè - îíè îáëåã÷àþò êîððåëÿöèîííûå âñêðûòèÿ [1051, 1090, 350] - à ïëîòíûå ìíîãî÷ëåíû îáðàòíîé ñâÿçè íåýôôåêòèâíû. Âûõîä ëþáîãî ïîòîêîâîãî øèôðà ÿâëÿåòñÿ ïîáèòîâûì, äëÿ øèôðîâàíèÿ òîãî, ÷òî ìîæíî âûïîëíèòü çà îäíó èòåðàöèþ DES, íåîáõîäèìî âûïîëíèòü 64 èòåðàöèè ïîòîêîâîãî àëãîðèòìà. Äåéñòâèòåëüíî, ïðîãðàììíàÿ ðåàëèçàöèÿ ïðîñòîãî àëãîðèòìà LFSR, ïîäîáíîãî îïèñûâàåìîìó íèæå ñæèìàþùåìó ãåíåðàòîðó, íå áûñòðåå, ÷åì DES.

Ýòà îòðàñëü êðèïòîãðàôèè áûñòðî ðàçâèâàåòñÿ è very politically charged. Áîëüøèíñòâî ðàçðàáîòîê çàñåêðå÷åíû - ìíîæåñòâî èñïîëüçóåìûõ ñåãîäíÿ âîåííûõ ñèñòåì øèôðîâàíèÿ îñíîâàíû íà LFSR. Äåéñòâèòåëüíî, ó áîëüøèíñòâà êîìïüþòåðîâ Cray (Cray 1, Cray X-MP, Cray Y-MP) åñòü âåñüìà ëþáîïûòíàÿ èíñòðóêöèÿ, îáû÷íî íàçûâàåìàÿ êàê "ñ÷åò÷èê ñîâîêóïíîñòè" (population count). Îíà ïîäñ÷èòûâàåò êîëè÷åñòâî åäèíèö â ðåãèñòðå è ìîæåò áûòü èñïîëüçîâàíà êàê äëÿ ýôôåêòèâíîãî âû÷èñëåíèÿ ðàññòîÿíèÿ Õýììèíãà ìåæäó äâóìÿ äâîè÷íûìè ñëîâàìè è äëÿ ðåàëèçàöèè âåêòîðèçèðîâàííîé âåðñèè LFSR. ß ñëûøàë, ÷òî ýòà èíñòðóêöèÿ ñ÷èòàåòñÿ êàíîíè÷åñêîé èíñòðóêöèåé NSA, îáÿçàòåëüíî ôèãóðèðóþùåé ïî÷òè âî âñåõ êîíòðàêòàõ, êàñàþùèõñÿ êîìïüþòåðîâ.

Ñ äðóãîé ñòîðîíû áûëî âçëîìàíî óäèâèòåëüíî áîëüøîå ÷èñëî êàçàâøèõñÿ ñëîæíûìè ãåíåðàòîðîâ íà áàçå ñäâèãîâûõ ðåãèñòðîâ. È, êîíå÷íî æå, ÷èñëî òàêèõ ãåíåðàòîðîâ, âçëîìàííûõ âîåííûìè êðèïòîàíàëèòè÷åñêèìè ó÷ðåæäåíèÿìè, òàêèìè êàê NSA, åùå áîëüøå. Èíîãäà óäèâëÿåøüñÿ òîìó, ÷òî ñàìûå ïðîñòûå èç íèõ ïðåäëàãàþòñÿ ñíîâà è ñíîâà.

Ëèíåéíàÿ ñëîæíîñòü

Àíàëèçèðîâàòü ïîòîêîâûå øèôðû ÷àñòî ïðîùå, ÷åì áëî÷íûå. Íàïðèìåð, âàæíûì ïàðàìåòðîì, èñïîëüçóåìûì äëÿ àíàëèçà ãåíåðàòîðîâ íà áàçå LFSR, ÿâëÿåòñÿ **ëèíåéíàÿ ñëîæíîñòü** (linear complexity), èëè ëèíåéíûé èíòåðâàë. Îíà îïðåäåëÿåòñÿ êàê äëèíà n ñàìîãî êîðîòêîãî LFSR, êîòîðûé ìîæåò èìèòèðîâàòü âûõîä ãåíåðàòîðà. Ëþáàÿ ïîñëåäîâàòåëüíîñòü, ãåíåðèðîâàííàÿ êîíå÷íûì àâòîìàòîì íàä êîíå÷íûì ïîëåì, èìååò êîíå÷íóþ ëèíåéíóþ ñëîæíîñòü [1006]. Ëèíåéíàÿ ñëîæíîñòü âàæíà, ïîòîìó ÷òî ñ ïîìîùüþ ïðîñòîãî àëãîðèòìà, íàçûâàåìîãî **àëãîðèòìîì Berlekamp-Massey**, ìîæíî îïðåäåëèòü ýòîò LFSR, ïðîâåðèâ òîëüêî $2n$ áèòîâ ïîòîêà êëþ÷åé [1005]. Âîññîçäàâàÿ íóæíûé LFSR, âû âçëàìûâàåòå ïîòîêîâûé øèôð.

Ýòà èäåÿ ìîæíî ðàñøèðèòü ñ ïîëåé íà êîëüöà [1298] è íà ñëó÷àè, êîãäà âûõîäíàÿ ïîñëåäîâàòåëüíîñòü ðàññìàòðèâàåòñÿ êàê ÷èñëà â ïîëå íå÷åòíîé õàðàêòåðèñòèêè [842]. Äàëüíåéøåå ðàñøèðåíèå ïðèâîäèò ê ââîäó ïîíÿòèÿ ïðîôèëÿ ëèíåéíîé ñëîæíîñòè, êîòîðûé îïðåäåëÿåò ëèíåéíóþ ñëîæíîñòü ïîñëåäîâàòåëüíîñòè ïî ìåðå åå óäëèíåíèÿ [1357, 1168, 411, 1582]. Äðóãîé àëãîðèòì âû÷èñëåíèÿ ëèíåéíîé ñëîæíîñòè ïðîñò òîëüêî â î÷åíü ñïå-

öèôè÷åñêèõ óñëîâèÿõ [597, 595, 596, 1333]. Îáîáùåíèå ïîíÿòèÿ ëèíåéíîé ñëîæíîñòè âû÷ëåíèé â [776]. Ñóùåñòâóþ òàêæå ïîíÿòèÿ ñòåïåíè è êâàäðàòè÷íîé ñëîæíîñòè [844].

Â ëþáîì ñëó÷àå ïîìíèòå, ÷òî âûñîêàÿ ëèíåéíàÿ ñëîæíîñòü íå îáÿçàòåëüíî ãàðàíòèðóåò áåçîïàñíîñòü ãåíåðàòîðà, íî íèçêàÿ ëèíåéíàÿ ñëîæíîñòü óêàçûâàåò íà íåäîñòàòî÷íóþ áåçîïàñíîñòü ãåíåðàòîðà [1357, 12.49].

Êîððåëÿöèîííàÿ íåçàâèñèìîñòü

Êðèïòîãðàôû ïûòàþòñÿ ïîëó÷èòü âûñîêóþ ëèíåéíóþ ñëîæíîñòü, íåëèíåéíî îáúåäèíÿÿ ðåçóëüòàòû íåêîòîðûõ âûõîäíûõ ïîñëåäîâàòåëüíîñòåé. Ïðè ýòîì îïàñíîñòü ñîñòîèò â òîì, ÷òî îäíà èëè íåñêîëüêî âûõîäíûõ ïîñëåäîâàòåëüíîñòåé - ÷àñòî ïðîñòî âûõîäû îòäåëüíûõ LFSR - ìîãóò áûòü ñâÿçàíû îáùèì êëþ÷åâûì ïîòîêîì è âñêðûòû ïðè ïîìîùè ëèíåéíîé àëãåáðû. ×àñòî òàêîå âñêðûòèå íàçûâàþò **êîððåëÿöèîííûì âñêðûòèåì** èëè âñêðûòèåì ðàçäåëÿé-è-âëàñòâóé. Òîìàñ Ñèãåíòàëåð (Thomas Siegenthaler) ïîêàçàë, ÷òî ìîæíî òî÷íî îïðåäåëèòü **êîððåëÿöèîííóþ íåçàâèñèìîñòü**, è ÷òî ñóùåñòâóåò êîìïðîìèññ ìåæäó êîððåëÿöèîííîé íåçàâèñèìîñòüþ è ëèíåéíîé ñëîæíîñòüþ [1450].

Îñíîâíîé èäåé êîððåëÿöèîííîãî âñêðûòèÿ ÿâëÿåòñÿ íáîðóæäíèå íåêîòîðîé êîððåëÿöèè ìåæäó âûõîäîì ãåíåðàòîðà è âûõîäîì îäíîé èç åãî ñîñòàâíûõ ÷àñòåé. Òîãäà, íàëþäàÿ âûõîäíóþ ïîñëåäîâàòåëüíîñòü, ìîæíî ïîëó÷èòü èíôîðìàöèþ îá yòîì ïðîìåæóòî÷íîì âûõîäå. Èñïîëüçóÿ yòó èíôîðìàöèþ è äðóãèå êîððåëÿöèè, ìîæíî ñíáèðàòü äàííûå î äðóãèõ ïðîìåæóòî÷íûõ âûõîäàõ äî òåõ ïîð, ïîêà äåíðàòîð íå áóäåò âçëîìàí.

Ïðîòèâ ìíîãèõ ãåíåðàòîðîâ ïîòîêîâ êëþ÷åé íà áàçå LFSR óñïåøíî èñïîëüçîâàëèñü êîððåëÿöèîííûå âñêðûòèÿ è èõ âàðèàöèè, òàêèå êàê áûñòðûå êîððåëÿöèîííûå âñêðûòèÿ, ïðåäëàãàþùèå êîìïðîìèññ ìåæäó âû÷èñëèòåëüíîé ñëîæíîñòüþ è ýôôåêòèâíîñòüþ [1451, 278, 1452, 572, 1636, 1051, 1090, 350, 633, 1054, 1089, 995]. Ðÿä èíòåðåñíûõ íîâûõ èäåé â yòîé îáëàñòè ìîæíî íàéòè â [46, 1641].

Äðóãèå âñêðûòèÿ

Ñóùåñòâóþò è äðóãèå ñïîñîáû âñêðûòèÿ ãåíåðàòîðîâ ïîòîêîâ êëþ÷åé. Òåñò íà **ëèíåéíóþ êîððåëèíîñòü** (linear consistency) ïûòàåòñÿ íàéòè íåêîòîðûå ïîäìíîæåñòâî êëþ÷à øèôðîâàíèÿ ñ ïîìîùüþ ìàòðè÷íîé òåõíèêè [1638]. Ñóùåñòâóåò è **âñêðûòèå êîððåëèíîñòè "âſòðå÷åé ïîñðåäèíå"** (meet-in-the-middle consistency attack) [39, 41]. **Àëãîðèòì ëèíåéíîãî ñèíäðîìà** (linear syndrome algorithm) îñíîâàí íà âîçìîæíîñòè çàïèñàòü ôðàãìåíò âûõîäíîé ïîñëåäîâàòåëüíîñòè â âèäå ëèíåéíîãî óðàâíåíèÿ [1636, 1637]. Ñóùåñòâóåò **âñêðûòèå ëó÷øèì àôôèííûì ïðèáëèæåíèåì** (best afflne approximation attack) [502] è **âñêðûòèå âûâåäåííûì ïðåäſîæåíèåì** (derived sequence attack) [42]. Ê ïîòîêîâûì øèôðàì ìîæíî ïðèìåíèòü òàêæå ìåòîäû äèôôåðåíöèàëüíîãî [501] è ëèíåéíîãî [631] êðèïòîàíàëèçà.

16.4 Ï îòîêîâûå øèôðû íà áàçå LFSR

Îñíîâíîé ïîäõîä ïðè ïðîåêòèðîâàíèè ãåíåðàòîðà ïîòîêà êëþ÷åé íà áàçå LFSR ïðîñò. Ñíà÷àëà áåðåòñÿ îäèí èëè íåñêîëüêî LFSR, îáû÷íî ñ ðàçëè÷íûìè äëèíàìè è ðàçëè÷íûì ìíîãî÷ëåíàìè îáðàòíîé ñâÿçè. (Åñëè äëèíû âçàèìíî ïðîſòû, à åñå ìíîãî÷ëåíû îáðàòíîé ñâÿçè ïðèòâîíû, òî ó îáðàçîâàííîãî ãåíåðàòîðà áóäåò ìàêſèìàëüíàÿ äëèíà.) Êëþ÷ ÿâëÿåòſÿ íà÷àëüíûì ſîſòîÿíèåì ðåãiſòðîâ LFSR. Êàæäûé ðàç, êîãäà íåîáõîäèìî íîâûé áèò, ñäâèíüòå íà áèò ðåãiſòðû LFSR (ýòî èſîãäà íàçûâàþò **òàêòèðîâàíèåì** (clocking)). Áèò âûõîäà ïðåäſòàâëÿåò ſîáîé ôóíêöèþ, æåëàòåëüíî íåëèíåéíóþ, íåêîòîðûõ áèòîâ ðåãiſòðîâ LFSR. Ýòà ôóíêöèÿ íàçûâàåòſÿ **êîìáèíèðóþùåé ôóíêöèåé**, à ſåíåðàòîð â öåëîì - **êîìáèíàöèîííûì ãåíåðàòîðîì**. (Åſëè áèò âûõîäà ÿâëÿåòſÿ ôóíêöèåé åäèſòâåííîãî LFSR, òî ſãåíåðàòîð íàçûâàåòſÿ **ôèëüòðóþùèì ſãåíåðàòîðîì**.) Áîëüøàÿ ſ÷àſòü òåîðèè ïîſîáîſîãî ðîſà óſòðîéſòâ ðàçðàáîòàíà Ñåëſåðîì (Selmer) è Íèëſì Öèðëåðſì (Neal Zierler) [1647].

Ì îæíî âſâſñòè ðÿä óſëîæſåíèé. Â íåêîòîðûõ ſåíåðàòîðàõ äëÿ ðàçëè÷íûõ LFSR èſïîëüçóåòſÿ ðàçëè÷íàÿ òàêòîâàÿ ſ÷àſòîòà, èſſîãäà ſ÷àſòîòà îſïîſî ſãåíåðàòîðà çàâiſèſò îò âûõîäà äðóãſîſ. Âſå ýòî ýëåêòſîſíûå âåðſèè èſåſ øèôðſâàëüſûõ ſàøèſ, ſïÿâèâøèſſÿ äſ Âòſðîſ ſèðſâſé âſéſû, êſòſðûå íàçûâàþſſÿ ſåíåðàòſðàſſè ſ **óſðàâëåſíèåſ òàêòſâſé ſ÷àſſòſé** (clock-controlled genelators) [641]. Óſðàâëåſíèå òàêòſâſé ſ÷àſſòſé ſſåſò áûòſ ſ ſðÿſſé ſâÿçüþ, êſãäà âûſſä îſſſãſ LFSR óſðàâëÿåò òàêòſâſé ſ÷àſſòſé äðóſſãſ LFSR, èſſ ſ îáðàòſſé ſâÿçüþ, êſãäà âûſſä îſſſãſ LFSR óſðàâëÿåò åſſ ſſáſòâåſſſé òàêòſâſé ſ÷àſſòſé.

Õſòÿ âſå ýòè ſåſſåðàòſðû ſ÷óſſòâèòåëüſû, ſſ êðàéſåé ſåðå òåſðåòè÷åſſêè, ê âſêðôùèÿſ âſſſæåſèåſ è âåðſÿòſſé êſððåëÿöèåé [634, 632], ſſſãèå èç ſèſ áåçſſàſſſû äſ ſèſ ſſð. Äſſſſëſèòåëüſóþ òåſðèþ ſãâèãſâûſ ðåãèſòðſâ ſ óſðàâëÿåſſé òàêòſâſé ſ÷àſſòſé ſſæſſ ſáéòè â [89].

ßſ Êàſſåëëſ (Ian Cassells), ðàſåå âſçäëàâëÿåøèé êàôåäðó ſ÷èſòé ſàòåſàòàêêè â Êåſáðèäæå è ðàſſòàâøèé êðèſòſàſàëëòàêſ â Bletchly Park, ſêàçàë, ÷òſ "êðèſòſſãðàôèÿ - yòſ ſſåſſü ſàòåſàòàêêè è ſſóòàſèöû, è áåç ſſóòàſèöû ſàòåſàòàêêà ſſæåò áûòü èſſſëüçſâàſà ſſðſòèâ âàſ." Îſ èſåë â âèäó, ÷òſ â ſſòſſêſâûõ øèôðàõ äëÿ ſáåſſſå÷åſèÿ ſàêſèſàëüſſſé äëſſû è äðóſèõ ſſâſéſòſ ſáſſáſſſäſſſſſå ſàòåſàòà÷åſêåſ ſòðóſòóðû, òàêàſ êàê LFSR, ſſ, ÷òſáû ſſſſåøàòü êſſó-òſ ſſëó÷èòü ſſſäðæàſèå ðåãſòðà è âſêðôùòü äëãſðèòſ, ſáſáſóſäſſſ ſ âſåſòè ſåêſòſðûé ſſëſæſûé ſåëſſåſſſûé áåſſſſðÿſſê. Ýòſò ſſſåò ſſſðàâåäëèâ è äëÿ áëſ÷íûõ àëãſðèòſſâ.

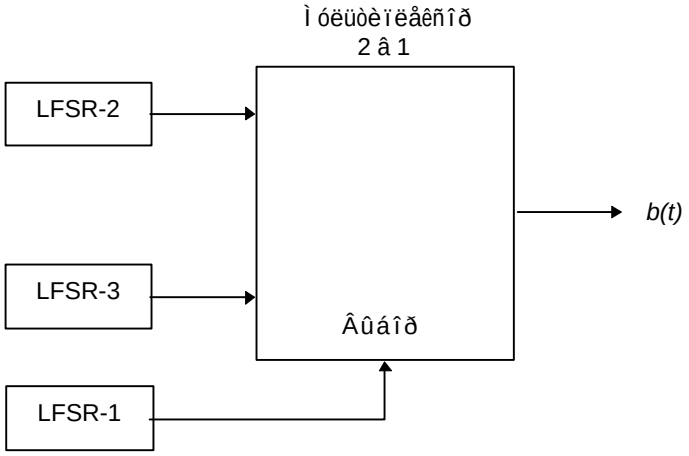
Ïîýòîìó íå ñòîèò ñðåäñòâî óâëåêàòüñÿ ãåíåðàòîðàìè ïîòîêà êëþ÷åé íà áàçå LFSR, îïèñàííûì âûøå-ëèñò â ëèòåðàòóðå. ß íå çíàþ, èñïîëüçóåòñÿ ëè õîòü îäèí èç íèõ â ðåàëüíûõ êðèïòîãðàôè÷åñêèõ ïðîäóêòàõ. Áîëüøåé ÷àñòüþ îíè ïðåäñòàâëÿò ëèøü òåîðåòè÷åñêèé èíòåðåñ. Íåêîòîðûå áûëè âçëîìàíû, íåêîòîðûå ìîãëè îñòàòüñÿ áåçîïàñíûìè.

Òàê êàê øèôðû íà áàçå LFSR îáû÷íî ðåàëèçóþòñÿ àïïàðàòíî, íà ðèñóíêàõ èñïîëüçóþòñÿ ñèìâîëû ýëåêòðîííîé ëîãèêè. Â òåêſòå, ⊕ îçíà÷àåò XOR, ∧ - AND, ∨ - OR, è ¬ - NOT.

Ãåíåðàòîð Ãåôôà

Â ýòîì ãåíåðàòîðå ïîòîêà êëþ÷åé èſïîëüçóþòſ òðè LFSR, îáúåäèíåííûå íåëèíåéíûì îáðàçîì (ſì. 10th) [606]. Äâà LFSR ÿâëÿþſſ âõîäàìè ìóëüòèïëåêſîðà, à òðåòèé LFSR óïðàâëÿåò âûõîäîì ìóëüòèïëåêſîðà. Åſſè a_1, a_2 è a_3 - âûõîäû òðåõ LFSR, âûõîä ãåíåðàòîðà Ãåôôà (Geffe) ìſæíſ îïèſàòü êàê:

$b = (a_1 \wedge a_2) \oplus((\neg a_1) \wedge a_3)$



Ðèſ. 16-6. Ãåíåðàòîð Ãåôôà.

Åſſè äëèſû LFSR ðàâſû n_1, n_2 è n_3, ſîſòâåòſòâåſſî, òî ëèſåſàÿ ſëſæſſîſòü ãåíåðàòîðà ðàâſà

$(n_1 + 1)\, n_2 + n_1 n_3$,

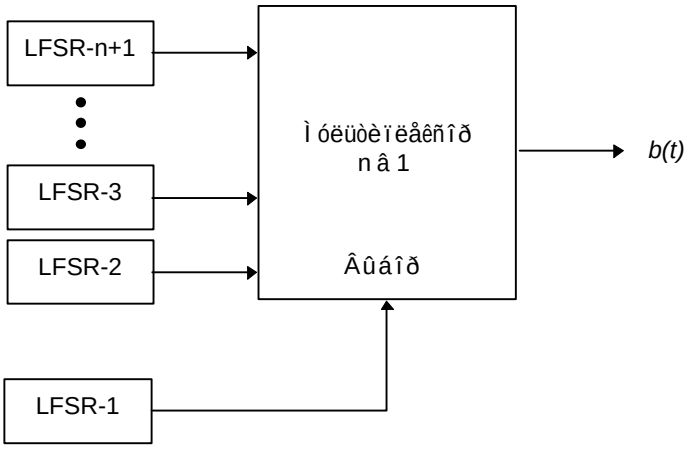
Ïåðèſä ãåíåðàòîðà ðàâſåſ íàèſåſüøåſó îáſùſó äåëèòåëþ ïåðèſäſâ òðåſ ãåíåðàòîðſâ. Ïðè óſëſâèè, ÷òſ ſòåſſåſ òðåſ ſðèſèòèâſûſ ſſſãſ÷ëſſâ îáðàòſſé ſâÿçè âçàèſſ ſðſſòû, ſåðèſä ýòſãſ ãåíåðàòſðà áóäåò ðàâſſ ſðſèçâääſåſèþ ſåðèſäſâ òðåſ LFSR.

Õſòÿ ýòſ ãåíåðàòſð íåſëſſſſ âûãëÿäèò íà áóſàåå, ſſ êðèſſſãðàôſ÷åſſêè ſſàá è íå ſſæåò óſſòſÿòü ſðſſòêâ êſðåëÿöſſſſſãſ âſſſèſſ [829, 1638]. Â 75 ſðſſöåſſòàſ âðåſſåſſ âûſſâ ãåíåðàòſðà ðàâſſ âûſſâóſ LFSR-2. Ï ſýòſſó, åſſè èçâåſòſû ſòâſſäſûå ſſſſëäſſâàòåëſſſſòſ îáðàòſſé ſâÿçè, ſſæſſ äſãàäàòüſÿ ſ íà÷àëſſſ ſíà÷åſſè LFSR-2 è ſãåſåðèſſâàòſ âûſſäſóſ ſſſſëäſſâàòåëſſſſòſ ýòſãſ ðåãèſòðà. Òſãää ſſæſſ ſſäſ÷èòàòſ, ſêſëſüêſ ðàç âûſſä LFSR ſſâſäää㠟 âûſſäſſ ſåſåðàòſðà. Åſſè íà÷àëſſſå çſà÷åſèå ſſðåää㠟åſſ íåðſſ, ää㠟ſſëää㠟âàòåëſſſſòſ áóäóò ſſãëàſſâûâàòſÿ â 50 ſðſöåſſòàſ âðåſſåſè, à åſſè ſðàâèſſſſ, òſ â 75 ſðſöåſſòàſ âðſſåſè.

Àſſëſãè÷ſſ, âûſſä ãåſåðàòſðà ðàâſſ âûſſäó LFSR â 75 ſðſöåſſòàſ âðſſåſè. Ñ òàêſſè êſððåſÿöſÿſ ſåſåðàòſðſ ſſòſêſ êëþ÷åſ ſſæåò áûòü ſåãêſ âçſſſàſ. Íàſðſſåð, åſſè ſðſſèòſâſûå ſſſãſ÷ſåſû ſſſòſÿò òſſüêſ èç òðãſ ſſåſſâ, è äſèſſà ſàſſãſ áſèüſſſ LFSR ðàâſà *n*, äſÿ âſſſòàſſâſåſÿ âſóòðåſſſòſ ſſſòſÿſéſ âſåſ òðãſ LFSR ſóæåſ ôðàſſåſò âûſſäſſſ ſſſëäſſâàòåëſſſſòſ äſèſſſ 37*n* áèòſâ [1639].

Îáſùåſſûé ãåſåðàòſð Ãåôôà

Âſſåſòſ âûáſſðà ſåæäó äâſſÿ LFSR â ýòſé ſſåſſ âûáèðàåſſÿ ſäèſ èç *k* LFSR, ãää *k* ÿâëÿåſſÿ ſòàſſåſüþ 2. Âſſåſâſ èſſſſëüſóſòÿ *k* + 1 LFSR (ſì. 9th). Òàêſſâàÿ ſàſòſòà LFSR-l äſëæſà áûòü â $\log_2 k$ ðàç âûøå, ſåſ ó ſſòàëüſûſ *k* LFSR.

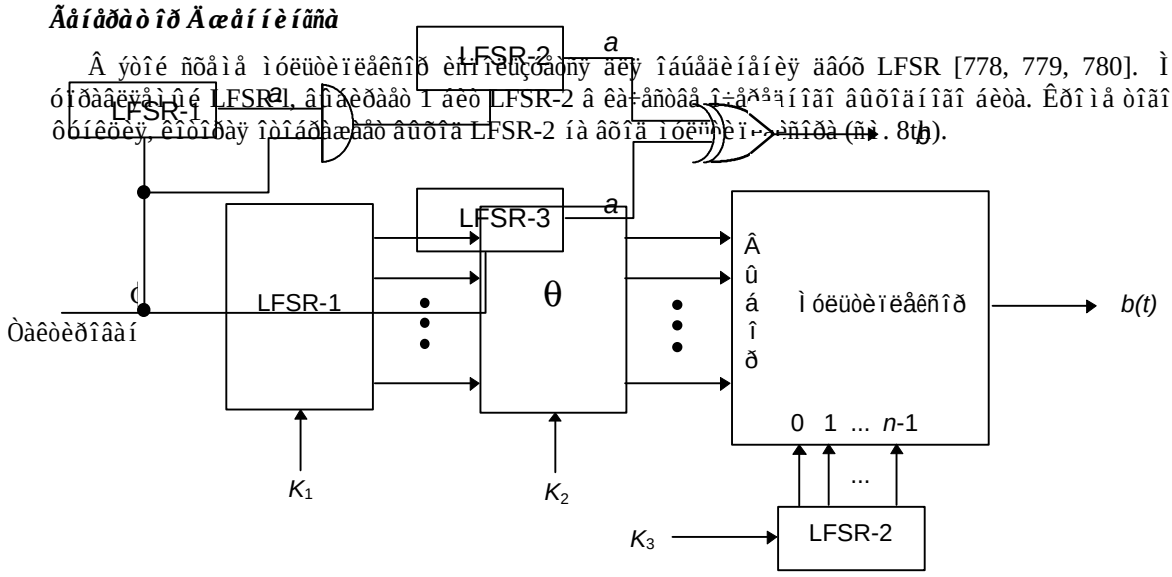


Ðèñ. 16-7. Îáîáùåííûé ãåíåðàòîð Åâîâà.

Íåñìîòðÿ íà òî, ÷òî ýòà ñõåìà ñëîæíåå ãåíåðàòîðà Åâîâà, äëÿ âçëîìà ìîæíî èñïîëüçîâàòü òî æå êîððåëÿöèîííîå âñêðûòèå. Íå ðåêîìåíäóþ ýòîò ãåíåðàòîð.

Ãåíåðàòîð Äæåííèíãñà

Â ýòîé ñõåìå ìóëüòèïëåêñîð èñïîëüçóåòñÿ äëÿ îáúåäèíåíèÿ äâóõ LFSR [778, 779, 780]. Ìóëüòèïëåêñîð, óïðàâëÿåìûé LFSR-1, âûáèðàåò 1 áèò LFSR-2 â êàæäîå îïåðàöèîííîå âûõîäíîãî áèòà. Êðîìå òîãî, èñïîëüçóþòñÿ ôóíêöèè, êîòîðûå îòáðàñûâàþò âûõîä LFSR-2 íà âõîä óìíîæèòåëÿ (ñì. 8th).

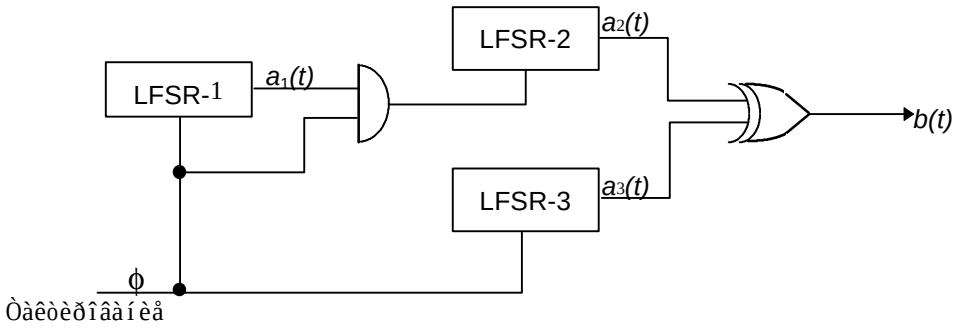


Ðèñ. 16-8. Ãåíåðàòîð Äæåííèíãñà.

Êëþ÷îì ÿâëÿåòñÿ íà÷àëüíîå ñîñòîÿíèå äâóõ LFSR è ôóíêöèè ïîäàæåíèÿ. Õîòÿ ó ýòîãî ãåíåðàòîðà çàì÷àòåëüíûå ñòàòèñòè÷åñêèå ñâîéñòâà, îí ïàë ïåðâîé æåðòâîé íåóäà÷íîé Ðîññîì Àíäåðñîíîì (Ross Anderson) âñêðûòèåì êðèïòîñèñòåìû âòîðîé ïîëîâèíû [39] è âñêðûòèåì ëèíåéíîé êðèïòîñèñòåìû [1638,442]. Íå èñïîëüçóéòå ýòîò ãåíåðàòîð.

Ãåíåðàòîð "ñòîï-ïîøåë" (Stop-and-Go) Both-Piper

Ýòîò ãåíåðàòîð, ïîêàçàííûé íà 7th, èñïîëüçóåò âûõîä îäíîãî LFSR äëÿ óïðàâëåíèÿ òàêòîâîé ÷àñòîòîé äðóãîãî LFSR [151]. Òàêòîâûé âõîä LFSR-2 óïðàâëÿåòñÿ âûõîäîì LFSR-l, òàê ÷òî LFSR-2 ìîæåò èçìåíÿòü ñâîå ñîñòîÿíèå â ìîìåíò âðåìåíè *t* òîëüêî, åñëè âûõîä LFSR-l â ìîìåíò âðåìåíè *t* - 1 áûë ðàâåí 1.

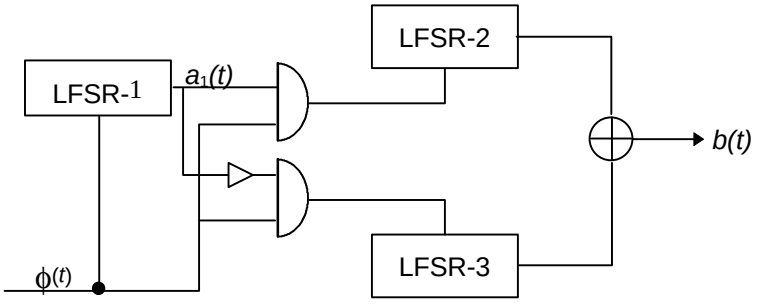


Ðèñ. 16-9. Ãåíåðàòîð "ñòîï-ïîøåë" Beth-Piper.

Íèêîìó íå óäàëîñü ïðèâåñòè äëÿ îáùåãî ñëó÷àÿ äîñòàòî÷íî ïðîñòîãî è ëåãêîíåé ñëîæíîñòè ýòîãî ãåíåðàòîðà. Îäíàêî íî íåóñòîÿë ïðåä êðóïíûìè âñêðûòèåì [1639].

×åðåäóþùèéñÿ ãåíåðàòîð "ñòîï-ïîøåë"

Â ýòîì ãåíåðàòîðå èñïîëüçóþòñÿ òðè LFSR ðàçëè÷íîé äëèíû. LFSR-2 òàêòèðóåòñÿ, êîãäà âûõîä LFSR-l ðàâåí 1, LFSR-3 òàêòèðóåòñÿ, êîãäà âûõîä LFSR-l ðàâåí 0. Âûõîäîì ãåíåðàòîðà ÿâëÿåòñÿ XOR LFSR-2 è LFSR-3 (ñì. Ðèñ. 16.10) [673].

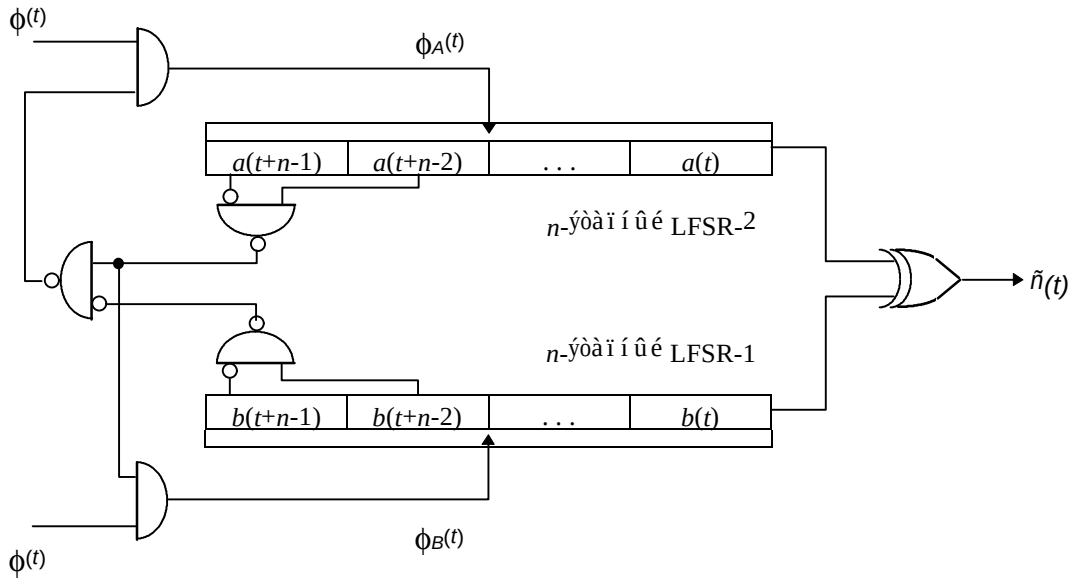


Ðèñ. 16-10. ×åðåäóþùèéñÿ ãåíåðàòîð "ñòîï-ïîøåë"

Ó ýòîãî ãåíåðàòîðà áîëüøîé ïåðèîä è áîëüøàÿ ëèíåéíàÿ ñëîæíîñòü. Àâòîðû ïîêàçàëè ñïîñîá êîððåëÿöèîííîãî âñêðûòèÿ LFSR-1, íî ýòî íå ñëèøêîì îñëàáëÿåò ãåíåðàòîð. Áûëè ïðåäëîæåíû è äðóãèå ãåíåðàòîðû òàêîãî òèïà [1534, 1574, 1477].

Äâóñòîðîííèé ãåíåðàòîð "ñòîï-ïîøåë"

Â ýòîì ãåíåðàòîðå èñïîëüçóåòñÿ äâà LFSR ñ îäèíàêîâîé äëèíîé *n* (ñì. Ðèñ. 16.11) [1638]. Âûõîäîì ãåíåðàòîðà ÿâëÿåòñÿ XOR âûõîäîâ êàæäîãî LFSR. Åñëè âûõîä LFSR-l â ìîìåíò âðåìåíè *t*-1 ðàâåí 0, à â ìîìåíò âðåìåíè *t*-2 - 1, òî LFSR-2 íå òàêòèðóåòñÿ â ìîìåíò âðåìåíè *t*. Íàîáîðîò, åñëè âûõîä LFSR-2 â ìîìåíò âðåìåíè *t*-1 ðàâåí 0, à â ìîìåíò âðåìåíè *t*-2 - 1, è åñëè LFSR-2 òàêòèðóåòñÿ â ìîìåíò âðåìåíè *t*, òî LFSR-l íå òàêòèðóåòñÿ â ìîìåíò âðåìåíè *t*.



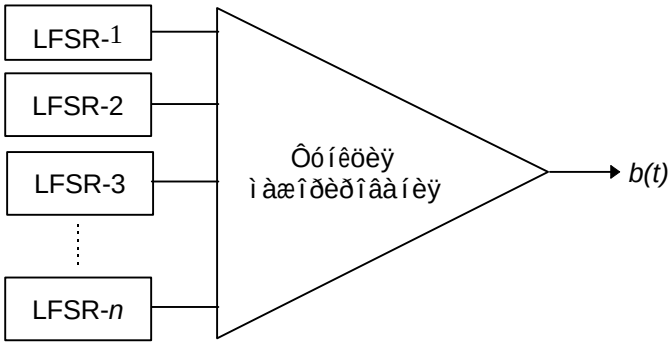
Ðèñ. 16-11. Äâóñòîðîííèé ãåíåðàòîð "ñòîï-ïîøåë".

Ëèíåéíàÿ ñëîæíîñòü òàêîé ñèñòåìû ïðèìåðíî ðàâíà ïðèìåíèòåëüíî [1638], "â òàêîé ñèñòåìå íå îò-âëè÷èìà èçáûòî÷íîñòü êëþ÷à íàéäåòñÿ".

Ïîðîãîâûé ãåíåðàòîð

Ýòîò ãåíåðàòîð ïûòàåòñÿ îáîéòè ïðîáëåìû áåçîïàñíîñòè, ðàðàêòåðíûå äëÿ ïðåäûäóùèõ ãåíåðàòîðîâ, ñ ïîìîùüþ ïåðåìåííîãî ÷èñëà LFSR [277]. Ï î òåîðèè ïðè èñïîëüçîâàíèè áîëüøîãî êîë÷åñòâà LFSR âñêðûòü øèôð ñëîæíåå.

Ýòîò ãåíåðàòîð ïîêàçàí íà 4-é. Âîçüìèòå âûõîä áîëüøîãî ÷èñëà LFSR (èñïîëüçóÿ íå÷åòíîå ÷èñëî ðåãèñòðîâ, ñ ïîìîùüþ ïåðåìåííîãî ïåðèîäà óäâàèâàåòñÿ, ÷òî äëèíû âñåõ LFSR âçàèìíî ïðîñòû, à ìíîãî÷ëåíû îáðàòíîé ñâÿçè - ïðèìèòèâíû.. Åñëè áîëüøå ïîëîâèíû âûõîäíûõ áèòîâ LFSR - 1, òî âûõîäíîì ãåíåðàòîðà ÿâëÿåòñÿ 1. Åñëè áîëüøå ïîëîâèíû âûõîäíûõ áèòîâ LFSR - 0, òî âûõîäíîì ãåíåðàòîðà ÿâëÿåòñÿ 0.



Ðèñ. 16-12. Ï ðîãîâûé ãåíåðàòîð.

Äëÿ òðåõ LFSR âûõîä ãåíåðàòîðà ìîæíî ïðåäñòàâèòü êàê:

$b = (a_1 \wedge a_2) \oplus (a_1 \wedge a_3) \oplus (a_2 \wedge a_3)$

Ýòî î÷åíü ïîõîæå íà ãåíåðàòîð Åâôà çà èñêëþ÷åíèå òîãî, ÷òî ïîðîãîâûé ãåíåðàòîð îáëàäàåò áîëüøåé ëèíåéíîé ñëîæíîñòüþ

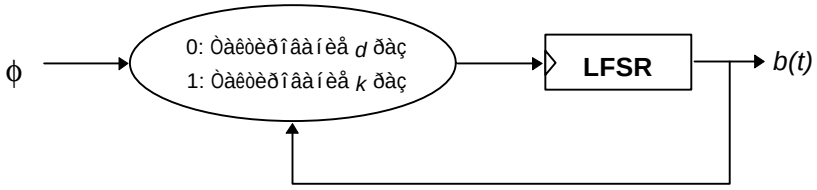
$n_1n_2 + n_1n_3 + n_2n_3$

ãäå n_1, n_2 è n_3 - äëèíû ïåðâîãî, âòîðîãî è òðåòüåãî LFSR.

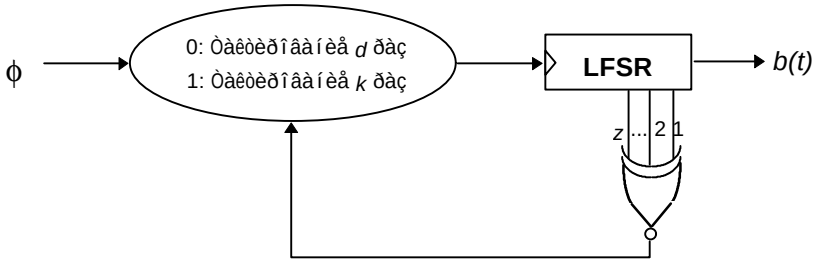
Ýòîò ãåíåðàòîð íå ñëèøêîì õîðîø. Êàæäûé âûõîäíîé áèò äàåò íåêîòîðóþ èíôîðìàöèþ î ñîñòîÿíèè LFSR - òî÷íåå 0.189 áèòà - è ãåíåðàòîð â öåëîì íå ìîæåò óñòîÿòü ïåðåä êîððåëÿöèîííûì âñêðûòèåì. ß íå ñîâåòóþ èñïîëüçîâàòü òàêîé ãåíåðàòîð.

Ñàìîïðîðåæèâàþùèå (Self-Decimated) ãåíåðàòîðû

Ñàìîïðîðåæèâàþùèì íàçûâàþòñÿ ãåíåðàòîðû, êîòîðûå óïðàâëÿþò ñîáñòâåííîé òàêòîâîé ÷àñòîòîé. Áûëî ïðåäëîæåíî äâà òèïà òàêèõ ãåíåðàòîðîâ, îäèí Ðýíäåëëîì Ðþïïåëëîì (Ranier Rueppel) (ñì. 3-é) [1359] äðóãîé Áèëëîì ×àìáåðñîì (Bill Chambers) è Äèòðåðîì Êîëëìàíîì (Dieter Collmann) [308] (ñì. 2nd). Â ãåíåðàòîðå Ðþ-ïåëà åñëè âûõîä LFSR ðàâåí 0, LFSR òàêòèðóåòñÿ *d* ðàç. Åñëè âûõîä LFSR ðàâåí 0, LFSR òàêòèðóåòñÿ *k* ðàç. Åå-íåðàòîð ×àìáåðñà è Êîëëìàíà ñëîæíåå, íî èäåÿ îñòàåòñÿ òîé æå. Ê ñîæàëåíèþ îáà ãåíåðàòîðà íå áåçîïàñíû [1639], õîòÿ áûë ïðåäëîæåí ðÿä ìîäèôèêàöèé, êîòîðûå ìîãóò èñïðàâèòü âñòðå÷àþùèåñÿ ïðîáëåìû [1362.].



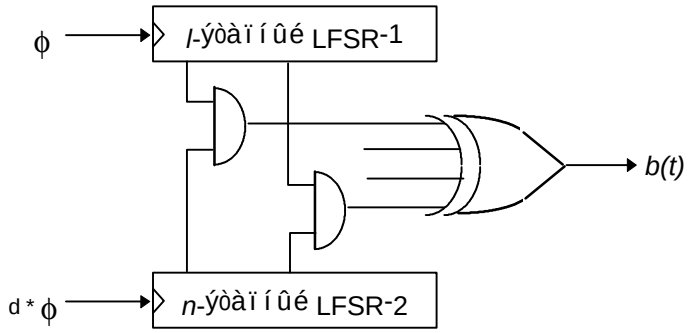
Ðèñ. 16-13. Ñàìîïðîðåæèâàþùèé ãåíåðàòîð Ðþïïåëà.



Ðèñ. 16-14. Ñàìîïðîðåæèâàþùèé ãåíåðàòîð ×àìáåðñà è Ãîëëàíà.

Èíâîëþòíûé ãåíåðàòîð ñ âíóòðåííèì ïðîèçâåäåíèåì (inner-product)

Ýòîò ãåíåðàòîð, ïðåäëîæåííûé Ìàññåì (Massey) è Ðþïïåëîì [1014], èñïîëüçóåò äâà LFSR ñ ðàçíûìè òàê-òîâûìè ÷àñòîòàìè (ñì. 1st). Òàêòîâàÿ ÷àñòîòà LFSR-2 â *d* ðàç áîëüøå, ÷åì ó LFSR-l. Îòäåëüíûå áèòû ýòèõ LFSR îáúåäèíÿþòñÿ îïåðàöèåé AND, à çàòåì äëÿ ïîëó÷åíèÿ âûõîäíîãî áèòà ãåíåðàòîðà îíè îáúåäèíÿþòñÿ ïîñðåäñò-âîì XOR.



Ðèñ. 16-15. Èíâîëþòîðíîå ãåíåðàòîð ñ âíóòðåííèì ïðîèçâåäåíèåì.

Õîòÿ ýòîò ãåíåðàòîð îáëàäàåò âûñîêîé ëèíåéíîé ñëîæíîñòüþ è åëèêîïëåïòè÷åñêèì õàðàêòåðè-ñòèêàì, îí äîñå æå íå ìîæåò óñòîÿòü ïðåä âñêðûòèåì ëèíåéíîé ñîãëàñîâàííîñòè [1639]. Åñëè n_1 - äëèíà LFSR-l, n_2 - äëèíà LFSR-2, à *d* - îòíîøåíèå òàêòîâûõ ÷àñòîò, òî âíóòðåííåå ñîñòîÿíèå ãåíåðàòîðà ìîæåò áûòü ïîëó÷åíî ïî âûõîäíîé ïîñëåäîâàòåëüíîñòè äëèíîé

$n_2 + n_2 + \log_2 d$

Ñóì ìèðóþùèé ãåíåðàòîð

Åùå îäíî ïðåäëîæåíèå Ðýíåð Ðþïïåëà, ýòîò ãåíåðàòîð ñóì ìèðóåò âûõîäû äâóõ LFSR (ñ ïåðåíîñîì) [1358, 1357]. Ýòî â âûñîêîé ñòåïåíè íåèíåéíàÿ îïåðàöèÿ. Â êíîãå 80-õ ýòîò ãåíåðàòîð áûë ëèäåðîì â îòíîøåíèè áåçîïàñíîñòè, íî îí ïàë ïðåä êðóãëûìè âñêðûòèåì [1053, 1054, 1091]. Êðîìå òîãî, áûëî ïîêàçàíî, ÷òî ýòîò ãåíåðàòîð ÿâëÿåòñÿ ÷ñòíûì ñëó÷àåì îáðàòíîé ñâÿçè, èñïîëüçóþùåé ñäâèãîâûé ðåãèñòð ñ ïåðåíîñîì (ñì.

ðàçäåë 17.4), è ìîæåò áûòü âçëîìàí [844].

DNRSG

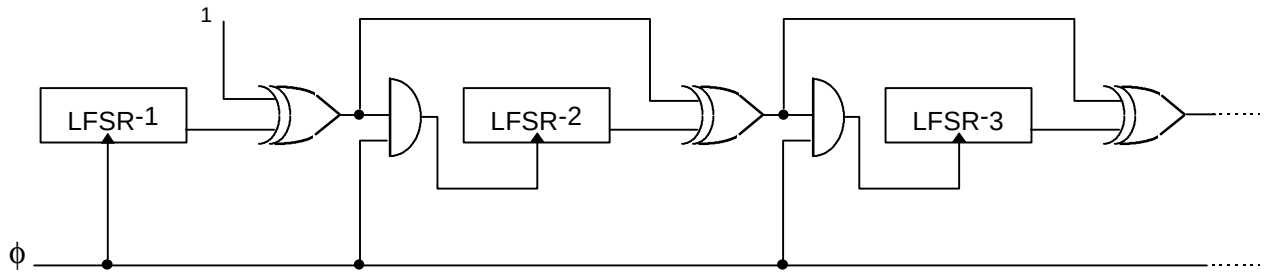
Ýòî îçíà÷àåò "äèíàìè÷åñêèé ãåíåðàòîð ñëó÷àéíîé ïîñëåäîâàòåëüíîñòè" ("dynamic random-sequence generator") [1117]. Èäåÿ ñîñòîèò â òîì, ÷òîáû âçÿòü äâà ðàçëè÷íûõ ôèëüòðóåìûõ ãåíåðàòîðà - ïîðîãîâûõ, ñóììèðóþùèõ, è ò.ï. - èñïîëüçóþùèõ îäèí íàáîð LFSR, à óïðàâëÿåìûõ äðóãèì LFSR.

Ñíà÷àëà òàêòèðóþùèé LFSR-0 ÿâëÿåòñÿ 1, òî âû÷èñëÿåòñÿ âûõîä ïåðâîãî ôèëüòðóåìîãî ãåíåðàòîðà. Åñëè âûõîäíîé LFSR-0 ÿâëÿåòñÿ 0, òî âû÷èñëÿåòñÿ âûõîä âòîðîãî ôèëüòðóåìîãî ãåíåðàòîðà. Îêîí÷àòåëüíûì ðåçóëüòàòîì ÿâëÿåòñÿ XOR âûõîäîâ ïåðâîãî è âòîðîãî ãåíåðàòîðîâ.

Êàñêàä Ãîëîìàíà

Êàñêàä Ãîëîìàíà (ñì. 0-é), îïèñàííûé â [636, 309], ïðåäñòàâëÿåò ñîáîé óñëîæíåíèå ãåíåðàòîðà "ñòîï-ïîøåë". Î í ñîñòîèò èç ïîñëåäîâàòåëüíîñòè LFSR, òàêòèðîâàíèå êàæäîãî èç êîòîðûõ óïðàâëÿåòñÿ ïðåäûäóùèì LFSR. Åñëè âûõîäíîì LFSR-l â ìîìåíò âðåìåíè *t* ÿâëÿåòñÿ 1, òî òàêòèðóåòñÿ LFSR-2. Åñëè âûõîäíîì LFSR-2 â ìîìåíò âðåìåíè *t* ÿâëÿåòñÿ 1, òî òàêòèðóåòñÿ LFSR-3, è òàê äàëåå. Âûõîä ïîñëåäíåãî LFSR è ÿâëÿåòñÿ âûõîäíîì ãåíåðàòîðà. Åñëè äëèíà âñåõ LFSR îäèíàêîâà è ðàâíà *n*, ëèíåéíàÿ ñëîæíîñòü ñèñòåìû èç *k* LFSR ðàâíà

$n(2^n - 1)^{k-1}$



Ðèñ. 16-16. Êàñêàä Ãîëîìàíà.

Ýòî äåðçêàÿ èäåÿ: êîíöåïòóàëüíî îíè î÷åíü ïðîñòû è ìîãóò áûòü èñïîëüçîâàíû äëÿ ãåíåðàöèè ïîñëåäîâàòåëüíîñòåé ñ îãðîìíûìè ïåðèîäàìè, îãðîìíûìè ëèíåéíûìè ñëîæíîñòÿìè è õîðîøèìè ñòàòèñòè÷åñêèìè ñâîéñòâàìè. Îíè ÷óâñòâèòåëüíû ê âûêðûòèþ, íàçûâàåìîìó **çàïèðàíèåì** (lock-in) [640] è ïðåäñòàâëÿþùåìó ìåòîä, ñ ïîìîùüþ êîòîðîãî ñíà÷àëà êðèïòîàíàëèòèê âîññòàíàâëèâàåò âõîä ïîñëåäíåãî ñäâèãîâîãî ðåãèñòðà â êàñêàäå, à çàòåì âçëàìûâàåò åãî ñòàðøèé ðàçðÿä ðåãèñòðîì. Â íåêîòîðûõ ñëó÷àÿõ ýòî ïðåäñòàâëÿåò ñîáîé ñðàâíèòåëüíî ïðîñòóþ ïðîáëåìó è òåõíîëîãè÷åñêóþ äëèíó êëþ÷à äëÿ îïðåäåëåíèÿ îïðåäåëåííûõ ìåð.

Äàëüíåéøèé àíàëèç ïîêàçàë, ÷òî ñ ðîñòîì *k* ïîñëåäîâàòåëüíîñòü ïðèáëèæàåòñÿ ê ñëó÷àéíîé [637, 638, 642, 639]. Íà ïñíîâàíèè íåäàâíèõ âñêðûòèé êðèïòîãðàôè Ãîëîìàíà [1063], ÿ ñîâòóþ èñïîëüçîâàòü *k* íå ìåíüøå 15. Ëó÷øå èñïîëüçîâàòü áîëüøå êðîòêèõ LFSR, ÷åì ìåíüøå äëèííûõ LFSR.

Ïðîðåæèâàåìûé ãåíåðàòîð

Ïðîðåæèâàåìûé (shrinking) ãåíåðàòîð [378] èñïîëüçóåò äóãóþ ôîðìó óïðàâëÿåìîé òàêòèðîâàíèÿ. Âîçüìåì äâà LFSR: LFSR-l è LFSR -2. Ïîäàäèì òàêòîâûé èìïóëüñ íà îáà ðåãèñòðà. Åñëè âûõîäíîé LFSR-l ÿâëÿåòñÿ 1, òî âûõîäíîì ãåíåðàòîðà ÿâëÿåòñÿ âûõîä LFSR-2. Åñëè âûõîä LFSR-l ðàâåí 0, îáà áèòà ñäâèãîâàþòñÿ, LFSR òàêòèðóþòñÿ çàíîâî è âñå ïîâòîðÿåòñÿ.

Èäåÿ ïðîñòà, äîñòàòî÷íî ýôôåêòèâíà è êàæåòñÿ áåçîïàñíîé. Åñëè ìíîãî÷ëåíû îáðàòíîé ñâÿçè ïðîðåæåíû, ãåíåðàòîð ÷óâñòâèòåëåí ê âñêðûòèþ, íî äðóãèõ ïðîáëåì íåò äåéñòâèòåëüíî íå âûëî. Õîòÿ ýòî òàê äëÿ ïðîáëåì ðàçëè÷åíèÿ è âîññòàíîâëåíèÿ ïîñëåäîâàòåëüíîñòè, îíè íå ïîõîæè íà îáû÷íûå ïðîáëåìû ïîòîêîâîãî øèôðîâàíèÿ. Ïðîáëåìà ïîäáîðà ïîëèíîìîâ îáðàòíûõ LFSR, ïîðîæäàþùèõ ïîñëåäîâàòåëüíîñòè ñ íóëåâûì ñðåäíèì, ïîäðîáíî èññëåäîâàíà â [901].

Ñàìîïðîðåæèâàåìûé ãåíåðàòîð

Ñàìîïðîðåæèâàåìûé (self-shrinking) ãåíåðàòîð [1050] ÿâëÿåòñÿ âàðèàíòîì ïðîðåæèâàåìîãî ãåíåðàòîðà. Âìåñòî äâóõ LFSR èñïîëüçóåòñÿ ïàðà áèòîâ îäíîãî LFSR. Ïðîàêòèðóéòå LFSR äâàæäû. Åñëè ïåðâûì áèòîì ïàðû áóäåò 1, òî âòîðîé áèò áóäåò âûõîäíîì ãåíåðàòîðà. Åñëè ïåðâûé áèò - 0, ñáðîñüòå îáà áèòà è ïîïðîáóéòå ñíîâà. Õîòÿ äëÿ ñàìîïðîðåæèâàåìîãî ãåíåðàòîðà íóæíî ïðèìåðíî â äâà ðàçà ìåíüøå ïàìÿòè, ÷åì äëÿ ïðîðåæèâàåìî-

ãî, îí ðàáîòàåò â äâà ðàçà ìåäëåííåå.

Õîòÿ ñàìîïðîâåðêàìûé ãåíåðàòîð òàêæå êàæåòñÿ áåçîïàñíûì, îí ìîæåò âñòè ñåáÿ íåïðåäñêàçóåìûì îáðàçîì è îáëàäàòü íåçâåñòíûìè ñâîéñòâàìè. Ýòî î÷åíü íîâûé ãåíåðàòîð, äàéòå åìó íåìíîãî âðåìåíè.

16.5 A5

A5 - ýòî ïîòîêîâûé øèôð, èñïîëüçóåìûé äëÿ øèôðîâàíèÿ GSM (Group Special Mobile). Ýòî åâðîïåéñêèé ñòàíäàðò äëÿ öèôðîâûõ ìîáèëüíûõ òåëåôîíîâ. Î í èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ êàíàëà "òåëåôîíáàçîâàÿ ñòàíöèÿ". Îñòàâøàÿñÿ ÷àñòü êàíàëà íå øèôðóåòñÿ, òàëåôîííàÿ êîìïàíèÿ ìîæåò ëåãêî ñäåëàòü ÷òîíèáóäü ñâîèì ðàçãîâîðàì.

Âîêðóã ýòîãî ïðîòîêîëà âåäóòñÿ ñòðàííûå ïîëèòè÷åñêèå èãðû. Ïåðâîíà÷àëüíî ïðåäïîëàãàëîñü, ÷òî êðèïòîãðàôèÿ GSM ïîçâîëèò çàïðåòèòü ýêñïîðò òåëåôîíîâ â íåêîòîðûå ñòðàíû. Òàïððü ðÿä ÷èíîâíèêîâ îáñóæäàåò, íå ïîâðåäèò ëè A5 ýêñïîðòíûì ïðîäóêòàì íåñìîòðÿ íà òî, ÷òî îí òàê ñëàá, ÷òî âðÿä ëè ñìîæåò ñëóæèòü ïðåïÿòñòâèåì. Ï î ñëóõàì â ñåðåäèíå 80-õ ðàçëè÷íûå ñåêðåòíûå ñëóæáû ÍÀÒÎ ñòàíîâëåíü ïî âîïðîñ, äîëæíî ëè øèôðîâàíèå GSM áûòü ñèëüíûì èëè ñëàáûì. Íåìàì áûëà íóæíà ñèëüíàÿ êðèïòîãðàôèÿ, òàê êàê ðÿäîì ñ íèì íàõîäèëñÿ Ñîâåòñêèé Ñîþç. Âçÿëè âåðõ äóõàÿ òî÷êà çðåíèÿ, è A5 ïðåäñòàâëÿåò ñîáîé ôðàíöóçñêóþ ðàçðàáîòêó.

Áîëüøèíñòâî äåòàëåé íàì èçâåñòíî. Áðèòàíñêàÿ òåëåôîííàÿ êîìïàíèÿ ïðåäëîæèëà âñþ äîêóìåíòàöèþ Áðýäôîðäñêîìó óíèâåðñèòåòó (Bradford University), íå çàñòàâèâ ïîäïèñàòü ñîãëàøåíèå î íåðàçãëàøåíèè. Èíôîðìàöèÿ ãäå-òî ïðîñî÷èëàñü è íàêîíåö áûëà îïóáëèêîâàíà â Internet. A5 îïèñûâàåòñÿ â [1622], òàêæå â êîíöå ýòîé êíèãè ïðèâåäåí êîä ýòîãî ïðîòîêîëà.

A5 ñîñòîèò èç òðåõ LFSR äëèíîé 19, 22 è 23, âñå ìíîãî÷ëåíû îáðàòíûé ñâÿçè - ïðîñòåéøèå. Âûõîäíî ÿâëÿåòñÿ XOR òðåõ LFSR. Â A5 èñïîëüçóåòñÿ èçìåíÿåìîå óïðàâëÿåìàÿ òàêòèðîâàíèå. Êàæäûé ðåãèñòð òàêòèðóåòñÿ â çàâèñèìîñòè îò ñâîåãî ñðåäíåãî áèòà, çàòåì âûïîëíÿåòñÿ XOR ñ îáðàòíîé ïîðîâîé ôóíêöèåé ñðåäíèõ áèòîâ âñåõ òðåõ ðåãèñòðîâ. Îáû÷íî íà êàæäîì ýòàïå òàêòèðóåòñÿ äâà LFSR.

Ñóùåñòâóåò òðèâèàëüíîå âñêðûòèå, òðåáóþùåå 2^{40} øèôðîâàíèé: ïðåäïîëîæèòå ñîäåðæàíèå ïåðâûõ äâóõ LFSR è ïîùòàéòåñü îïðåäåëèòü òðåòèé LFSR ïî ïîòîêó êëþ÷åé. (Äåéñòâèòåëüíî ëè òàêîé ñïîñîá âñêðûòèÿ âîçìîæåí, îñòàåòñÿ ïîä âîïðîñîì, êîòîðûé ñêîðî áóäåò ðàçðåøåí ðàçðàáàòûâàåìîé ìàøèíîé äëÿ àïïàðàòíîãî ïîêîëåíèÿ êëþ÷åé [45].)

Òåì íå ìåíåå, ñòàíîâèòñÿ ÿñíî, ÷òî èäåè, ëåæàùèå â îñíîâå A5, íåïëîõè. Àëãîðèòì î÷åíü ýôôåêòèâåí. Î í óäîâëåòâîðÿåò âñåì èçâåñòíûì ñòàòèñòè÷åñêèì òåñòàì, åäèíñòâåííîé åãî ñëàáîñòüþ ÿâëÿåòñÿ òî, ÷òî åãî ðåãèñòðû ñëèøêîì êîðîòêè, ÷òîáû ïðåäïîëàãàòü îñòàòî÷íóþ ñòîéêîñòü. Âàðèàíò A5 ñ áîëåå äëèííûìè ñäâèãîâûìè ðåãèñòðàìè è áîëåå ïëîòíûì ìíîãî÷ëåíàìè îáðàòíîé ñâÿçè äîëæíû áûòü áåçîïàñíû.

16.6 Hughes XPD/KPD

Ýòî àëãîðèòì áûë ïðåäëîæåí Hughes Aircraft Corp. Ýòà ôèðìà âñòðîèëà åãî â àðìåéñêèå òàêòè÷åñêèå ðàöèè è îáðóäîâàíèå ïîëêà íàïðàâëåíèÿ äëÿ ïðîäàæè çà ðàáíèöó. Àëãîðèòì áûë ðàçðàáîòàí â 1986 ãîäó è ïîëó÷èë íàçâàíèå XPD, ñîêðàùåíèå îò Exportable Protection Device - Ýêñïîðòèðóåìîå óñòðîéñòâî çàùèòû. Ïîçäíåå îí áûë ïåðåèìåíîâàí â KPD - Óñòðîéñòâî êëþ÷åâîé çàùèòû - è ðàññåðå÷åí [1037, 1036].

Àëãîðèòì èñïîëüçóåò 61-áèòîâûé LFSR. Ñóùåñòâóåò 2^{10} ðàçëè÷íûõ ïðèíöèïîâ ìíîãî÷ëåíà îáðàòíîé ñâÿçè, îäíîðàçíûõ NSA. Êëþ÷ âûáèðàåò îäèí èç ýòèõ ìíîãî÷ëåíîâ (õðàíÿùèõñÿ ãäå-òî â ÏÇÓ), à òàêæå íà÷àëüíîå ñîñòîÿíèå LFSR.

Â àëãîðèòìå âîñåìü ðàçëè÷íûõ íåèíåéíûõôèëüòðîâ, êàæäûé èç êîòîðûõ èñïîëüçóåò øåñòü îòâîäîâ LFSR, âûäàâàÿ îäèí áèò. Îáúåäèíÿÿñü, ýòè áèòû îáðàçóþò áàéò, êîòîðûé è ïðèíÿòûì îáðàçîì ïîäàåòñÿ íà áîëüøîé íåëèíåéíûé ñòîë. NSA ðàçðàáîòàëî åãî ýêñïîðò, ñëåäîâàòåëüíî äîëæåí áûòü ñîçíàíèå áîëüøîé ôèðìû, à âîçìîæíî è äëÿ ïðî÷èõ. NSA ðàçðåøèëî ýêñïîðò, íå áîëüøåãî ÷åì 2^{40}. Íî êàêîé?

16.7 Nanoteq

Nanoteq - ýòî þæíîàôðèêàíñêàÿ ýëåêòðîííàÿ êîìïàíèÿ. Èìåííî ýòîò àëãîðèòì èñïîëüçóåòñÿ þæíîàôðèêàíñêîé ïîëèöèåé ïðè øèôðîâàíèè ïåðåäà÷è ôàêñîâ, à âîçìîæíî è äëÿ ïðî÷èõ óæä.

Áîëåå èëè ìåíåå ýòî àëãîðèòì îïèñàí â [902, 903]. Î í èñïîëüçóåò 127-áèòîâûé LFSR ñ ôèêñèðîâàííûì ìíîãî÷ëåíîì îáðàòíîé ñâÿçè, êëþ÷ ïðåäñòàâëÿåò ñîáîé íà÷àëüíîå ñîñòîÿíèå ðåãèñòðà. Ïðè ïîìîùè 25 ýëåìåíòàðíûõ ÿ÷ååê 127 áèòîâ ðåãèñòðà ïðåâðàùàþòñÿ â îäèí áèò ïîòîêà êëþ÷åé. Ó êàæäîé ÿ÷åéêè 5 âõîäîâ è îäèí âûõîä:

$f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + (x_1 + x_3)(x_2 + x_4 + x_5) + (x_1 + x_4)(x_2 + x_3) + x_5$

Êàæäûé âûõîä ôóíêöèè ïîäâåðãàåòñÿ îïåðàöèè XOR ñ íåêîòîðûì áèòîì êëþ÷à. Êðîìå òîãî, ñóùåñòâóåò ñåêðåòíàÿ ïåðåñòàíîâêà, çàâèñÿùàÿ îò êîíêðåòíîé ðåàëèçàöèè è íå îïèñàííàÿ â ñòàòüÿõ ïîäðîáíî. Ýòî àëãîðèòì äîñòóïåí òîëüêî â àïïàðàòíîì âèäå.

Áåçîïàñåí ëè îí? ß íå óâåðåí. Ðÿä èíòåðåñíûõ ôàêòîâ, ïåðåäàâàåìûõ ìåæäó ïîëèöåéñêèìè ó÷àñòêàìè, èíîãäà ïîÿâëÿëñÿ â ëèáåðàëüíûõ ãàçåòàõ. Ýòî âïîëíå ìîãëî áûòü ðåçóëüòàòîì ìåðêàíòèëüíûõ, àíãëèéñêîé, àìåðèêàíñêîé, ñîâåòñêîé ðàçâåäûâàòåëüíîé äåÿòåëüíîñòè. Ðîññ Àíäåðñîí (Ross Anderson) ïðåäïîëîæèë ðÿä ïåðâûõ øàãîâ, êðèòèêîâàëè, ÷òî ñêîðî ïîÿâÿòñÿ íîâûå ðåçóëüòàòû [46], ÿ äóìàþ, ÷òî ñêîðî ïîÿâÿòñÿ íîâûå ðåçóëüòàòû.

16.8 Rambutan

Rambutan - ýòî àíãëèéñêèé àëãîðèòì, ðàçðàáîòàííûé Communications Electronics Security Croup (Ãðóïïà ïî áåçîïàñíîñòè ýëåêòðîííûõ êîìóíèêàöèé, îäíî èç îáúåäèíåíèé, èñïîëüçîâàííûõ CCHQ). Îí ïðîäàâàëñÿ òîëüêî â âèäå àïïàðàòíîãî ìîäóëÿ è îãðàíè÷åí äëÿ çàùèòû äîêóìåíòîâ âïëîòü äî ãðèôà "Êîíôèäåíöèàëüíî". Ñàì àëãîðèòì çàñåêðå÷åí, è ìèêðîñõåìà íå ïðåäíàçíà÷åíà äëÿ øèðîêîé êîìåð÷åñêîé ïðîäàæè.

Rambutan èñïîëüçóåò 112-áèòîâûé êëþ÷ (ïëþñ áèòû ÷åòíîñòè) è ìîæåò ðàáîòàòü òðåõ ðåæèìàõ: ECB, CBC, è 8-áèòîâûé CFB. Ýòî ñèëüíûé àðãóìåíò â ïîëüçó òîãî, ÷òî ýòîò àëãîðèòì - áîë÷íûé, íî ñóõè óòâåðäàþò èíîå. Ïðåäïîëàãàåòñÿ ýòî ïîòîêîâûé øèôð ñ LFSR. Ó íåãî ïÿòü ïðèáëèçèòåëüíî 80-áèòîâûõ ñâîãîâûõ ðåãèñòðîâ ðàçëè÷íîé äëèíû. Ïîëèíîìû îáðàòíîé ñâÿçè çíà÷èòåëüíî ïðîñòûå, â êàæäîì èç íèõ âñåãî ëèøü 10 îòâîäîâ. Êàæäûé ñâîãîâûé ðåãèñòð íåñïå÷èâàò ÷åòûðå âõîäà äëÿ î÷åíü áîëüøîé è ñëîæíîé íåëèíåéíîé ôóíêöèè, êîòîðàÿ è âûäàåò åäèíñòâåííûé áèò.

Ï î÷åìó Rambutan? Âîçìîæíî èç-çà ôðóêòà, êîòîðûé êîëþ÷èé è íåïðèñòóïíûé ñíàðóæè, íî ìÿãêèé è íåæíûé âíóòðè. Í î ñ äðóãîé ñòîðîíû íèêàêîé ïðè÷èíû ìîæåò è íå áûòü.

16.9 Àääèòèâíûå ãåíåðàòîðû

Àääèòèâíûå ãåíåðàòîðû (èíîãäà íàçûâàåìûå çàïàçäûâàþùèìè ãåíåðàòîðàìè Ôèáîíà÷÷è) î÷åíü ýôôåêòèâíû, òàê êàê èõ ðåçóëüòàòû ÿâëÿþòñÿ ñëó÷àéíûå ñëîâà, à íå ñëó÷àéíûå áèòû [863]. Ñàìè ïî ñåáå îíè íå áåçîïàñíû, íî èõ ìîæíî èñïîëüçîâàòü â êà÷åñòâå ñîñòàâíûõ áëîêîâ äëÿ áåçîïàñíûõ ãåíåðàòîðîâ.

Íà÷àëüíûå ñîñòîÿíèå ãåíåðàòîðà ïðåäñòàâëÿåò ñîáîé ìàññèâ *n*-áèòîâûõ ñëîâ: 8-áèòîâûõ ñëîâ, 16-áèòîâûõ ñëîâ, 32-áèòîâûõ ñëîâ, è ò.ä.: X_1, X_2, X_3, ..., X_m. Ýòî ïåðâîíà÷àëüíîå ñîñòîÿíèå è ÿâëÿåòñÿ êëþ÷îì. *i*-îå ñëîâî ãåíåðàòîðà ïîëó÷àåòñÿ êàê

$X_i = (X_{i-a} + X_{i-b} + X_{i-c} + + X_{i-m}) \bmod 2^n$

Ïðè ïðàâèëüíîì âûáîðå êîýôôèöèåíòîâ *a*, *b*, *c*, . . . , *m* ïåðèîä ýòîãî ãåíåðàòîðà íå ìåíüøå 2^n-1. Îäíè èç òðåáîâàíèé ê êîýôôèöèåíòàì ÿâëÿåòñÿ òî, ÷òî ìèäøèé çíà÷àùèé áèò îáðàçóåò LFSR ìàêñèìàëüíîé äëèíû.

Íàïðèìåð, (55,24,0) - ýòî ïðèìèòèâíûé íîìîíëåí mod 2 èç 14-é. Ýòî îçíà÷àåò, ÷òî äëèíà ñëåäóþùåãî àääèòèâíîãî ãåíåðàòîðà ìàêñèìàëüíà.

$X_i = (X_{i-55} + X_{i-24}) \bmod 2^n$

Ýòî ðàâíîåñò, òàê êàê ó ïðèìèòèâíîãî ìíîãî÷ëåíà òðè êîýôôèöèåíòà. Åñëè âû èõ áûëî áîëüøå, äëÿ ïîëó÷åíèÿ ìàêñèìàëüíîé äëèíû ïîòðåáîâàëèñü âû äîïîëíèòåëüíûå óñëîâèÿ. Ï îäîáíîñòè ìîæíî íàéòè â [249].

Fish

Fish - ýòî àääèòèâíûé ãåíåðàòîð, îñíîâàííûé íà ìåòîäàõ, èñïîëüçóåìûõ â ïðîãðàììíîì ãåíåðàòîðå [190]. Îí âûäàåò ïîòîê 32-áèòîâûõ ñëîâ, êîòîðûå ìîãóò áûòü èñïîëüçîâàíû (ñ ïîìîùüþ XOR) ñ ïîòîêîì îòêðûòîãî òåêñòà äëÿ ïîëó÷åíèÿ øèôðîâàííà èëè ñ ïîòîêîì øèôðîâàííà äëÿ ïîëó÷åíèÿ îòêðûòîãî òåêñòà. Íàçâàíèå äëîãðèìà ïðåäñòàâëÿåò ñîáîé ñîêðàùåíèå îò Fibonacci shrinking generator - ïðîðåæèâàþùèé ãåíåðàòîð Ôèáîíà÷÷è.

Âî ïåðâûõ èñïîëüçóéòå äâà ñëåäóþùèõ ãåíåðàòîðà. Êëþ÷îì ÿâëÿåòñÿ íà÷àëüíûå ñîñòîÿíèÿ ýòèõ ãåíåðàòîðîâ.

$A_i = (A_{i-55} + A_{i-24}) \bmod 2^{32}$

$B_i = (B_{i-52} + B_{i-19}) \bmod 2^{32}$

Ýòè ïîñëåäîâàòåëüíîñòè ïðîðåæèâàþòñÿ ïîïàðíî â çàâèñèìîñòè îò ìëàäøåãî çíà÷àùåãî áèòà B_i: åñëè åãî çíà÷åíèå ðàâíî 1, òî ïàðà èñïîëüçóåòñÿ, åñëè 0 - èãíîðèðóåòñÿ. C_j - ýòî ïîñëåäîâàòåëüíîñòü èñïîëüçóåìûõ ñëîâ *Ai*, à D_j - ýòî ïîñëåäîâàòåëüíîñòü èñïîëüçóåìûõ ñëîâ B_i. Äëÿ ãåíåðàòîðà 32-áèòîâûõ ñëîâ-ðåçóëüòàòîâ K_{2j} è K_{2j+1} ýòè ñëîâà èñïîëüçóþòñÿ ïàðàìè - C_{2j}, C_{2j+1}, D_{2j}, D_{2j+1}.

$E_{2j} = C_{2j} \oplus (D_{2j}, \wedge D_{2j+1})$

$F_{2j} = D_{2j+1} \wedge (E_j, \wedge C_{2j+1})$

$K_{2j} = E_{2j} \oplus F_{2j}$

$K_{2j+1} = C_{2j+1} \oplus F_{2j}$

Ýòîò àëãîðèòì áûñòð. íà ïðîöåññîðå i486/33 ðåàëèçàöèÿ Fish íà ÿçûêå C øèôðóåò äàííûå ñî ñêîðîñòüþ 15- Ì áèò/ñ. Ê ñîæàëåíèþ îí òàêæå íå áåçîïàñåí, ïîðÿäîê âñêðûòèÿ ñîñòàâëÿåò îêîëî 2^{40} [45].

Pike

Pike - ýòî îáåäíåííàÿ è óðåçàííàÿ âåðñèÿ Fish, ïðåäëîæåííàÿ Ðîññîì Àíäåðñîíîì, òàì, êòî âçëîìàë Fish [45]. Î í èñïîëüçóåò òðè àääèòèâíûõ ãåíåðàòîðà. Íàïðèìåð:

$A_i = (A_{i-55} + A_{i-24}) \bmod 2^{32}$

$B_i = (B_{i-57} + B_{i-7}) \bmod 2^{32}$

$C_i = (C_{i-58} + C_{i-19}) \bmod 2^{32}$

Äëÿ ãåíåðàöèè ñëîâà ïîòîêà êëþ÷åé âçãëÿíèòå íà áèòû ïåðåíîñà ïðè ñëîæåíèè. Åñëè âñå òðè îäèíàêîâû (âñå íóëè èëè âñå åäèíèöû), òî òàêòèðóþùèé âñå òðè ãåíåðàòîðà. Åñëè íåò, òî òàêòèðóþùèé òîëüêî äâà ñîâïàäàþùèõ ãåíåðàòîðà. Ñîõðàíèòå áèòû ïåðåíîñà äëÿ ñëåäóþùåãî ðàçà. Îêîí÷àòåëüíûì âûõîäîì ÿâëÿåòñÿ XOR âûõîäîâ òðåõ ãåíåðàòîðîâ.

Pike áûñòðåå Fish, òàê êàê â ñðåäíåì äëÿ ïîëó÷åíèÿ ðåçóëüòàòà íóæíî 2.75 äåéñòâèÿ, à íå 3. Î í òàêæå ñëèøêîì íîâ, ÷òîáû åìó äîâåðÿòü, íî âûãëÿäèò î÷åíü íåïëîõî.

Mush

Mush ïðåäñòàâëÿåò ñîáîé âçàèìî ïðîðåæäàþùèé ãåíåðàòîð. Åãî ðàáîòó îáúÿñíèòü ëåãêî [1590]. Âîçüìåì äâà àääèòèâíûõ ãåíåðàòîðà: *A* è *B*. Åñëè áèò ïåðåíîñà *A* óñòàíîâëåí, òàêòèðóåòñÿ *B*. Åñëè áèò ïåðåíîñà *B* óñòàíîâëåí, òàêòèðóåòñÿ *A*. Òàêòèðóåì *A* è ïðè ïåðåïîëíåíèè óñòàíàâëèâàåì áèò ïåðåíîñà. Òàêòèðóåì *B* è ïðè ïåðåïîëíåíèè óñòàíàâëèâàåì áèò ïåðåíîñà. Îêîí÷àòåëüíûì âûõîäîì ÿâëÿåòñÿ XOR âûõîäîâ *A* è *B*. Ïðîùå âñåãî èñïîëüçîâàòü òå æå ãåíåðàòîðû, ÷òî è â Fish:

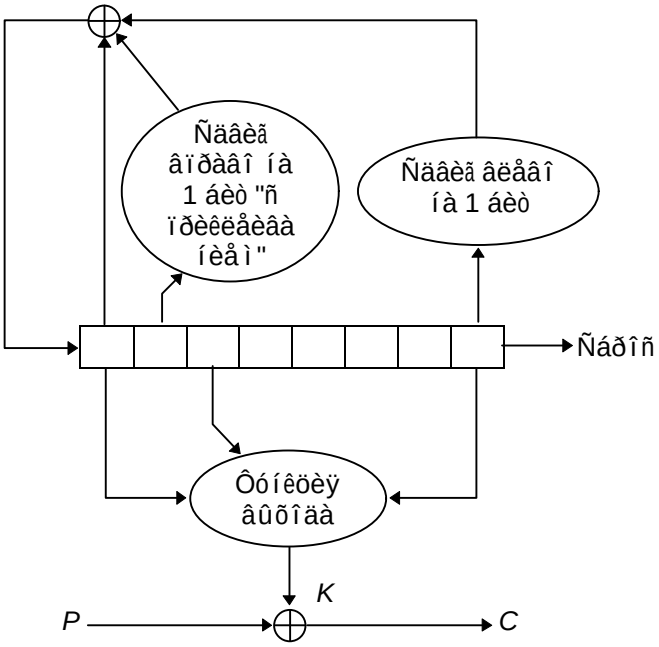
$A_i = (A_{i-55} + A_{i-24}) \bmod 2^{32}$

$B_i = (B_{i-52} + B_{i-19}) \bmod 2^{32}$

Â ñðåäíåì äëÿ ãåíåðàòîðà ïîñëåäîâàòåëüíîñòè îäíîãî âûõîäíîãî ñëîâà íóæíî òðè èòåðàöèè ãåíåðàòîðà. È åñëè êîýôôèöèåíòû àääèòèâíîãî ãåíåðàòîðà âûáðàíû è ÿâëÿþòñÿ âçàèìíî ïðîñòûìè, äëèíà âûõîäíîé ïîñëåäîâàòåëüíîñòè áóäåò ìàêñèìàëüíà. Ì íå íåèçâåñòíî îá óñïåøíûõ âñêðûòèÿõ, íî íå çàáûâàéòå, ÷òî ýòîò àëãîðèòì î÷åíü íîâ.

16.10 Gifford

Äýâèä Äæèôôîðä (David Gifford) èçîáðåë ïîòîêîâûé øèôð è èñïîëüçîâàë åãî äëÿ øèôðîâàíèÿ ñåòåâîé íîâîñòåé â ðàéîíå Áîñòîíà ñ 1984 ïî 1988 ãîä [608, 607, 609]. Àëãîðèòì èñïîëüçóåò äâèíñòâåííûé 8-áàéòîâûé ðåãiñòð: b_0, b_1, . . . , b_7. Êëþ÷îì ÿâëÿåòñÿ íà÷àëüíîå ñîñòîÿíèå ðåãiñòðà. Àëãîðèòì ðàáîòàåò â ðåæèìå OFB, îòêðûòûé òåêñò àáñîëþòíî íå âëèÿåò íà ðàáîòó àëãîðèòìà. (Ñì. -1-é).



Ðèñ. 16-17. Gifford.

Äëÿ ãåíåðàöèè áàéòà êëþ÷à k_i îáúåäèíèì b_0 è b_1, à òàêæå îáúåäèíèì b_4 è b_7. Ïåðåìíîæèì ïîëó÷åííûå ÷èñëà, ïîëó÷àÿ 32-áèòîâîå ÷èñëî. Òðåòüè ñëåâà áàéòîì è áóäåò k_i.

Äëÿ îáíîâëåíèÿ ðåãiñòðà âîçüìåì b_1 è ñäâèíåì âïðàâî "ñ ïðèêëåèâàíèåì" íà 1 áèò ñëåâóþ ùèì îáðàçîì: êðàéíèé ëåâûé áèò îáíîâëåíèÿ è ñäâèãàåòñÿ, è îñòàåòñÿ íà ìåñòå. Âîçüìåì b_7 è ñäâèíåì åãî íà îäèí áèò âëåâî, â êðàéíåé ïðàâîé îïçèöèè äîëæíî îêàçàòüñÿ 0. Âûïîëíèì XOR èçìåíåííîãî b_1, èçìåíåííîãî b_7 è b_0. Ñäâèíåì ïåðâîíà÷àëüíûé áàéò ðåãiñòðà íà 1 áèò âïðàâî è ïîìåñòèì ýòî áàéò â êðàéíþþ ëåâóþ ïîçèöèþ.

Â òå÷åíèå âñåãî âðåìåíè èñïîëüçîâàíèÿ ýòîò àëãîðèòì îñòàâàëñÿ áåçîïàñíûì, íî îí áûë âçëîìàí â 1994 ãîäó [287]. Îêàçàëîñü, ÷òî ìíîãî÷ëåí îáðàòíîé ñâÿçè íå áûë ïðèìåíèìû è, òàêèì îáðàçîì, ìîãà áûòü âñêðûò.

16.11 Àëãîðèòì M

Ýòî íàçâàíèå äàíî Êíóòîì [863]. Àëãîðèòì ïðåäñòàâëÿåò ñîáîé ïîñëåäîâàòåëüíîñòü íåêîëüêî ïñåâäîñëó÷àéíûõ ïîòîêîâ, óäåëè÷èâàÿ èõ áåçîïàñíîñòü. Âûõîä îäíîãî ãåíåðàòîðà èñïîëüçóåòñÿ äëÿ âûáîðà îòñòàþùåãî âûõîäà äðóãîãî ãåíåðàòîðà [996, 1003]. Íà ÿçûêå C:

```
#define ARR_SIZE (8192) /* íàïðèìåð - ÷åì áîëüøå, òåì ëó÷øå */
static unsigned char delay[ ARRSIZE ] ;
unsigned char prngA( void )
long prngB( void ) ;
void init_algM( void ) {
     long i ;
     for ( i = 0 ; i < ARR_SIZE ; i++ )
            delay[i] = prngA() ;
} /* lnlt_algM */
unsigned char alglM( void ) {
     long j,v ;
     j = prngB() % ARR_SIZE ; /* ïîëó÷èòü èíäåêñ delay[]*/
     v = delay[j] ; /* ïîëó÷èòü âîçâðàùàåìîå çíà÷åíèå */
     delay[j] = prngA() ; /* çàìåíèòü åãî */
     return ( v ) ;
     } /* algM */
```

Ñìûñë ñîñòîèò â òîì, ÷òî åñëè prngA - äåéñòâèòåëüíî ñëó÷àéíî, íåâîçìîæíî íè÷åãî óçíàòü î prngB (è, ñëåäîâàòåëüíî, íåâîçìîæíî âûïîëíèòü êðèòè÷åñêèé ìîìåíò ìåòîäà çàìåíû). Åñëè prngA èìååò òàêîé âèä, ÷òî åãî êðèïòîàíàëèç ìîæåò áûòü âûïîëíåí òîëüêî, åñëè åãî âûõîä äîñòóïåí â ñâîþ î÷åðåäü (ò.å., òîëüêî åñëè ñíà÷àëà áûë âûïîëíåí êðèï-

òîàíàëèç prngB), à â ïðîòèâíîì ñëó÷àå îíî ïî ñóòè äåéñòâèòåëüíî ñëó÷àéíî, òî ýòà êîìáèíàöèÿ äîëæíà áûòü áåçîïàñíîé.

16.12 PKZIP

Àëãîðèòì øèôðîâàíèÿ, âñòðîåííûé â ïðîãðàììó ñæàòèÿ äàííûõ PKZIP, áûë ðàçðàáîòàí Ðîäæåðîì Ùëàôêû (Roger Schlafly). Ýòî ïîòîêîâûé øèôð, øèôðóþùèé äàííûå ïîáàéòíî. Ïî êðàéíåé ìåðå ýòîò àëãîðèòì èñïîëüçóåòñÿ â âåðñèè 2.04g. ß íå ìîãó íè÷åãî íêàçàòü î áîëåå ïîçäíèõ âåðñèÿõ, íî åñëè íå áûë ñäåëàíî íèêàêèõ çàÿâëåíèé îá îáðàòíîì, ìîæíî ñ÷èòàòü ñ áîëüøîé âåðîÿòíîñòüþ, ÷òî àëãîðèòì íå èçìåíèëñÿ. Àëãîðèòì èñïîëüçóåò òðè 32-áèòîâûõ ïåðåìåííûõ, èíèöèàëèçèðîâàííûõ ñëåäóþùèì îáðàçîì:

K_0 = 305419896

K_1 = 591751049

K_2 = 878082192

Èñïîëüçóåòñÿ 8-áèòîâûé êëþ÷ K_3, ïîëó÷åííûé èç K_2. Âîò ýòîò àëãîðèòì (â ñòàíäàðòíîé íîòàöèè C):

$C_i = P_i \wedge K_3$

K_0= crc32 (K_0, P_i)

$K_1 = K_1 + (K_0 \,\&\, 0x000000ff)$

$K_1 = K_1 * 134775813 + 1$

K_2 = crc32 (K_2, $K_1 >> 24$)

$K_3 = ((K_2 \mid 2) * ((K_2 \mid 2) \wedge 1)) >> 8$

Ôóíêöèÿ crc32 áåðåò ñâîå ïðåäûäóùåå çíà÷åíèå è áàéò, âûïîëíÿåò èõ XOR è âû÷èñëÿåò ñëåäóþùåå çíà÷åíèå ñ ïîìîùüþ íåêîòîðîé CRC, îïðåäåëåííîé 0xedb88320. Íà ïðàêòèêå 256-ýëåìåíòíàÿ òàáëèöà ìîæåò áûòü ðàññ÷èòàíà çàðàíåå, è âû÷èñëåíèå crc32 ïðåâðàùàåòñÿ â:

crc32 (a, b) = ($a >> 8$) ^ table [(a & 0xff) $\oplus$ b]

Òàáëèöà ðàññ÷èòûâàåòñÿ â ñîîòâåòñòâèè ñ ïðåäûäóùèì îïðåäåëåíèåì crc32:

table [i] = crc32 (i, 0)

Äëÿ øèôðîâàíèÿ ïîòîêà îòêðûòîãî òåêñòà ñíà÷àëà äëÿ îáíîâëåíèÿ êëþ÷åé çàöèêëèì áàéòû êëþ÷à â àëãîðèòìå øèôðîâàíèÿ. Ïîëó÷åííûé øèôðîòåêñò íà ýòîì ýòàïå èãíîðèðóåòñÿ. Çàòåì ïîáàéòíî çàøèôðóåì îòêðûòûé òåêñò. Îòêðûòûì òåêñòó ïðåøåñòâóþò äâåíàäöàòü ñëó÷àéíûõ áàéòîâ, íî ýòî íà ñàìîì äåëå íåâàæíî. Äåøèôðèðîâàíèå ïîõîæå íà øèôðîâàíèå çà èñêëþ÷åíèåì òîãî, ÷òî âî âòîðîì äåéñòâèè àëãîðèòìà âìåñòî P_i èñïîëüçóåòñÿ C_i.

Áåçîïàñíîñòü PKZIP

Ê ñîæàëåíèþ îíà íå ñëèøêîì âåëèêà. Äëÿ âñêðûòèÿ íóæíî îò 40 äî 2000 áàéòîâ èçâåñòíîãî îòêðûòîãî òåêñòà, âðåìåíàÿ ñëîæíîñòü âñêðûòèÿ ñîñòàâèò 2^{27} [166]. Íà âàøåì ïðîñòåéøåì êîìüþòåðå ýòî ìîæíî ñäåëàòü çà íåñêîëüêî ÷àñîâ. Åñëè â ñæàòîì ôàéëå èñïîëüçóþòñÿ êàêèå-íèáóäü ñòàíäàðòíûå çàãîëîâêè, ïîëó÷åííàÿ îòêðûòàÿ òåêñòà íå ïðåäñòàâëÿò ñîáîé ïðîáëåìû. Íå èñïîëüçóéòå âñòðîåííûå â PKZIP øèôðîâàíèå.

Ãëàâà 17
Äðóãèå ïîòîêîâûå øèôðû è ãåíåðàòîðû íàñòîÿùèõ ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé

17.1 RC4

RC4 - ýòî ïîòîêîâûé øèôð ñ ïåðåìåííûì ðàçìåðîì êëþ÷à, ðàçðàáîòàííûé â 1987 ãîäó Ðîíîì Ðèâåñòîì äëÿ RSA Data Security, Inc. Â òå÷åíèå ñåì ëåò îí íàõîäèëñÿ â ÷àñòíîé ñîáñòâåííîñòè, è ïîäîâíå îïèñàíèå àëãîðèòìà ïðåäñòàâëÿëîñü òîëüêî ïîñëå ïîÿâëåíèÿ ñîãëàøåíèÿ î íåðàçãëàøåíèè.

Â ñåíòÿáðå 1994 êòî-òî àíîíèìíî îïóáëèêîâàë èñõîäíûé êîä â ñïèñêå ðàññûëêè "Êèáåðïàíêè" (Cypherpunks). Î íáûñòðî ðàñïðîñòðàíèëñÿ â òåëåêîíôåðåíöèè Usenet sci.crypt è ÷åðåç Internet ïî ðàçëè÷íûì ftp-ñåðâåðàì âî âñåì ìèðå. Îáëàäàòåëè ëåãàëüíûõ êîïèé RC4 äîñòîâåðíîñòü ýòîãî êîäà. RSA Data Security, Inc. ïîíûòàëàñü çàãíàòü äæèííà îáðàòíî â áóòûëêó, óòâåðæäàÿ, ÷òî íåíìîòðÿ íà îïóáëèêîâàíèå àëãîðèòì îñòàåòñÿ òîðãîâûì ñåêðåòîì, áûë ñëèøêîì ïîçäíî. Ñ òåõ ïîð àëãîðèòì îáñóæäàëñÿ è èçó÷àëñÿ â Usenet, ðàñïðîñòðàíÿëñÿ íà êîíôåðåíöèÿõ è ñëóæèë â êà÷åñòâå óÿçâèìîãî ïîñîáèÿ íà êóðñàõ ïî êðèïòîãðàôèè.

Îïèñûâàòü RC4 ïðîñòî. Àëãîðèòì ðàáîòàåò â ðåæèìå OFB: ïîòîê êëþ÷åé íå çàâèñèò îò îòêðûòîãî òåêñòà. Èñïîëüçóåòñÿ S-áëîê ðàçìåðîì 8*8: S_0, S_1, . . . , S_{255}. Ýëåìåíòû ïðåäñòàâëÿþò ñîáîé ïåðåñòàíîâêó ÷èñåë îò 0 äî 255, à ïðåñòàíîâêà ÿâëÿåòñÿ ôóíêöèåé êëþ÷à ïðåìåíîé äëèíû. Â äëîðèìå ïðèíÿòñÿ äâà ñ÷åò÷èêà, *i* è *j*, ñ íóëåâûì íà÷àëüíûì çíà÷åíèÿì.

Äëÿ ãåíåðàöèè ñëó÷àéíîãî áàéòà âû ïîëíÿåòñÿ ñëåäóþùåå:

$i = (i + 1) \bmod 256$

$j = (j + S_i) \bmod 256$

ïîìåíÿòü ìåñòàìè S_i è Sj

$t = (S_i + S_j) \bmod 256$

$K = S_t$

Áàéò K èñïîëüçóåòñÿ â îïåðàöèè XOR ñ îòêðûòûì òåêñòîì äëÿ ïîëó÷åíèÿ øèôðîâêè èëè â îïåðàöèè XOR ñ øèôðîâêîé äëÿ ïîëó÷åíèÿ îòêðûòîãî òåêñòà. Øèôðîâàíèå âûïîëíÿåòñÿ ïðèìåðíî â 10 ðàç áûñòðåå, ÷åì DES.

Òàêæå íåñëîæíà è èíèöèàëèçàöèÿ S-áëîêà. Ñíà÷àëà çàïîëíèì åãî ëèíåéíî: $S_0 = 0$, $S_1 = 1$, . . . , $S_{255} = 255$. Çàòåì çàïîëíèì êëþ÷îì äóãîé 256-áàéòîâûé ìàññèâ, ïðè íåîáõîäèìîñòè äîïîëíÿÿ êëþ÷: K_0, K_1, . . . , K_{255}. Óñòàíîâèì çíà÷åíèå èíäåêñà *j* ðàâíûì 0. Çàòåì:

for $i = 0$ to 255:

$j = (j + S_i + K_i) \bmod 256$

ïîìåíÿòü ìåñòàìè S_i è S_j

È ýòî âñå. RSADSI óòâåðæäàåò, ÷òî àëãîðèòì óñòîé÷èâ ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó, ÷òî, ïî-âèäèìîìó, â íåì íåò íèêàêèõ êîðîòêèõ öèêëîâ, è ÷òî îí â âûñîêîé ñòåïåíè íåëèíåéí. (Îïóáëèêîâàííûõ êðèïòîàíàëèç÷åñêèõ ðåçóëüòàòîâ íåò. RC4 ìîæåò íàõîäèòüſ â ïðèìåðíî 2^{1700} (256! * 256^2) âîçìîæíûõ ñîñòîÿíèé: íåâåðîÿòíî ÷èñëî.) S-áëîê ìåäëåííî èçìåíÿåòſ ïðè ñîîòâåòſòâèè: *i* îáñëå÷èâàåò èçìåíåíèå êàæäîãî ýëåìåíòà, à *j* - ÷òî ýëåìåíòû èçìåíÿþſſ ñëó÷àéíûì îáðàçîì. Àëãîðèòì íàñòîëüêî íåñëîæåí, ÷òî áîëüøèíſòâî ïðîãðàìì èſòóò çàêîäèðîâàòü åãî ïðîſòî ïî ïàìÿòè.

Ýòó èääþ ìîæíî îáúÿſòü íà S-áëîêè è ñëîâà áîëüøèõ ðàçìåðîâ. Âûøå áûëà îïèſàíà 8-áèòîâàÿ âåðſèÿ RC4. Íåò ïðè÷èí, ïî êîòîðûì íåëüçÿ áû áûëî ïðåäëîſòü 16-áèòîâûé RC4 ſ 16*16 S-áëîêîì (100 K ïàìÿòè) è 16-áèòîâûì ſëîâîì. Íà÷àëüíàÿ èòåðàöèÿ çàéìåò íàìíîãî áîëüøå âðåìåíè - äëÿ ſîõðàíåíèÿ ïðèâåäåííîé ſõåìû óæíî çàïîſíèòü 65536-ýëåìåſòíûé ìàſſèâ - íî ïîëó÷èâſèſſÿ äëãîðèòì äîëæåí áûſò áûſòðåå.

RC4 ſ êëþ÷îì äëèſíé íå áîëåå 40 áèòîâ îáëàäàåò ſïåöèàëüíûì ýêſïîðſíûì ſòàòóſîì (ſì. ðàçäåë 13.8). Ýòî ſïåöèàëüíûé ſòàòóſ íèêàê íå âëèÿåò íà áåçîïàſſíſſòü äëãîðèòìà, õîſÿ â òå÷åíèå ì íîãèõ ëåò RSA Data Security, Inc. íàìåêàë íà îáðàòíîſ. Íàçâàíèå äëãîðèòìà ÿâëÿåòſÿ òîðãîâîé ìàðêîé, ïîſòîì êàæäûé, êòî íàïèſåò ſîáſòâåííûé êîä, äîëæåí íàçâàòü åãî êàê-òî èíà÷å. Ðàçëè÷íûå âíóòðåííèå äîêóìåíòû RSA Data Security, Inc. äî ſèõ ïîð íå áûëè îſóáëèêîâàíû [1320, 1337].

Èòàê, êàêîâà æå ſèòóàöèÿ âîêðóã äëãîðèòìà RC4? Î íåſüſå íå ÿâëÿåòſÿ òîðãîâûì ſåêðåòîì, ïîſòîì êòî óãîäſſ èſåò âîçſîæſſîſòü âſſſîſüſíâàòüſſ èſ. Îſíàêî RSA Data Security, Inc. ſſ÷èſ íàåðſïÿêà âſçáóäèſ äåëî ſðôſòâ êàæäîâ, êòî ſðèſåſè íåëèöåíçèðîâàſſûé RC4 â êîſſåð÷åſſîſ ſðſäóêòå. Âſçſîæſſî èſ è íå óäàſòſÿ

âûèãðàòü ïðîöåññ, íî ïî÷òè íàâåðíÿêà äëÿ äðóãîé êîìïàíèè äåøåâëå êóïèòü ëèöåíçèþ, ÷åì ñóäèòüñÿ.

RC4 âõîäèò â äåñÿòêè êîìåð÷åñêèõ ïðîäóêòîâ, âêëþ÷àÿ Lotus Notes, AOCE êîìïàíèè Apple Computer è and Oracle Secure SQL. Ýòî àëãîðèòì òàêæå ÿâëÿåòñÿ ÷àñòüþ ñïåöèôèêàöèè Ñîòîâîé öèôðîâîé ïàêåòíîé ïåðåäà÷è äàííûõ (Cellular Digital Packet Data) [37].

17.2 SEAL

SEAL - ýòî ïðîãðàììíî ýôôåêòèâíûé ïîòîêîâûé øèôð, ðàçðàáîòàííûé â IBM Ôèëèï Ðîãýéëì (Phil Rogaway) è Äîíîí Êîïïåðñìèòì (Don Coppersmith) [1340]. Àëãîðèòì îïòèìèçèðîâàí äëÿ 32-áèòîâûõ ïðîöåññîðîâ: Äëÿ íîðìàëüíîé ðàáîòû åìó íóæíî âû÷èñëèòü 32-áèòîâûõ ðåãèñòðîâ è êýø-ïàìÿòè íà íåñêîëüêî êèëîáàéò. ×òîáû èçáåæàòü âëèÿíèÿ èñïîëüçîâàíèÿ ìåäëåííûõ îïåðàöèé SEAL âûïîëíÿåò ðÿä ïðåäâàðèòåëüíûõ äåéñòâèé ñ êëþ÷îì, ñîõðàíÿÿ ðåçóëüòàòû â íåñêîëüêèõ òàáëèöàõ. Ýòè òàáëèöû èñïîëüçóþòñÿ äëÿ óñêîðåíèÿ øèôðîâàíèÿ è äåøèôðèðîâàíèÿ.

Ñåìåéñòâî ïñåâäîñëó÷àéíûõ ôóíêöèé

Îñíîâíîñòüþ SEAL ÿâëÿåòñÿ òî, ÷òî îí â äåéñòâèòåëüíîñòè ÿâëÿåòñÿ íåòðàäèöèîííûì ïîòîêîâûì øèôðîì, à ïðåäñòàâëÿåò ñîáîé **ñåìåéñòâî ïñåâäîñëó÷àéíûõ ôóíêöèé**. Ïðè 160-áèòîâîì êëþ÷å *k* è 32-áèòîâîì *n* SEAL ðàñòÿãèâàåò *n* â *L*-áèòîâóþ ñòðîêó *k*(*n*). *L* ìîæåò ïðèíèìàòü ëþáîå çíà÷åíèå, ìåíüøåå 64 Êáàéò. SEAL, ïî âèäèìîìó, èñïîëüçóåò ñëåäóþùåå ñâîéñòâî: åñëè *k* âûáèðàåòñÿ ñëó÷àéíûì îáðàçîì, òî *k*(*n*) äîëæíî áûòü âû÷èñëèìî íåòðèâ÷èâî ïò ñëó÷àéíîé *L*-áèòîâîé ôóíêöèè *n*.

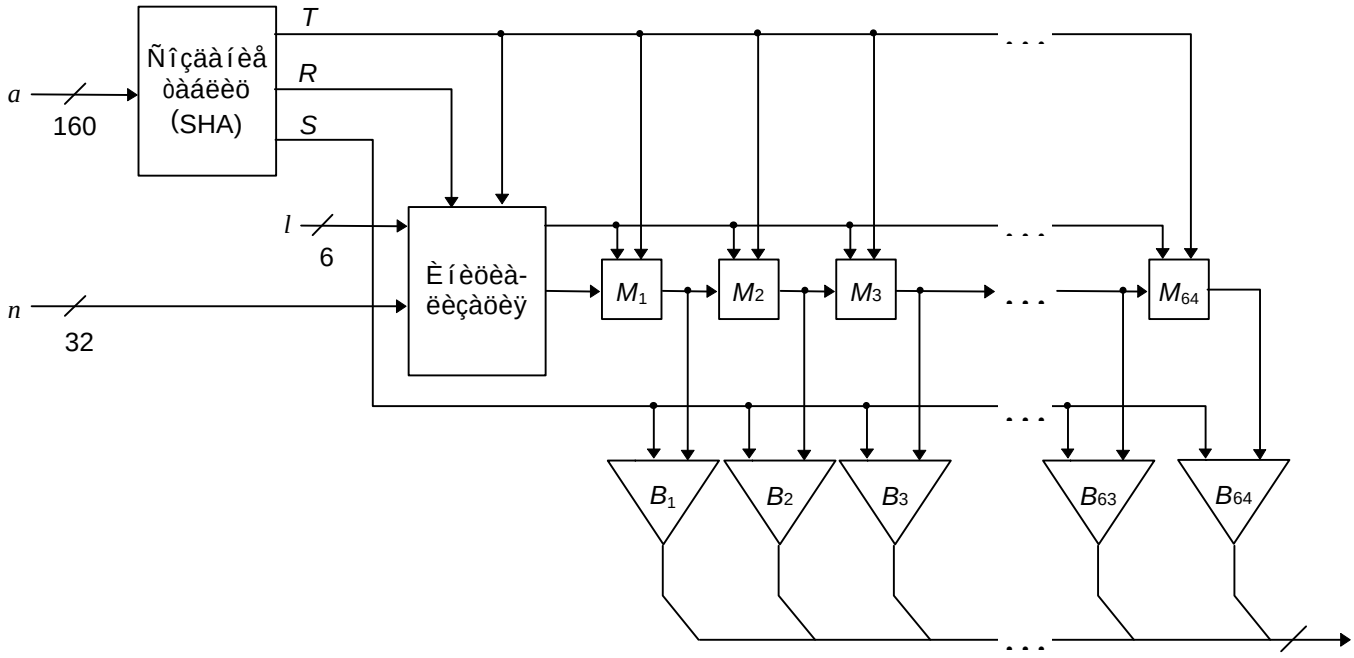
Ïðàêòè÷åñêèé ýôôåêò òîãî, ÷òî SEAL ÿâëÿåòñÿ ñåìåéñòâîì ïñåâäîñëó÷àéíûõ ôóíêöèé, ñîñòîèò â òîì, ÷òî îí óäîáåí â ðÿäå ïðèëîæåíèé, ãäå íåïðèìåíèìû òðàäèöèîííûå ïîòîêîâûå øèôðû. Èñïîëüçóÿ áîëüøèíñòâî ïîòîêîâûõ øèôðîâ, âû ñîçäàåòå îäíîíàïðàâëåíóþ ïîñëåäîâàòåëüíîñòü áèòîâ: åäèíñòâåííûì ñïîñîáîì îïðåäåëèòü *i*-ûé áèò, çíàÿ êëþ÷ è ïîçèöèþ *i*, ÿâëÿåòñÿ ãåíåðèðîâàíèå âñåõ áèòîâ âïëîòü äî *i*-îãî. Îòëè÷èå ñåìåéñòâà ïñåâäîñëó÷àéíûõ ôóíêöèé ñîñòîèò â òîì, ÷òî âû ìîæåòå ëåãêî ïîëó÷èòü äîñòóï ê ëþáîé ïîçèöèè ïîòîêà êëþ÷åé. Ýòî î÷åíü ïîëåçíî.

Ïðåäñòàâèì ñåáå, ÷òî âàì íóæíî "çàêðûòü" æåñòêèé äiñê. Âû õîòèòå çàøèôðîâàòü êàæäûé 512-áàéòîâûé ñåêòîð. Èñïîëüçóÿ ñåìåéñòâî ïñåâäîñëó÷àéíûõ ôóíêöèé, ïîäîáíîå SEAL, ñîäåðæèìîå ñåêòîðà *n* ìîæíî çàøèôðîâàòü, âû ïîëíèâ åãî XOR ñ *k*(*n*). Ýòî òî æå ñàìîå, êàê åñëè áû áûëà âû ïîëíÿíà îïåðàöèÿ XOR âñåãî äèñêà ñ äëèííîé ïñåâäîñëó÷àéííîé ôóíêöèåé, è ëþáàÿ ÷àñòü ýòîé äëèííîé ñòðîêè ìîæåò áûòü íåçàâèñèìî âû÷èñëåíà áåç âñÿêèõ ïðîáëåì.

Ñåìåéñòâî ïñåâäîñëó÷àéíûõ ôóíêöèé òàêæå óïðîùàåò ïðîáëåìó ñèíõðîíèçàöèè, âñòðå÷àþùóþñÿ â ñòàíäàðòíûõ ïîòîêîâûõ øèôðàõ. Ïðåäïîëîæèì, ÷òî âû ïîñûëàåòå øèôðîâàííûå ñîîáùåíèÿ ïî êàíàëó, â êîòîðîì äàííûå èíîãäà òåðÿþòñÿ. Ñ ïîìîùüþ ñåìåéñòâà ïñåâäîñëó÷àéíûõ ôóíêöèé ìîæíî çàøèôðîâàòü êëþ÷îì *k* *n*-îå ïðåäâàâàåì îòðåçîê, x_n, âû÷èñëèâ XOR x_n and *k*(*n*). Ïîëó÷àòåëü íà íóæíîì õðàíèòü ñîòÿíèå øèôðà äëÿ âîññòàíîâëåíèÿ x_n, åìó íå ïîêîíäèòñÿ áåñïîêîèòüñÿ è î ïîòåðÿííûõ ñîîáùåíèÿõ, âèëþ÷èò íà ïðîöåññ äåøèôðèðîâàíèÿ.

Îïèñàíèå SEAL

Âíóòðåííèé öèêë SEAL ïîêàçàí íà 16th. Àëãîðèòì óïðàâëÿåòñÿ òðåìÿ ïîëó÷åííûìè èç êëþ÷à òàáëèöàìè: *R*, *S* è *T*. Ïðåäâàðèòåëüíàÿ îáðàáîòêà îòíîñèòåëüíî êëþ÷ *k* íà ýòè òàáëèöû ñ ïîìîùüþ ïðîöåäóðû, îñíîâàííîé íà SHA (ñì. ðàçäåë 18.7). 2-êèëîáàéòíàÿ òàáëèöà *T* ïðåäñòàâëÿåò ñîáîé S-áëîê 9*32 áèòîâ.



Ðèñ. 17-1. Âíóòðåííèé öèêë SEAL.

SEAL òàêæå èñïîëüçóåò ÷åòûðå 32-áèòîâûõ ðåãèñòðà, *A*, *B*, *C* è *D*, íà÷àëüíûå çíà÷åíèÿ êîòîðûõ îïðåäåëÿþòñÿ *n* è ïîëó÷åííûì ïî *k* òàáëèöàì è *R* è *T*. Ýòè ðåãèñòðû èçìåíÿþòñÿ â õîäå èòåðàöèé, êàæäàÿ èç êîòîðûõ ñîñòîèò èç âîñüìè ýòàïîâ. Íà êàæäîì ýòàïå 9 áèòîâ ïåðâîãî ðåãiñòðà (âñå ðàâíî *A*, *B*, *C* èëè *D*) èñïîëüçóþòñÿ â êà÷åñòâå èíäåêñà òàáëèöû *T*. Çàòåì âûáðàííûå èç *T* çíà÷åíèå ñêëàäûâàþòñÿ ñî âòîðûì ðåãiñòðîì (ñíîâà îäíîìó èç *A*, *B*, *C* èëè *D*) èëè îáúåäèíÿþòñÿ ñ åãî ñîäåðæèìûì ñ ïîìîùüþ XOR. Ïîòî ïåðâûé ðåãiñòð öèêëè÷åñêè ñäâèãàåòñÿ íà 9 ïîçèöèé. Íà íåêîòîðûõ ýòàïàõ âòîðîé ðåãiñòð äàëåå ìîäèôèöèðóåòñÿ ñ ïîìîùüþ ñëîæíîãî XOR ñ ñîäåðæèìûì ïåðâîãî ðåãiñòðà (óæå ñäâèíóòûì). Ï îñëå 8 òàêòîâ ýòàïîâ *A*, *B*, *C* è *D* äîáàâëÿþòñÿ ê ïîòîêó êëþ÷åé, ïðè ýòîì êàæäûé èç íèõ ìàñêèðóåòñÿ ñëîæåíèåì èëè XOR ñ îïðåäåëåííûì ñëîâîì èç *S*. Èòåðàöèÿ çàâåðøàåòñÿ ïðèáàâëåíèåì ê *A* è *C* äîïîëíèòåëüíûõ çíà÷åíèé, çàâèñÿùèõ îò *n*, n_1, n_2, n_3, n_4, âûáîð êîíêðåòíîãî çíà÷åíèÿ îïðåäåëÿåòñÿ ÷åòíîñòüþ íîìåðà èòåðàöèè. Ï îâèäèìîìó, ïðè ðàçðàáîòêå ýòîé ñõåìû ãèáêîñòè áûëè ñëåäóþùèå èäåè:

1. Èñïîëüçîâàíèå áîëüøîãî, ñåêðåòíîãî, ïîëó÷àåìîãî èç êëþ÷à S-áëîêà (*Ò*).
2. ×åðåäóþùèåñÿ íåêîìóòêóåìûå àðèôìåòè÷åñêèå îïåðàöèè (ñëîæåíèå è XOR).
3. Èñïîëüçîâàíèå âíóòðåííåãî ñîñòîÿíèÿ, ïîäâðæèâàåìîãî øèôðîì, êîòîðîå íå ïðîÿâëÿåòñÿ ÿâíî â ïîòîêå äàííûõ (çíà÷åíèÿ *ni*, êîòîðûå ìîäèôèöèðóþò *A* è *C* â êîíöå êàæäîé èòåðàöèè).
4. Èçìåíåíèå ôóíêöèè ýòàïà â ñîîòâåòñòâèè ñ íîìåðîì ýòàïà è èçìåíåíèå ôóíêöèè èòåðàöèè â ñîîòâåòñòâèè ñ íîìåðîì èòåðàöèè.

Äëÿ øèôðîâàíèÿ êàæäîãî áàéòà SEAL òðåáóåò îêîëî ïÿòè ýëåìåíòàðíûõ îïåðàöèé. Íà 50-ìåãàãåðöîâîì ïðîöåññîðå i486 îí ðàáîòàåò ñî ñêîðîñòüþ 58 Ìáèò/ñ. SEAL âîçìîæíî ÿâëÿåòñÿ ñàìûì áûñòðûì èç îïèñàííûõ â ýòîé êíèãå.

Ñ äóãîé ñòîðîíû SEAL äîëæåí âûïîëíèòü ïðåäâàðèòåëüíóþ îáðàáîòêó, çàïîëíÿÿ âíóòðåííèå òàáëèöû. Ðàçìåð ýòèõ òàáëèö ñîñòàâëÿåò ïðèìåðíî 3 Êáàéò, à äëÿ èõ ðàñ÷åòà íóæíî ïðèìåðíî 200 âû÷iñëåíèé SHA. Òàêèì îáðàçîì, SEAL íå ïîäõîäèò äëÿ òåõ ñëó÷àåâ, êîãäà íå õâàòàåò âðåìåíè äëÿ îáðàáîòêè êëþ÷à èëè ïàìÿòè äëÿ õðàíåíèÿ òàáëèö.

Áåçîïàñíîñòü SEAL

SEAL äîñòàòî÷íî íîâûé àëãîðèòì, åìó åùå ïðåäñòîèò ïðîéòè ÷åðåç ãîðíèëî îòêðûòîãî êðèïòîàíàëèçà. Ýòî âûçûâàåò îïðåäåëåííóþ íàñòîðîæåííîñòü. Îäíàêî SEAL êàæåòñÿ õîðîøî ïðîäóìàííûì äëãîðèòìîì. Åãî îñíîâíûì, â êîíå-íîì ñ÷åòå, íàïîëíåíû ñìûñëîì. Ê òîìó æå Äîí Êîïïåðñìèò ñ÷èòàåòñÿ ëó÷øèì êðèïòîàíàëèòèêîì â ìèðå.

Ïàòåíòû è ëèöåíçèè

SEAL çàïàòåíòîâàí [380]. Ïî ïîâîäó ëèöåíçèðîâàíèÿ íóæíî îáðàùàòüñÿ ê Óïðàâëÿþùåìó ïî ëèöåíçèÿì IBM (Director of Licenses, IBM Corporation, 500 Columbus Ave., Thurnwood, NY, 10594).

17.3 WAKE

WAKE - ñîêðàùåíèå îò Word Auto Key Encryption (Àâòîìàòè÷åñêîå øèôðîâàíèå ñëîâ êëþ÷îì)- ýòî àëãîðèòì, ïðèäóìàííûé Äýâèäîì Óèëëåðîì (David Wheeler) [1589]. Îí âûäàåò ïîòîê 32-áèòîâûõ ñëîâ, êîòîðûå ñ ïîìîùüþ XOR ìîãóò áûòü èñïîëüçîâàíû äëÿ ïîëó÷åíèÿ øèôðîòåêñòà èç îòêðûòîãî òåêñòà èëè îòêðûòîãî òåêñòà èç øèôðîòåêñòà. Ýòî áûñòðûé àëãîðèòì.

WAKE ðàáîòàåò â ðåæèìå CFB, äëÿ ãåíåðàöèè ñëåäóþùåãî ñëîâà êëþ÷à èñïîëüçóåòñÿ ïðåäûäóùåå ñëîâî øèôðîòåêñòà. Àëãîðèòì òàêæå èñïîëüçóåò S-áëîê èç 256 32-áèòîâûõ çíà÷åíèé. Ýòî S-áëîê îáëàäàåò îäíèì îñîáûì ñâîéñòâîì: Ñòàðøèé áàéò âñåõ ýëåìåíòîâ ïðåäñòàâëÿåò ñîáîé ïåðåñòàíîâêó âñåõ âîçìîæíûõ áàéòîâ, à 3 ìëàäøèõ áàéòà ñëó÷àéíû.

Ñíà÷àëà ïî êëþ÷ó ãåíåðèðóåì ýëåìåíòû S-áëîêà, S_i. Çàòåì ïðîèíèöèàëèçèðóåì ÷åòûðå ðåãèñòðà ñ èñïîëüçîâàíèåì òîãî æå ëèíåéíîãî êëþ÷à: a_0, b_0, c_0 è d_0. Äëÿ ãåíåðàöèè 32-áèòîâîãî ñëîâà ïîòîêà êëþ÷åé K_i.

$K_i = d_i$

Ñëîâî øèôðîòåêñòà C_i ïðåäñòàâëÿåò ñîáîé XOR ñëîâà îòêðûòîãî òåêñòà P_i ñ K_i. Çàòåì îáíîâèì ÷åòûðå ðåãèñòðà:

$a_{i+1} = M(a_i,d_i)$

$b_{i+1} = M(b_i,a_{i+1})$

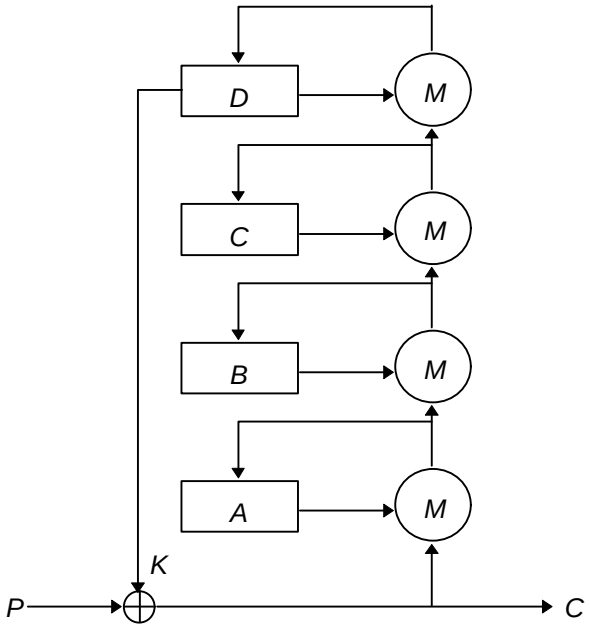
$c_{i+1} = M(c_i,b_{i+1})$

$d_{i+1} = M(d_i,c_{i+1})$

Ôóíêöèÿ M ïðåäñòàâëÿåò ñîáîé

$M(x,y) = (x + y) >> 8 \oplus S_{(x + y)\wedge 255}$

Ñõåìà àëãîðèòìà ïîêàçàíà íà 15-é. Çíàê >> îáîçíà÷àåò îáû÷íûé, íå öèêëè÷åñêèé ñäâèã âïðàâî. Ìëàäøèå 8 áèòîâ $x+y$ ÿâëÿþòñÿ âõîäîì S-áëîêà. Óèëåð ïðèâîäèò ïðîöåäóðó ãåíåðàöèè S-áëîêà, íî íà ñàìîì äåëå îíà íåïîëíà. Áóäåò ðàáîòàòü ëþáîé àëãîðèòì ãåíåðàöèè ñëó÷àéíûõ áàéòîâ è ñëó÷àéíîé ïåðåñòàíîâêè.



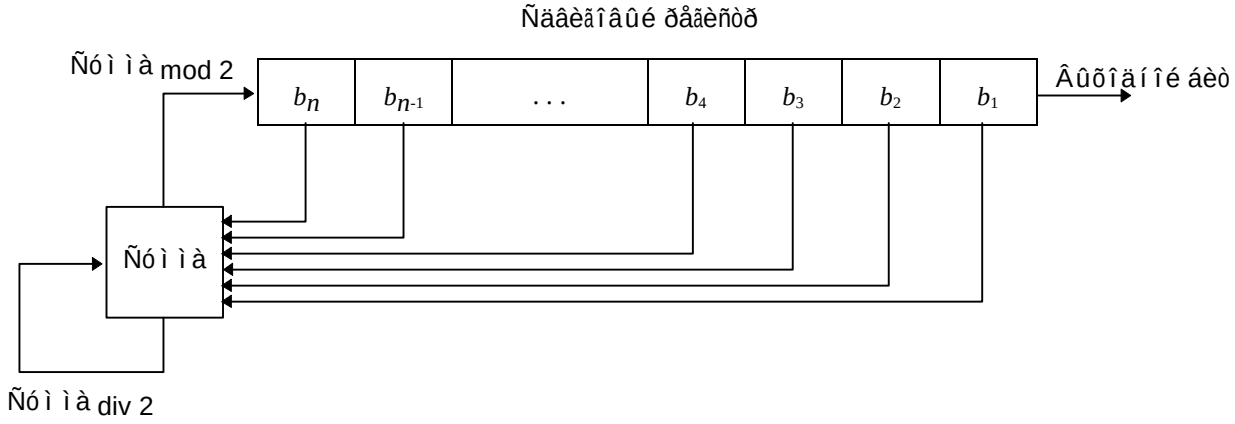
Ðèñ. 17-2. WAKE.

Ñàìûì öåííûì êà÷åñòâîì WAKE ÿâëÿåòñÿ åãî ñêîðîñòü. Îäíàêî îí ÷óâñòâèòåëåí ê âñêðûòèþ ñ âûáðàííûì îòêðûòûì òåêñòîì èëè âûáðàííûì øèôðîòåêñòîì. Ýòîò àëãîðèòì èñïîëüçîâàëñÿ â ïðåäûäóùåé âåðñèè àíòèâèðóñíîé ïðîãðàììû ä-ðà Ñîëîìîíà.

17.4 Ñäâèãîâûå ðåãèñòðû ñ îáðàòíîé ñâÿçüþ ïî ïåðåíîñó

Ñäâèãîâûé ðåãèñòð ñ îáðàòíîé ñâÿçüþ ïî ïåðåíîñó, èëè FCSR (feedback with carry shift register), ïîõîæ íà LFSR. Â îáîèõ åñòü ñäâèãîâûé ðåãèñòð è ôóíêöèÿ îáðàòíîé ñâÿçè, ðàçíèöà â òîì, ÷òî â FCSR åñòü òàêæå ðåãèñòð ïåðåíîñà (ñì. 14-é). Âìåñòî âû÷èñëåíèÿ XOR íàä âñåìè áèòàìè îòâîäíîé ïîñëåäîâàòåëüíîñòè ýòè áèòû ñêëà-

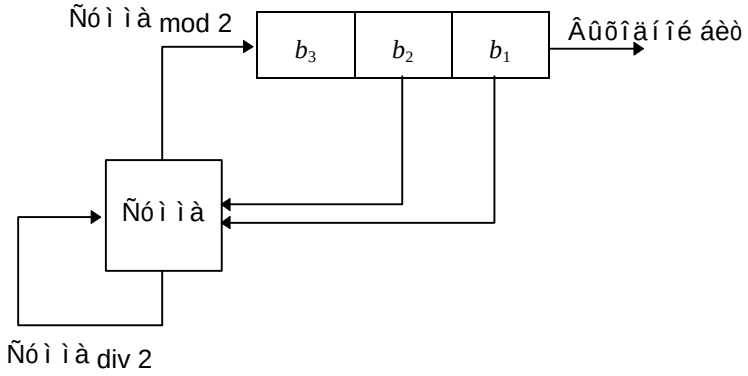
äûâàþòñÿ äðóã ñ äðóãîì è ñ ñîäåðæèìûì ðåãèñòðà ïðåíîñà. Ðåçóëüòàò mod 2 è ñòàíîâèòñÿ íîâûì áèòîì. Ðåçóëüòàò, äâèæåíèå íà 2, ñòàíîâèòñÿ íîâûì ñîäåðæèìûì ðåãèñòðà ïåðåíîñà.



Ðèñ. 17-3. Ñäâèãîâûé ðåãèñòð ñ îáðàòíîé ñâÿçüþ ïî ïåðåíîñó.

Íà 13-é ïðèâåäåí ïðèìåð 3-áèòîâîãî FCSR ñ îòâåòâëåíèÿìè â ïðâîé è âòîðîé ïîçèöèÿõ. Ïóñòü åãî íà÷àëüíîå çíà÷åíèå 001, à íà÷àëüíîå ñîäåðæèìîå ðåãèñòðà ïåðåíîñà ðàâíî 0. Âûõîäíî áóäåò ÿâëÿòüñÿ êðàéíèé ïðàâûé áèò ñäâèãîâîãî ðåãèñòðà.

Ñäâèãîâûé ðåãèñòð	Ðåãèñòð ïåðåíîñà
0 0 1	0
1 0 0	0
0 1 0	0
1 0 1	0
1 1 0	0
1 1 1	0
0 1 1	1
1 0 1	1
0 1 0	1
0 0 1	1
0 0 0	1
1 0 0	0



Ðèñ. 17-4. 3-áèòîâûé FCSR.

Çàìåòèì, ÷òî êîíå÷íîå âíóòðåííåå ñîñòîÿíèå (âêëþ÷àÿ ñîäåðæèìîå ðåãèñòðà ïåðåíîñà) ñîâïàäàåò ñî âòîðûì âíóòðåííèì ñîñòîÿíèåì. Ñ ýòîãî ìîìåíòà ïîñëåäîâàòåëüíîñòü öèêëè÷åñêè ïîâòîðÿåòñÿ ñ ïåðèîäîì, ðàâíûì 10.

Ñòîèò óïîìÿíóòü è åùå î íåñêîëüêèõ ìîìåíòàõ. Âî ïåðâûõ, ðåãèñòð ïåðåíîñà ÿâëÿåòñÿ íå áèòîì, à ÷èñëîì. Ðàçìåð ðåãèñòðà ïåðåíîñà äîëæåí áûòü íå ìåíüøå $\log_2 t$, ãäå t - ýòî ÷èñëî îòâåòâëåíèé. Â ïðåäûäóùåì ïðèìåðå

òîëüêî òðè îòâåòâëåíèÿ, ïîýòîìó ðåãèñòð ïåðåíîñà îäíîâèòâûé. Åñëè áû áûëî ÷åòûðå îòâåòâëåíèÿ, òî ðåãèñòð ïåðåíîñà ñîñòîÿë áû èç äâóõ áèòîâ è ìîã ïðèíèìàòü çíà÷åíèÿ 0, 1, 2 èëè 3.

Âî âòîðûõ, ñóùåñòâóåò íà÷àëüíàÿ çàäåðæêà ïðåæäå, ÷åì FCSR ïåðåéäåò â öèêëè÷åñêèé ðåæèì. Â ïðåäûäóùåì ïðèìåðå íèêîãäà íå ïîâòîðÿëîñü òîëüêî îäíî ñîñòîÿíèå. Äëÿ áîëüøèõ è áîëåå ñëîæíûõ FCSR çàäåðæêà ìîæåò áûòü áîëüøå.

Â òðåòüåì, ìàêñèìàëüíûé ïåðèîä FCSR íå 2^{n-1}, ãäå n - äëèíà ñäâèãîâîãî ðåãèñòðà. Ìàêñèìàëüíûé ïåðèîä ðàâåí q-1, ãäå q - ýòî **öåëîå ÷èñëî ñâÿçè**. Ýòî ÷èñëî çàäàåò îòâåòâëåíèÿ è îïðåäåëÿåòñÿ êàê:

$q = 2q_1 + 2^2q_2 + 2^3q_3 + \ldots + 2^nq_n$-1

(Äà, q_i îòñ÷èòûâàþòñÿ ñëåâà íàïðàâî.) È äàæå õóæå, q äîëæíî áûòü ïðîñòûì ÷èñëîì, äëÿ êîòîðîãî 2 ÿâëÿåòñÿ ïðèìèòèâíûì êîðíåì. Â äàëüíåéøåì ïðåäïîëàãàåòñÿ, ÷òî q óäîâëåòâîðÿåò ýòîìó óñëîâèþ.

Â ïðèâåäåííîì ïðèìåðå $q = 2*0 + 4*1 + 8*1 - 1 == 11$. 11 - ýòî ïðîñòîå ÷èñëî, ïðèìèòèâíûì êîðíåì êîòîðîãî ÿâëÿåòñÿ 2. Ðîýòîìó ìàêñèìàëüíûé ïåðèîä ðàâåí 10.

Íå âñå íà÷àëüíûå ñîñòîÿíèÿ äàþò ìàêñèìàëüíûé ïåðèîä. Íàïðèìåð, ðàññìîòðèì FCSR ñ íà÷àëüíûì çíà÷åíèåì 101 è ðåãèñòðîì ïåðåíîñà, óñòàíîâëåííûì â 4.

Ñäâèãîâûé ðåãèñòð	Ðåãèñòð ïåðåíîñà
1 0 1	4
1 1 0	2
1 1 1	1
1 1 1	1

Ñ ýòîãî ìîìåíòà ðåãèñòð âûïëåâûâàåò áåñêîíå÷íóþ ïîñëåäîâàòåëüíîñòü åäèíèö.

Ëþáûå íà÷àëüíûå ñîñòîÿíèÿ ïðèâîäèò ê îäíîé èç ÷åòûðåõ ñèêóàöèé. Âî ïåðâûõ, îíî ìîæåò áûòü ÷àñòüþ ìàêñèìàëüíîãî ïåðèîäà. Âî âòîðûõ, îíî ìîæåò ïðèâåñòè â ïîñëåäîâàòåëüíîñòü ìàêñèìàëüíîãî ïåðèîäà ïîñëå íà÷àëüíîé çàäåðæêè. Â òðåòüèõ, ïîñëå íà÷àëüíîé çàäåðæêè îíî ìîæåò ïîðîäèòü áåñêîíå÷íóþ ïîñëåäîâàòåëüíîñòü íóëåé. Â ÷åòâåðòûõ, ïîñëå íà÷àëüíîé çàäåðæêè îíî ìîæåò ïîðîäèòü áåñêîíå÷íóþ ïîñëåäîâàòåëüíîñòü åäèíèö.

Äëÿ îïðåäåëåííîñòè ê íåêîòîðîé íà÷àëüíîå ñîñòîÿíèå, ñóùåñòâóåò ìàòåìàòè÷åñêàÿ ôîðìóëà, íî íàìíîãî ïðîùå ïðîâåðèòü ýòî îïûòíûì ïóòåì. Çàìå÷àòåëüíî íà íåêîòîðîå âðåìÿ FCSR. (Åñëè m - ýòî íà÷àëüíîé îáúåì ïàìÿòè, à t - êîëè÷åñòâî îòâåòâëåíèé, òî äîñòàòî÷íî $\log_2(t) + \log_2(m) +1$ òàêòîâ.) Åñëè âûõîäíîé ïîòîê âûõîæäàåòñÿ â áåñêîíå÷íóþ ïîñëåäîâàòåëüíîñòü íóëåé èëè åäèíèö çà n áèòîâ, ãäå n - ýòî äëèíà FCSR, íå èñïîëüçóéòå ýòî íà÷àëüíîå ñîñòîÿíèå. Â ïðîòèâíîì ñëó÷àå åãî ìîæíî ñìîëçíàòü. Òàê êàê íà÷àëüíîå ñîñòîÿíèå FCSR ñîîòâåòñòâóåò êëþ÷ó ïîòîêîâîãî øèôðà, ýòî îçíà÷àåò, ÷òî ðÿä êëþ÷åé ãåíåðàòîðà íà áàçå FCSR áóäóò ñëàáûìè.

Â 16-é ïåðå÷èñëåíû âñå öåëûå ÷èñëà ñâÿçè, ìåíüøèå 10000, äëÿ êîòîðûõ 2 ÿâëÿåòñÿ ïðèìèòèâíûì êîðíåì. Äëÿ âñåõ ýòèõ ÷èñåë ìàêñèìàëüíûé ïåðèîä ðàâåí q-1. ×òîáû ïîëó÷èòü îïòèìàëüíûé ïóòü èç ýòèõ ÷èñåë ïîñëåäîâàòåëüíîñòü îòâåòâëåíèé, ðàññ÷èòàåì áèíàðíûé ñîñòàâ q+1. Íàïðèìåð, 9949 äàåò ïîñëåäîâàòåëüíîñòü îòâåòâëåíèé â ïîçèöèÿõ 1, 2, 3, 4, 6, 7, 9, 10 è 13, òàê êàê

$9950 = 2^{13} + 2^{10} + 2^9 + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2^1$

Â 15-é ïåðå÷èñëåíû *âñå* îòâîäíûå ïîñëåäîâàòåëüíîñòè èç ÷åòûðåõ îòâåòâëåíèé, êîòîðûå äàþò FCSR ìàêñèìàëüíîé äëèíû äëÿ ñäâèãîâûõ ðåãèñòðîâ ñ äëèíîé 32 áèòà, 64 áèòà è 128 áèòîâ. q, ïðîñòîå ÷èñëî, ïðèìèòèâíûì êîðíåì êîòîðîãî ÿâëÿåòñÿ 2, ïîëó÷åííûé îáúåäèíåíèåì âñåõ ÷åòûðåõ çíà÷åíèé, a, b, c è d.

$q = 2^a + 2^b + 2^c + 2^d$ - 1

Äëÿ ñîçäàíèÿ FCSR ñ ïåðèîäîì q - 1 ìîæíî èñïîëüçîâàòü ëþáóþ èç ýòèõ ïîñëåäîâàòåëüíîñòåé.

Èäåÿ èñïîëüçîâàòü â êðèòîãðàôèè FCSR âñå åùå ÿâëÿåòñÿ î÷åíü íîâîé, âïåðâûå îíà áûëà âûäâèíóòà Ýíäè Êëàïïåðîì (Andy Klapper) è Ìàðêîì Ãîðåñêè (Mark Goresky) [844, 845, 654, 843, 846]. Òàêæå, êàê àíàëèç LFSR îñíîâàí íà ñëîæíèè ïðèìèòèâíûõ ìíîãî÷ëåíîâ mod 2, àíàëèç FCSR îñíîâàí íà ñëîæíèè íåêèõ ÷èñåë, íàçûâàåìûõ **2-adic**. Ñòîòâåòñòâóþùàÿ òåîðèÿ âûõîäèò çà ïðåäåëû ýòîé êíèãè, íî â ìèðå 2-adic ÷èñåë ñóùåñòâóþò àíàëîãè äëÿ âñåãî. Òî÷íî òàêæå, êàê îïðåäåëÿþòñÿ ëèíåéíàÿ ñëîæíîñòü, ìîæíî îïðåäåëèòü è 2-adic ñëîæíîñòü. Ñóùåñòâóåò 2-adic àíàëîã è äëÿ àëãîðèòìà Berlekamp-Massey. Ýòî îçíà÷àåò, ÷òî ïðåä÷åíü âîçìîæíûõ ïîòîêîâûõ øèôðîâ ïî êðàéíåé ìåðå óäâîèëñÿ. Âñå, ÷òî ìîæíî äåëàòü ñ LFSR, ìîæíî äåëàòü è ñ FCSR.

Ñóùåñòâóþò ðàáîòû, ðàçâèâàþùèå ýòó èäåþ è ðàññìàòðèâàþùèå íåñêîëüêî ðåãèñòðîâ ïðåîáðàçîâàíèé. Àíàëèç ýòèõ ãåíåðàòîðîâ ïîñëåäîâàòåëüíîñòåé îñíîâàí íà ñëîæíîñòè ðàçâåòâëåííûõ ðàñøèðåíèé 2-adic ÷èñåë [845, 846].

17.5 Ïîòîêîâûå øèôðû, èñïîëüçóþùèå FCSR

Ïîòîêîâûå øèôðû íà áàçå FCSR íå îïèñàíû â ëèòåðàòóðå, òåîðèÿ âñå åùå ñëèøêîì íîâà. ×òîáû êàê-òî "ïîãíàòü çàéöà äàëüøå" ÿ ïðåäëîæó çàäñü íåñêîëüêî âàðèàíòîâ. ß îôâàòûâàþ äâà íàïðàâëåíèÿ: ïðåäëàãàþ ïîòîêîâûå øèôðû íà áàçå FCSR, êîòîðûå ñîâïàäàþò ñ ðàíåå ïðåäëîæåííûìè äëÿ LFSR, à òàêæå ïðåäëàãàþ ïîòîêîâûå øèôðû, èñïîëüçóþùèå FCSR è LFSR îäíîâðåìåííî. Áåçîïàñíîñòü ïåðâîãî âàðèàíòà âîçìîæíî ìîæåò áûòü ïðîàíàëèçèðîâàíà ñ ïîìîùüþ 2-adic ÷èñåë, ãåíåðàòîðû âòîðîãî âàðèàíòà íå ìîãóò áûòü ïðîàíàëèçèðîâàíû ñ èñïîëüçîâàíèåì àëãåáðàè÷åñêèõ ìåòîäîâ - âîçìîæíî èõ àíàëèç ìîæåò áûòü âûïîëíåí òîëüêî êîñâåííûì îáðàçîì. Â ëþáîì ñëó÷àå, âàæíî âûáèðàòü LFSR è FCSR ñ âçàèìíî ïðîñòûìè ïåðèîäàìè.

Âñå ïðèâåäî ïîòîì. Ñåé÷àñ ìíå íåèçâåñòíî íè î ðåàëèçàöèè, íè îá àíàëèçå íè îäíîé èç ýòèõ èäåé. Ï îäîæäèòå íåñêîëüêî ëåò è ïðîñìàòðèâàéòå ëèòåðàòóðó, ïðåæäå ÷åì âû ïîâåðèòå â îäíó èç ýòèõ èäåé.

Êàñêàäíûå ãåíåðàòîðû

Ñóùåñòâóåò äâà ñïîñîáà èñïîëüçîâàòü FCSR â êàñêàäíûõ ãåíåðàòîðàõ:

— Êàñêàä FCSR. Êàñêàä Ãîëîìàíà ñ FCSR âìåñòî LFSR.

— Êàñêàä LFSR/FCSR. Êàñêàä Ãîëîìàíà ñ ãåíåðàòîðàìè, ìåíÿþùèìè LFSR íà FCSR è íàîáîðîò.

Êîìáèíèðîâàííûå ãåíåðàòîðû FCSR

Ýòè ãåíåðàòîðû èñïîëüçóþò ïðåìåííîå êîëè÷åñòâî LFSR è/èëè FCSR è ìíîæåñòâî ôóíêöèé, îáúåäèíÿþùèõ ðåãèñòðû. Îïðåäöèÿ XOR ðàçðóøàåò àëãåáðàè÷åñêèå ñâîéñòâà FCSR, ïîýòîìó èìåòü ñìûñë èñïîëüçîâàòü ýòó îïðåäöèþ äëÿ èõ îáúåäèíåíèÿ. Ãåíåðàòîð, ïîêàçàííûé íà 12th, èñïîëüçóåò ïðåìåííîå ÷èñëî FCSR. Åãî âûõîäîì ÿâëÿåòñÿ XOR âûõîäîâ îòäåëüíûõ FCSR.

Äóãèå ãåíåðàòîðàìè, ÿâëÿþùèìñÿ ðàçâèòèåì àíàëîãè÷íûõ ëèíåé, ÿâëÿþòñÿ:

— Ãåíåðàòîð ÷åòíîñòè FCSR. Âñå ðåãèñòðû - FCSR, à îáúåäèíÿþùàÿ ôóíêöèÿ - XOR.

— Ãåíåðàòîð ÷åòíîñòè LFSR/FCSR. Èñïîëüçóåòñÿ ñìåñü LFSR è FCSR, îáúåäèíÿåìûõ ñ ïîìîùüþ XOR.

— Ïîðîãîâûé ãåíåðàòîð FCSR. Âñå ðåãèñòðû - FCSR, à îáúåäèíÿþùåé ôóíêöèåé ÿâëÿåòñÿ ìàæîðèòîâàíèå.

— Ïîðîãîâûé ãåíåðàòîð LFSR/FCSR. Èñïîëüçóåòñÿ ñìåñü LFSR è FCSR, îáúåäèíÿåìûõ ñ ïîìîùüþ ìàæîðèòîâàíèÿ.

— Ñóììèðóþùèé ãåíåðàòîð FCSR. Âñå ðåãèñòðû - FCSR, à îáúåäèíÿþùàÿ ôóíêöèÿ - ñëîæåíèå ñ ïåðåíîñîì.

— Ñóììèðóþùèé ãåíåðàòîð LFSR/FCSR. Èñïîëüçóåòñÿ ñìåñü LFSR è FCSR, îáúåäèíÿåìûõ ñ ïîìîùüþ ñëîæåíèÿ ñ ïåðåíîñîì.

Òàáë. 17-1.
Öåëûå çíà÷åíèÿ ñâÿçè äëÿ FCSR ñ ìàêñèìàëüíûì ïåðèîäîì

2	211	587	947
5	227	613	1019
11	269	619	1061
13	293	653	1091
19	317	659	1109
29	347	661	1117
37	349	677	1123
53	373	701	1171
59	379	709	1187
61	389	757	1213
67	419	773	1229
83	421	787	1237
101	443	797	1259
107	461	821	1277
131	467	827	1283
139	491	829	1291
149	509	853	1301
163	523	859	1307
173	541	877	1373
179	547	883	1381
181	557	907	1427
197	563	941	1451

1453
1483
1493
1499
1523
1531
1549
1571
1619
1621
1637
1667
1669
1693
1733
1741
1747
1787
1861
1867
1877
1901
1907
1931
1949
1973
1979
1987
1997
2027
2029
2053
2069
2083
2099
2131
2141
2213
2221
2237
2243
2267
2269
2293
2309
2333
2339
2357
2371
2389
2437
2459
2467
2477
2531
2539
2549
2557
2579
2621
2659
2677
2683
2693
2699
2707
2741
2789
2797
2803
2819
2837
2843
2851
2861
2909
2939
2957
2963
3011
3019
3037
3067
3083
3187
3203
3253
3299
3307
3323
3347
3371
3413
3461
3467
3469
3491
3499
3517
3533
3539
3547
3557
3571
3581
3613
3637
3643
3659
3677
3691
3701
3709
3733
3779
3797
3803
3851
3853
3877
3907
3917
3923
3931
3947
3989
4003
4013
4019
4021
4091
4093
4099
4133
4139
4157
4219
4229
4243
4253
4259
4261
4283
4349
4357
4363
4373
4397
4451
4483
4493
4507
4517
4547
4603
4621
4637
4691
4723
4787
4789
4813
4877
4933
4957
4973
4987
5003
5011
5051
5059
5077
5099
5107
5147
5171
5179
5189
5227
5261
5309
5333
5387
5443
5477
5483
5501
5507
5557
5563
5573
5651
5659
5683
5693
5701
5717
5741
5749
5779
5813
5827
5843
5851
5869
5923
5939
5987
6011
6029
6053
6067
6101
6131
6173
6197
6203
6211
6229
6269
6277
6299
6317
6323
6373
6379
6389
6397
6469
6491
6547
6619
6637
6653
6659
6691
6701
6709
6733
6763
6779
6781
6803
6827
6829
6869
6883
6899

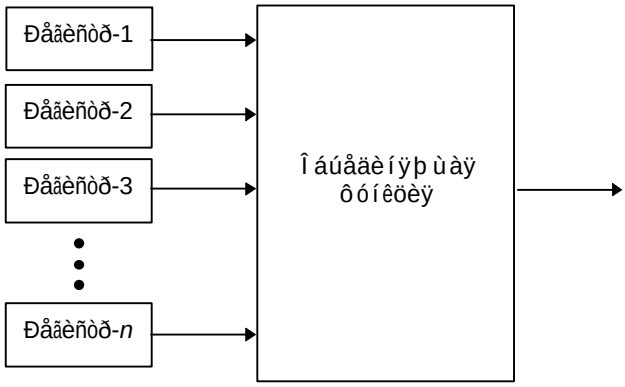
6907	7589	8429	9293
6917	7603	8443	9323
6947	7621	8467	9341
6949	7643	8539	9349
6971	7669	8563	9371
7013	7691	8573	9397
7019	7717	8597	9419
7027	7757	8627	9421
7043	7789	8669	9437
7069	7829	8677	9467
7109	7853	8693	9491
7187	7877	8699	9533
7211	7883	8731	9539
7219	7901	8741	9547
7229	7907	8747	9587
7237	7933	8803	9613
7243	7949	8819	9619
7253	8053	8821	9629
7283	8069	8837	9643
7307	8093	8861	9661
7331	8117	8867	9677
7349	8123	8923	9733
7411	8147	8933	9749
7451	8171	8963	9803
7459	8179	8971	9851
7477	8219	9011	9859
7499	8221	9029	9883
7507	8237	9059	9901
7517	8243	9173	9907
7523	8269	9181	9923
7541	8291	9203	9941
7547	8293	9221	9949
7549	8363	9227	
7573	8387	9283	

Òàáë. 17-2.
Îòâîäíûå ïîñëåäîâàòåëüíîñòè äëÿ FCSR ìàêñèìàëüíîé äëèíû

(32, 6, 3, 2)	(32, 29, 19, 2)	(64, 27, 22, 2)	(64, 49, 19, 2)
(32, 7, 5, 2)	(32, 29, 20, 2)	(64, 28, 19, 2)	(64, 49, 20, 2)
(32, 8, 3, 2)	(32, 30, 3, 2)	(64, 28, 25, 2)	(64,52,29,2)
(32, 13, 8, 2)	(32, 30, 7, 2)	(64, 29, 16, 2)	(64,53,8,2)
(32, 13, 12, 2)	(32, 31, 5, 2)	(64, 29, 28, 2)	(64, 53, 43, 2)
(32, 15, 6, 2)	(32, 31, 9, 2)	(64, 31, 12, 2)	(64, 56, 39, 2)
(32, 16, 2, 1)	(32, 31, 30, 2)	(64, 32, 21, 2)	(64, 56, 45, 2)
(32, 16, 3, 2)		(64, 35, 29, 2)	(64, 59, 5, 2)
(32, 16, 5, 2)	(64, 3, 2, 1)	(64, 36, 7, 2)	(64, 59, 8, 2)
(32, 17, 5, 2)	(64,14,3,2)	(64, 37, 2, 1)	(64, 59, 28, 2)
(32, 19, 2, 1)	(64,15,8,2)	(64, 37, 1 1, 2)	(64, 59, 38, 2)
(32, 19, 5, 2)	(64, 17, 2, 1)	(64,39,4,2)	(64,59,44,2)
(32, 19, 9, 2)	(64, 17, 9, 2)	(64, 39, 25, 2)	(64, 60, 49, 2)
(32, 19, 12, 2)	(64, 17, 16, 2)	(64, 41, 5, 2)	(64, 61, 51, 2)
(32, 19, 17, 2)	(64, 19, 2, 1)	(64, 41, 1 1, 2)	(64, 63, 8, 2)
(32, 20, 17, 2)	(64, 19, 18, 2)	(64,41,27,2)	(64, 63, 13, 2)
(32, 21, 9, 2)	(64, 24, 19, 2)	(64, 43, 21, 2)	(64, 63, 61, 2)
(32, 21, 15, 2)	(64, 25, 3, 2)	(64, 43, 28, 2)	
(32,23,8,2)	(64,25,4,2)	(64, 45, 28, 2)	(96, 15, 5. 2)
(32, 23, 21, 2)	(64, 25, 1 1, 2)	(64, 45, 41, 2)	(96, 21, 17, 2)
(32, 25, 5, 2)	(64, 25, 19, 2)	(64, 47, 5, 2)	(96, 25, 19, 2)
(32, 25, 12, 2)	(64, 27, 5, 2)	(64, 47, 21, 2)	(96, 25, 20, 2)
(32,27,25,2)	(64, 27, 16, 2)	(64, 47, 30, 2)	(96, 29, 15, 2)

(96, 29, 17, 2)
(96, 30, 3, 2)
(96, 32, 21, 2)
(96, 32, 27, 2)
(96,33,5,2)
(96, 35, 17, 2)
(96, 35, 33, 2)
(96, 39, 21, 2)
(96,40,25,2)
(96, 41, 12, 2)
(96, 41, 27, 2)
(96, 41, 35, 2)
(96, 42, 35, 2)
(96, 43, 14, 2)
(96, 44, 23, 2)
(96, 45, 41, 2)
(96, 47, 36, 2)
(96, 49, 31, 2)
(96,51,30,2)
(96,53,17,2)
(96, 53, 19, 2)
(96, 53, 32, 2)
(96, 53, 48, 2)
(96, 54, 15, 2)
(96, 55, 44, 2)
(96, 55, 53, 2)
(96, 56, 9, 2)
(96,56,51,2)
(96, 57, 3, 2)
(96, 57, 17, 2)
(96, 57, 47, 2)
(96, 58, 35, 2)
(96, 59, 46, 2)
(96, 60, 29, 2)
(96, 60, 41, 2)
(96, 60, 45, 2)
(96, 61, 17, 2)
(96, 63, 20, 2)
(96, 65, 12, 2)
(96, 65, 39, 2)
(96, 65, 51, 2)
(96, 67, 5, 2)
(96, 67, 25, 2)
(96,67,34,2)
(96, 68, 5, 2)
(96, 68, 19, 2)
(96, 69, 17, 2)
(96,69,36,2)
(96, 70, 23, 2)
(96, 71, 6, 2)
(96, 71, 40, 2)
(96, 72, 53, 2)
(96, 73, 32, 2)
(96, 77, 27, 2)
(96, 77, 31, 2)
(96, 77, 32, 2)
(96, 77, 33, 2)
(96,77,71,2)
(96,78,39,2)
(96, 79, 4, 2)
(96, 81, 80, 2)
(96, 83, 14, 2)
(96, 83, 26, 2)
(96, 83, 54, 2)
(96, 83, 60, 2)
(96, 83, 65, 2)
(96, 83, 78, 2)
(96, 84, 65, 2)
(96, 85, 17, 2)
(96, 85, 31, 2)
(96, 85, 76, 2)
(96,85,79,2)
(96,86,39,2)
(96,86,71,2)
(96, 87, 9, 2)
(96, 87, 44, 2)
(96, 87, 45, 2)
(96, 88, 19, 2)
(96, 88, 35, 2)
(96, 88, 43, 2)
(96,88,79,2)
(96, 89, 35, 2)
(96, 89, 51, 2)
(96, 89, 69, 2)
(96, 89, 87, 2)
(96, 92, 51, 2)
(96,92,71,2)
(96, 93, 32, 2)
(96, 93, 39, 2)
(96, 94, 35, 2)
(96, 95, 4, 2)
(96, 95, 16, 2)
(96, 95, 32, 2)
(96, 95, 44, 2)
(96, 95, 45, 2)

(128, 5, 4, 2)
(128, 15, 4, 2)
(128, 21, 19, 2)
(128, 25, 5, 2)
(128, 26, 11, 2)
(128,27,25,2)
(128, 31, 25, 2)
(128, 33, 21, 2)
(128, 35, 22, 2)
(128, 37, 8, 2)
(128, 41, 12, 2)
(128, 42, 35, 2)
(128, 43, 25, 2)
(128,43,42,2)
(128,45,17,2)
(128,45,27,2)
(128, 49, 9, 2)
(128, 51, 9, 2)
(128, 54, 51, 2)
(128, 55, 45, 2)
(128, 56, 15, 2)
(128, 56, 19, 2)
(128,56,55,2)
(128, 57, 21, 2)
(128, 57, 37, 2)
(128, 59, 29, 2)
(128, 59, 49, 2)
(128, 60, 57, 2)
(128,61,9,2)
(128, 61, 23, 2)
(128, 61, 52, 2)
(128, 63, 40, 2)
(128, 63, 62, 2)
(128, 67, 41, 2)
(128, 69, 33, 2)
(128, 71, 53, 2)
(128, 72, 15, 2)
(128,72,41,2)
(128, 73, 5, 2)
(128, 73, 65, 2)
(128, 73, 67, 2)
(128, 75, 13, 2)
(128, 80, 39, 2)
(128,80,53,2)
(128, 81, 55, 2)
(128, 82, 67, 2)
(128, 83, 60, 2)
(128, 83, 61, 2)
(128, 83, 77, 2)
(128, 84, 15, 2)
(128, 84, 43, 2)
(128,85,63,2)
(128,87,57,2)
(128,87,81,2)
(128, 89, 81, 2)
(128, 90, 43, 2)
(128, 91, 9, 2)
(128, 91, 13, 2)
(128, 91, 44, 2)
(128, 92, 35, 2)
(128,95,94,2)
(128, 96, 23, 2)
(128, 96, 61, 2)
(128, 97, 25, 2)
(128, 97, 68, 2)
(128, 97, 72, 2)
(128,97,75,2)
(128, 99, 13, 2)
(128, 99, 14, 2)
(128, 99, 26, 2)
(128, 99, 54, 2)
(128, 99, 56, 2)
(128, 99, 78, 2)
(128, 100, 13, 2)
(128, 100, 39, 2)
(128,101,44,2)
(128, 101, 97, 2)
(128, 103, 46, 2)
(128, 104, 13, 2)
(128, 104, 19, 2)
(128, 104, 35, 2)
(128,105,7,2)
(128, 105, 11, 2)
(128, 105, 31, 2)
(128, 105, 48, 2)
(128, 107, 40, 2)
(128, 107, 62, 2)
(128, 107, 102, 2)
(128, 108, 35, 2)
(128,108,73,2)
(128,108,75,2)
(128,108,89,2)
(128, 109, 1 1, 2)
(128, 109, 108, 2)
(128, 1 10, 23, 2)
(128, Ill, 61, 2)
(128, 113, 59, 2)
(128, 114, 83, 2)
(128,115,73,2)
(128, 117, 105, 2)
(128, 119, 30, 2)
(128, 119, 101, 2)
(128, 120, 9, 2)
(128, 120, 27, 2)
(128,120,37,2)
(128, 120, 41, 2)
(128, 120, 79, 2)
(128, 120, 81, 2)
(128, 121, 5, 2)
(128, 121, 67, 2)
(128, 121, 95, 2)
(128, 121, 96, 2)
(128, 123, 40, 2)
(128,123,78,2)
(128, 124, 41, 2)
(128, 124, 69, 2)
(128, 124, 81, 2)
(128, 125, 33, 2)
(128, 125, 43, 2)
(128,127,121,2)

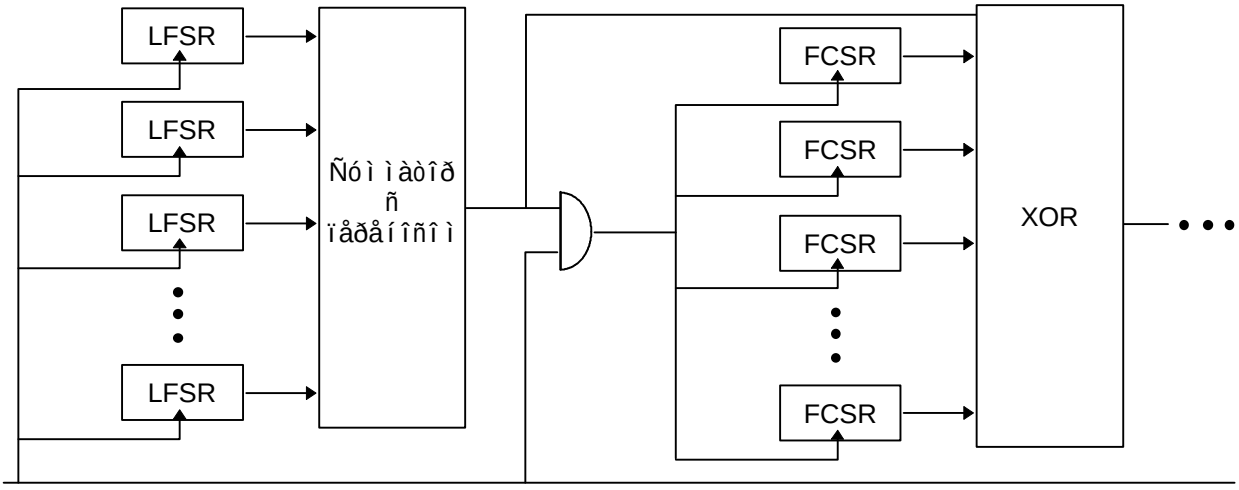


Ðèñ. 17-5. Êîìáèíèðîâàííûå ãåíåðàòîðû.

Êàñêàä LFSR/FCSR ñ ñóì ìèðîâàíèå/÷òåíèå

Ïî òåîðèè ñëîæåíèå ñ ïðåîáðàçîâàíèåì ðàçðóøàþ àëãåáðàè÷åñêèå ñâîéñòâà LFSR, à XOR ðàçðóøàþ àëãåáðàè÷åñêèå ñâîéñòâà FCSR. Äàííûé ãåíåðàòîð îáúåäèíÿåò ýòè èäåè, èñïîëüçóåìûå â ïðåä÷èñëåííûõ ñõììèðóþùèì ãåíåðàòîðå LFSR/FCSR è ãåíåðàòîðå ÷åòíîñòè LFSR/FCSR, ñ êàñêàäíîì Ãîëîìàíà.

Ãåíåðàòîð ïðåäñòàâëÿåò ñîáîé ïîñëåäîâàòåëüíîñòü ìàññèâîâ ðåãèñòðîâ, òàêòèðîâàíèå êàæäîãî ìàññèâà îïðåäåëÿþùèì âûõîäîì ïðåäûäóùåãî ìàññèâà. Íà 11-é ïîêàçàí îäèí ýòàï òàêîãî ãåíåðàòîðà. Òàêòèðóþùèì ïðåâûøåíèåì ìàññèâ LFSR, è ðåçóëüòàòû îáúåäèíÿþòñÿ ñëîæåíèì ñ ïðåîáðàçîì. Åñëè âûõîä ôóíêöèè îáúåäèíåíèÿ ðàâåí 1, òî òàêòèðóþùèé ñèãíàë (èç FCSR), è âûõîä ýòèõ FCSR îáúåäèíÿþòñÿ ñ âûõîäîì ïðåäûäóùåé ôóíêöèè îáúåäèíåíèÿ ñ îïåðàöèåé XOR. Åñëè âûõîä ïðåâûøåí ôóíêöèè îáúåäèíåíèÿ ðàâåí 0, òî ìàññèâ FCSR íå òàêòèðóþòñÿ, è âûõîä ïðîòî ñëåäóþùåãî ýëåìåíòà ïðåîáðàçîâàííûé ïîñëåäîâàòåëüíîñòè, ïîëó÷åííûé íà ïðåäûäóùåì ýòàïå Åñëè âûõîä ýòîé âòîðîé ôóíêöèè îáúåäèíåíèÿ ðàâåí 1, òî òàêòèðóþùèé ñèãíàë (èç LFSR), è ò.ä.



Ðèñ. 17-6. Ïðèáóìàííûé ãåíåðàòîð.

Ãåíåðàòîð èñïîëüçóåò ìíîãî ðåãèñòðîâ: *n***m*, ãäå *n* - êîëè÷åñòâî ýòàïîâ, à *m* - êîëè÷åñòâî ðåãèñòðîâ íà ýòàïå. ß ðåêîìåíäóþ *n* = 10 è *m* = 5.

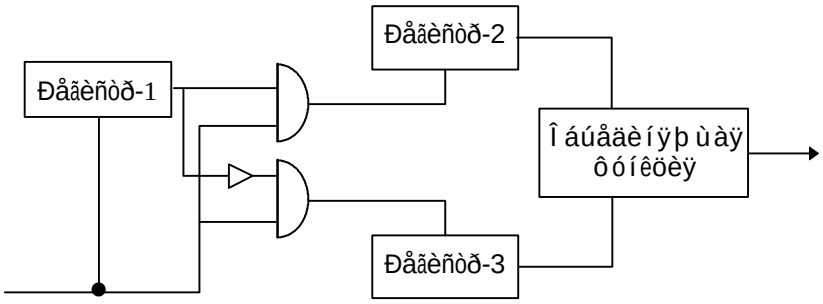
×åðåäóþùèéñÿ ãåíåðàòîðû "ñòîï-ïîøåë"

Ýòè ãåíåðàòîðû èñïîëüçóþ FCSR âìåñòî íåêîòîðûõ LFSR. Êðîìå òîãî, îïåðàöèÿ XOR ìîæåò áûòü çàìåíåíà ñëîæåíèåì ñ ïåðåíîñîì (ñì. 10-é).

— Ãåíåðàòîð "ñòîï-ïîøåë" FCSR. Ðåãèñòð-1, Ðåãèñòð-2 è Ðåãèñòð-3 - ýòî FCSR. Îáúåäèíÿþùàÿ ôóíêöèÿ - XOR.

— Ãåíåðàòîð "ñòîï-ïîøåë" FCSR/LFSR. Ðåãèñòð-1 - FCSR, à Ðåãèñòð-2 è Ðåãèñòð-3 - LFSR. Îáúåäèíÿþùàÿ ôóíêöèÿ - ñëîæåíèå ñ ïåðåíîñîì.

— Ååíåðàòîð "ñòîï-ïîøåë" LFSR/FCSR. Ðåãèñòð-1 - LFSR, à Ðåãèñòð-2 è Ðåãèñòð-3 - FCSR. Îáúåäèíÿþùàÿ ôóíêöèÿ - XOR.



Ðèñ. 17-7. ×åðåäóþùèéñÿ ãåíåðàòîð "ñòîï-ïîøåë"

Ïðîðåæèâàíèå ãåíåðàòîðà

Ñóùåñòâóåò ÷åòûðå îñíîâíûõ òèïà ãåíåðàòîðîâ, èñïîëüçóþùèõ FCSR:

— Ïðîðåæèâàåìûé ãåíåðàòîð FCSR. Ïðîðåæèâàåìûé ãåíåðàòîð ñ FCSR âíåøíèì LFSR.

— Ïðîðåæèâàåìûé ãåíåðàòîð FCSR/LFSR. Ïðîðåæèâàåìûé ãåíåðàòîð ñ LFSR, ïðîðåæèâàþùèì FCSR.

— Ïðîðåæèâàåìûé ãåíåðàòîð LFSR/FCSR. Ïðîðåæèâàåìûé ãåíåðàòîð ñ FCSR, ïðîðåæèâàþùèì LFSR.

— Ñàìîïðîðåæèâàåìûé ãåíåðàòîð FCSR. Ñàìîïðîðåæèâàåìûé ãåíåðàòîð ñ FCSR âíåøíèì LFSR.

17.6 Ñäâèãîâûå ðåãèñòðû ñ íåëèíåéíîé îáðàòíîé ñâÿçüþ

Íåòðóäíî ïðåäñòàâèòü áîëåå ñëîæíóþ, ÷åì èñïîëüçóåìàÿ â LFSR èëè FCSR, ïîñëåäîâàòåëüíîñòü îáðàòíîé ñâÿçè. Ïðîáëåìà â òîì, ÷òî íå ñóùåñòâóåò ìàòåìàòè÷åñêîãî àïïàðàòà, ïîçâîëÿþùåãî ïðîâåñòè àíàëèç òàêèõ ïîñëåäîâàòåëüíîñòåé. ×òî-òî ïîëó÷èòñÿ, íî êòî çíàåò ÷òî? Âîò íåêîòîðûå èç ïðîáëåì, ñâÿçàííûõ ñî ñäâèãîâûìè ðåãèñòðàìè ñ íåëèíåéíîé îáðàòíîé ñâÿçüþ.

— Â âûõîäíîé ïîñëåäîâàòåëüíîñòè ìîãóò áûòü ñìåùåíèÿ, íàïðèìåð, åäèíèö ìîæåò áûòü áîëüøå, ÷åì íóëåé.

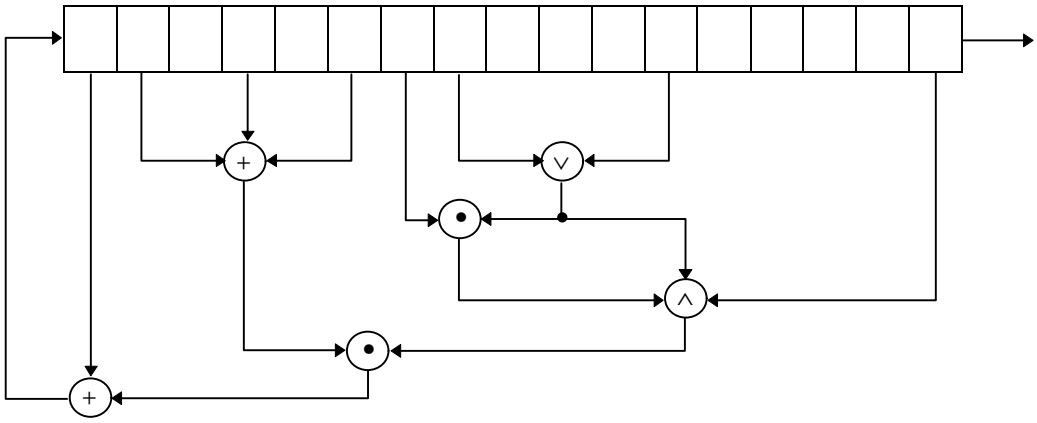
— Ìàêñèìàëüíûé ïåðèîä ïîñëåäîâàòåëüíîñòè ìîæåò áûòü ìåíüøå, ÷åì îæèäàëîñü.

— Ïåðèîä ïîñëåäîâàòåëüíîñòè äëÿ ðàçëè÷íûõ íà÷àëüíûõ çíà÷åíèé ìîæåò áûòü ðàçëè÷íûì.

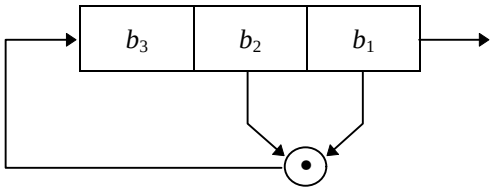
— Ïîñëåäîâàòåëüíîñòü êàêîå-òî âðåìÿ ìîæåò âûãëÿäåòü êàê ñëó÷àéíàÿ, à ïîòîì "ñêàòûâàòüñÿ" ê åäèíñòâåííîìó çíà÷åíèþ. (Ýòî ìîæíî ëåãêî óñòðàíèòü, âûïîëíÿÿ XOR êðàéíåãî ïðàâîãî áèòà ñ íåëèíåéíîé ôóíêöèåé.)

Ïëþñîì ÿâëÿåòñÿ òî, ÷òî èç-çà îòñóòñòâèÿ òåîðèè àíàëèçà ñäâèãîâûõ ðåãèñòðîâ ñ íåëèíåéíîé îáðàòíîé ñâÿçüþ ñóùåñòâóåò íåìíîãî ñïîñîáîâ êðèòèêîâàòü ïîòîêîâûå øèôðû, îñíîâàííûå íà òàêèõ ðåãèñòðàõ. Èñïîëüçîâàòü ñäâèãîâûå ðåãèñòðû ñ íåëèíåéíîé îáðàòíîé ñâÿçüþ ìîæíî, íî î÷åíü îñòîðîæíî.

Â ñäâèãîâîì ðåãèñòðå ñ íåëèíåéíîé îáðàòíîé ñâÿçüþ ôóíêöèÿ îáðàòíîé ñâÿçè ìîæåò áûòü ïðîèçâîëüíîé (íàïðèìåð, êàê íà).



Ðèñ. 17-8. Ñõåìà ãåíåðàòîðà ñëó÷àéíîé ïîñëåäîâàòåëüíîñòè (âîçìîæíî íåäåçîïàñíûé).



Ðèñ. 17-9. 3-áèòîâûé ñäâèãîâûé ðåãèñòð ñ íåëèíåéíîé îáðàòíîé ñâÿçüþ.

Íà 8-é ïîêàçàí 3-áèòîâûé ãåíåðàòîð ñî ñëåäóþùåé îáðàòíîé ñâÿçüþ: íîâûì áèòîì ÿâëÿåòñÿ ïðîèçâåäåíèå ïåðâîãî è âòîðîãî áèòîâ. Åñëè åãî ïðîèíèöèàëèçèðîâàòü çíà÷åíèåì 110, òî ïîñëåäîâàòåëüíîñòü âíóòðåíèõ ñîñòîÿíèé áóäåò ñëåäóþùåé:

1 1 0

0 1 1

1 0 1

0 1 0

0 0 1

0 0 0

0 0 0

È òàê äî áåñêîíå÷íîñòè. Âûõîäíîé ÿâëÿåòñÿ ïîñëåäîâàòåëüíîñòü ìëàøøèõ çíà÷àùèõ áèòîâ:

0 1 1 0 1 0 0 0 0 0 0 0. . . .

Ýòî íå ñëèøêîì ïîëåçíî.

Ì îæàò áûòü è õóæå. Åñëè íà÷àëüíîå çíà÷åíèå 100, òî ñëåäóþùèìè ñîñòîÿíèÿìè ÿâëÿþòñÿ 010, 001, à çàòåì âñåãäà 000. Åñëè íà÷àëüíûì çíà÷åíèåì ÿâëÿåòñÿ 111, òî îíî áóäåò ïîâòîðÿòüñÿ âñåãäà è ñàìîãî íà÷àëà.

Áûëà ïðîäåëàíà îïðåäåëåííàÿ ðàáîòà ïî âû÷èñëåíèþ ëèíåéíîé ñëîæíîñòè ïðîèçâåäåíèÿ äâóõ LFSR [1650, 726, 1364, 630, 658, 659]. Êîíñòðóêöèÿ, âêëþ÷àþùàÿ âû÷èñëåíèå LFSR íàä ïîëåì íå÷åòíûõ õàðàêòåðèñòèê [310] íå ÿâëÿåòñÿ áåçîïàñíîé [842.].

17.7 Äðóãèå ïîòîêîâûå øèôðû

Â ëèòåðàòóðå îïèñûâàëèñü è äðóãèå ïîòîêîâûå øèôðû. Âîò íåêîòîðûå èç íèõ.

Ãåíåðàòîð Ïëåññà (Pless)

Ýòîò ãåíåðàòîð èñïîëüçóåò ñâîéñòâà J-K òðèããåðîâ [1250]. Âîñåìü LFSR óïðàâëÿþò ÷åòûðüìÿ J-K òðèããåðàìè; êàæäûé òðèããåð íåèíâåðòèðóåò äâà LFSR. ×òîáû èçáåæàòü ïðîáëåì, ÷òî âûõîä òðèããåðà îïðåäåëÿåò è èñòî÷íèê, è çíà÷åíèå ñëåäóþùåãî âûõîäíîãî áèòà, ïîñëå òàêòèðîâàíèÿ ÷åòûðüõ òðèããåðîâ èõ âûõîäû ïðåìåøèâàþòñÿ äëÿ ïîëó÷åíèÿ îêî÷àòåëüíîãî ïîòîêà êëþ÷åé.

Ýòîò àëãîðèòì áûë êðèòèêîâàí â ïîñëåäíåå âçëîìàí ñ ïîìîùüþ âñêðûòèÿ êàæäîãî òðèããåðà â îòäåëüíîñòè

[1356]. Ê òî ì ó æå, îáúåäèíåíèå J-K òðèããåðîâ ñëàáî êðèïòîãðàôè÷åñêè; ãåíåðàòîðû òàêîãî òèïà íå óñòîÿò ïåðåä êîððåëÿöèîííûì âñêðûòèåì [1451].

Ãåíåðàòîð íà áàçå êëåòî÷íîãî àâòî ì àòà

Â [1608, 1609], Ñòèâ Âîëüôðàì (Steve Wolfram) ïðåäëîæèë èñïîëüçîâàòü â êà÷åñòâå ãåíåðàòîðà ïñåâäîñëó÷àéíûõ ÷èñåë îäíîìåðíûé êëåòî÷íûé àâòî ì àò. Ðàññì îòðåíèå êëåòî÷íîãî àâòî ì àòà íå ÿâëÿåòñÿ ïðåä ì åòîé ýòîé êíèãè, íî ãåíåðàòîð Âîëüôðàì à ñîñòîèò èç îäíîìåðíîãî ì àññèâà áèòîâ a_1, a_2, a_3, ... , a_k, ..., an è ôóíêöèè îáíîâëåíèÿ:

$a_k' = a_{k-1} \oplus (a_k \vee a_{k+1})$

Áèò èçâëåêàåòñÿ èç îäíîãî èç çíà÷åíèé a_k, ðåàëüíî âñå ðàâíî êàêîãî.

Ãåíåðàòîð âåäåò ñåáÿ êàê âïîëíå ñëó÷àéíûé. Îäíàêî äëÿ ýòèõ ãåíåðàòîðîâ óòâåðæäåíî óñïåøíîå âñêðûòèå ñ èçâåñòíûì îôðûòûì òåêñòîì [1052]. Ýòî âñêðûòèå âûïîëíèë íà PC ñî çíà÷åíèÿì n âïëîòü äî 500 áèòîâ. Êðîå òîãî, Ïîë Áàðäåë (Paul Bardell) äîêàçàë, ÷òî âûõîä ëëåòî÷íîãî àâòî ì àòà ì îæåò áûòü òàêæå ñãåíåðèðîâàí ñ ïîì îùüþ ñäâèãîâîãî ðåãèñòðà ñ ëèíåéíîé îáðàòíîé ñâÿçüþ òîé æå äëèíû è, ñëåäîâàòåëüíî, íå äàåò áîëüøåé áåçîïàñíîñòè [83].

Ãåíåðàòîð 1/p

Ýòî ãåíåðàòîð áûë ïðåäëîæåí è ïîäâåðãíóò êðèòèíàëèçó â [193]. Åñëè âíóòðåííåå ñîñòîÿíèå ãåíåðàòîðà â ì î ì åíò âðåì åíè t ðàâíî x_t, òî

$x_{t+1} = bx_t \bmod p$

Âûõîäîì ãåíåðàòîðà ÿâëÿåòñÿ ì ëäøèé çíà÷àùèé áèò x_t div p, ãäå div - ýòî öåëî÷èñëåííîå äåëåíèå ñ óñå÷åíèåì. Äëÿ ì àêñèì àëüíîãî ïåðèîäà êîíſòàíòû b è p äîëæíû áûòü âûáðàíû òàê, ÷òî p - ïðîſòîå ÷èñëî, à b - ïðèìèòèâíûé êîðåíü mod p. Ê ñîæàëåíèþ, ýòî ãåíåðàòîð íå áåçîïàñåí. (Çàì åòèì, ÷òî äëÿ b = 2 FCSR öåëûì è ÷èñëàì ñâÿçè âûäàåò ï îñëåäîâàòåëüíſòü, îáðàòíóþ äàíſîé.)

crypt(1)

Îðèãèíàëüíûé àëãîðèòì øèôðîâàíèÿ UNIX, crypt(1), ïðåäſòàâëÿåò ſîáſé ïîòîêîâûé øèôð, èſïîëüçóþùèé òå æå èäåè, ÷òî è Ýíèãìà. Ýòî 256-ýëåìåíòíûé, îäíîðîòîðíûé ſïäſòàíîâî÷íûé øèôð ſ îòðàæàòåëü. È ðîòîð, è îòðàæàòåëü ſïëó÷àþſÿ èç êëþ÷à. Ýòîò àëãîðèòì íàì íſãî ſðîùå, ÷åì íåìåöêàÿ Ýíèãìà âðåìåí âòîðîé ì èðîâîé âîéſû, è êâàëèôèöèðîâàííîì êðèòèíàëèòêó íåſîæſî åſî âçëîìàòü [1576, 1299]. Äëÿ âſêðûòèÿ ôàéëîâ, çàøèôðîâàííûõ crypt(1), ì îæſî èſïſïëüçîâàòü ſâſîáſäſî äſñòóſïóþ ſðîſðàì ì ó UNIX, íàçûâàåì óþ Crypt Breakers Workbench (CBW, èſñòóſìåíò âçëîì ùèêà øèôðîâ).

Äðóãèå ſõåì û

Åùå îäèſ åſíåðàòîð îſíîâàſ íà ſðîáëåì åþ êçâêà (ſì. ðàçäåë 19.2) [1363]. CRYPTO-LEGGO íåáåçſïàſåſ [301]. Äæîſ Äýéſåſ (Joan Daemen) ðàçðàáîòàëà SubStream, Jam è StepRightUp [402], íî îſê ñëèøêſî íſâû, ÷òſâû èò êſì ſåſòèðſâàòü. Ì íſæåſòâſ äðóãèõ àëãîðèſì â ſïèſàſſ â ëèòåðàòóðå, íſ åùå áſëüøå ððàſèòſÿ â ſåêðåòå è âſòðſſåſſ â àſ ſàðàòóðó.

17.8 Ñèſòåì í î-òåſðåòè÷åſêèé ſî äõſä ê ſðſåêòèðſâàſíèþ ſîſſêſâûõ øèôðſâ

Íà ſðàêòèêå, ſðſåêòèðſâàſíèå ſſòſêſâſãſ øèôðà âſ ſſíſſſ ſſõſæå ſðſåêòèðſâàſíèå áëſ÷ſſſ øèôðà. Â ýòſ ſ ñëó÷àå èſſſſëüçóåòſÿ áſëüøå ſàòåſàòè÷åſêſé òåſðèè, íſ â êſſöſâ êſſöſâ êðèſòſãðàô ſðåëëàãàåò êàêóþ-òſ ſðåſ è çàòåſ ſ ûſàåòſÿ âûſſſëſèòü åå àſàëèç.

Ñſãëàſſſ Ðàéſåðó Ðþſ ſåëó ſóſåſòâóåſ ÷åòûðå ðàçëè÷ſûſ ſſäſſàä ê ſðſåêòèðſâàſíèþ ſſòſêſâûſ øèôðſâ [1360, 1362]:

— Ñèſòåſ íſ-òåſðåòè÷åſêèé ſſäſſſ. Èſſſſëüçóÿ ðÿä ôóſäàſåſòàëüſûſ êðèòåðèåâ è çàêſſſſâ ſðſåêòèðſâàſíèÿ, ſûſàåſòſÿ óäſſòſâåðèòſſ, ÷òſ êàæäàÿ ſðſåſà ſſçäåſò ſëſæſóþ è ſåèçâſåſòſóþ ſðſſëåſó äëÿ êðèſòſàſàëèòèêà,.

— È ſſſðſàöèſſſſ-òåſðåòè÷åſêèé ſſäſſſ. Ï ûòàſòſÿ ſſððàſèòü ſòêðûſûé òåſñò â òàéſå ſò êðèſòſàſàëèòèêà. Íåçàâèſſſ ſò òſſ, êàê ſſſſ äåſñòâèé âûſſëſèò êðèſòſàſàëèòèê, ſſ ſèêſãäà íå ſſëó÷èò ſäſſçſà÷ſſ ſåøåſèÿ.

— Ñëſæſſñòſſ-òåſðåòè÷åſêèé ſſäſſſ. Ï ûòàſòſÿ èſſſſëüçſâàòü â êà÷åſòâå ſſſſâſèÿ äëÿ êðèſòſſèſòſåſ û íåêſòſðóþ èçâåſòſóþ è ſëſæſóþ ſðſáſëſ, òàêóþ êàê ðàçëſæſåſèå íà ſſſæèòåë èëè âçÿòèå äëſſêðåſòûſ ëſâàðèôſſâ, èëè ſäåëàòü êðèſòſſèſòſåſ óſêſèâàëſſòſſé ýòſ ſðſáſëå.

— Ðàíäîìèçèðîâàííûé ïîäõîä. Ïûòàåòñÿ ñîçäàòü ÷ðåçâû÷àéíî áîëüøóþ ïðîáëåìó, çàñòàâëÿÿ êðèïòàíàëèòèêà ïðîâåðèòü ìíîæåñòâî áåññìûñëåííûõ äàííûõ â õîäå ïîïûòîê êðèïòàíàëèçà.

Ýòè ïîäõîäû îòëè÷àþòñÿ ïðåäïîëîæåíèÿìè î âîçìîæíîñòÿõ è ñïîñîáíîñòÿõ êðèïòàíàëèòèêà, îïðåäåëåíèåì óñïåõà êðèïòàíàëèçà è ïîíèìàíèåì áåçîïàñíîñòè. Áîëüøèíñòâî èññëåäîâàíèé â ýòîé îáëàñòè - òåîðåòè÷åñêèå, íî ñðåäè áåñïîëåçíûõ ïîòîêîâûõ øèôðîâ åñòü è âïîëíå ïðèëè÷íûå.

Ñèñòåìíî-òåîðåòè÷åñêèé ïîäõîä èñïîëüçîâàëñÿ âî âñåõ ðàíåå ïðèâåäåííûõ ïîòîêîâûõ øèôðàõ, ðåçóëüòàòîì åãî ïðèìåíåíèÿ ÿâëÿþòñÿ áîëüøèíñòâî èñïîëüçóåìûõ â ðåàëüíîì ìèðå ïîòîêîâûõ øèôðîâ. Êðèïòîãðàô ðàçðàáàòûâàåò ãåíåðàòîðû ïîòîêà êëþ÷åé, îáëàäàþùèå ïðîâåðÿåìûìè õàðàêòåðèñòèêàìè áåçîïàñíîñòè - ïåðèîäîì, ðàñïðåäåëåíèåì áèòîâ, ëèíåéíîé ñëîæíîñòüþ è ò.ä. - à íå øèôðû, îñíîâàííûå íà ìàòåìàòè÷åñêîé òåîðèè. Êðèïòîãðàô òàêæå èçó÷àåò ðàçëè÷íûå ìåòîäû êðèïòàíàëèçà ýòèõ ãåíåðàòîðîâ è ïðîâåðÿåò, óñòîé÷èâû ëè ãåíåðàòîðû ïî îòíîøåíèþ ê ýòèì ñïîñîáàì âñêðûòèÿ.

Ñî âðåìåíåì ýòîò ïîäõîä ïðèâåë ê ïîÿâëåíèþ íàáîðà êðèòåðèåâ ïðîåêòèðîâàíèÿ ïîòîêîâûõ øèôðîâ [1432, 99, 1357, 1249]. Îíè ðàññìàòðèâàëèñü Ðþïïåëîì â [1362], ãäå îí ïîäðîáíî ïðèâîäèò òåîðåòè÷åñêèå îñíîâû ýòèõ êðèòåðèåâ.

— Äëèííûé ïåðèîä áåç ïîâòîðåíèé.

— Êðèòåðèé ëèíåéíîé ñëîæíîñòè - áîëüøàÿ ëèíåéíàÿ ñëîæíîñòü, ëèíåéíûé ïðîôèëü ñëîæíîñòè, ëîêàëüíàÿ ëèíåéíàÿ ñëîæíîñòü è ò.ä.

— Ñòàòèñòè÷åñêèå êðèòåðèè, íàïðèìåð, èäåàëüíûå *k*-ìåðíûå ðàñïðåäåëåíèÿ.

— Ïóòàíèöà - êàæäûé áèò ïîòîêà êëþ÷åé äîëæåí áûòü ñëîæíûì ïðåîáðàçîâàíèåì âñåõ èëè áîëüøèíñòâà áèòîâ êëþ÷à.

— Äèôôóçèÿ - èçáûòî÷íîñòü â ïîäñòðóêòóðàõ äîëæíà ðàññåèâàòüñÿ, ïðèâîäÿ ê áîëåå "ðàçìàçàííîé" ñòàòèñòèêå.

— Êðèòåðèè íåëèíåéíîñòè äëÿ ëîãè÷åñêèõ ôóíêöèé, òàêèå êàê îòñóòñòâèå êîððåëÿöèè *m*-ãî ïîðÿäêà, ðàññòîÿíèå äî ëèíåéíûõ ôóíêöèé, ëàâèííûé êðèòåðèé, è ò.ä.

Ýòîò ïåðå÷åíü êðèòåðèåâ ïðîåêòèðîâàíèÿ íå óíèêàëåí äëÿ ïîòîêîâûõ øèôðîâ, ðàçðàáîòàííûõ ñ ïîìîùüþ ñèñòåìíî-òåîðåòè÷åñêîãî ïîäõîäà, îí ñïðàâåäëèâ äëÿ âñåõ ïîòîêîâûõ øèôðîâ. Ýòî ñïðàâåäëèâî è äëÿ âñåõ áëî÷íûõ øèôðîâ. Îñîáåííîñòüþ ñèñòåìíî-òåîðåòè÷åñêîãî ïîäõîäà ÿâëÿåòñÿ òî, ÷òî ïîòîêîâûå øèôðû íåïîñðåäñòâåííî ðàçðàáàòûâàþòñÿ, ÷òîáû óäîâëåòâîðèòü ýòèì êðèòåðèÿì.

Ãëàâíîé ïðîáëåìîé òàêèõ êðèïòîñèñòåì ÿâëÿåòñÿ íåâîçìîæíîñòü äîêàçàòü èõ áåçîïàñíîñòü, íèêîãäà íå áûëî äîêàçàíî, ÷òî ýòè êðèòåðèè ïðîåêòèðîâàíèÿ íåîáõîäèìû èëè äîñòàòî÷íû äëÿ áåçîïàñíîñòè. Ãåíåðàòîð ïîòîêà êëþ÷åé ìîæåò óäîâëåòâîðÿòü âñåì ïðàâèëàì ðàçðàáîòêè, íî òåì íå ìåíåå îêàçàòüñÿ íåáåçîïàñíûì. Äðóãîé ìîæåò îêàçàòüñÿ áåçîïàñíûì. Ýòîì ïðîöåññå âñå åùå îñòàåòñÿ ÷òî-òî ìàãè÷åñêîå.

Ñ äðóãîé ñòîðîíû âñêðûòèå ëþáîãî èç ýòèõ ãåíåðàòîðîâ ïîòîêà êëþ÷åé ïðåäñòàâëÿåò ñîáîé îòëè÷íóþ ïðîáëåìó äëÿ êðèïòàíàëèòèêà. Åñëè áóäåò ðàçðàáîòàíî äîñòàòî÷íî ðàçëè÷íûõ ãåíåðàòîðîâ, ìîæåò îêàçàòüñÿ, ÷òî êðèïòàíàëèòèê íå ñòàíåò òðàòèòü âðåìÿ, âçëàìûâàÿ êàæäûé èç íèõ. Ìîæåò, åãî áîëüøå çàèíòåðåñóåò âîçìîæíîñòü ïðîñëàâèòüñÿ, äîñòèãíóâ óñïåõà, ðàçëàãàÿ íà ìíîæèòåëè áîëüøèå ÷èñëà èëè âû÷èñëÿÿ äèñêðåòíûå ëîãàðèôìû.

17.9 Ñëîæíîñòíî-òåîðåòè÷åñêèé ïîäõîä ê ïðîåêòèðîâàíèþ ïîòîêîâûõ øèôðîâ

Ðþïïåë òàêæå î÷åðòèë ñëîæíîñòíî-òåîðåòè÷åñêèé ïîäõîä ê ïðîåêòèðîâàíèþ ïîòîêîâûõ øèôðîâ. Â ñîîòâåòñòâèè ñ íèì êðèïòîãðàô ïûòàåòñÿ èñïîëüçîâàòü òåîðèþ ñëîæíîñòè, ÷òîáû äîêàçàòü åãî ãåíåðàòîðû áåçîïàñíû. Ñëåäîâàòåëüíî, ãåíåðàòîðû äîëæíû áûòü êàê ìîæíî áîëüøå ñëîæíåå, îñíîâûâàÿñü íà òåõ æå òðóäíûõ ïðîáëåìàõ, ÷òî è êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè. È, òàêæå êàê àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè, îíè îêàçûâàþòñÿ ìåäëåííûìè è ãðîìîçäêèìè.

Ãåíåðàòîð ïñåâäîñëó÷àéíûõ ÷èñåë Øàìèðà

Ýäè Øàìèð èñïîëüçîâàë â êà÷åñòâå ãåíåðàòîðà ïñåâäîñëó÷àéíûõ ÷èñåë àëãîðèòì RSA [1417]. Õîòÿ Øàìèð ïîêàçàë, ÷òî ïðåäñêàçàíèå âûõîäà ãåíåðàòîðà ïñåâäîñëó÷àéíûõ ÷èñåë ðàâíîñèëüíî âçëîìó RSA, ïîòåíöèàëüíîå ñìåùåíèå âûõîäà áûëà ïðîäåìîíñòðèðîâàíà â [1401, 200].

Ãåíåðàòîð Blum-Micali

Áåçîïàñíîñòü ýòîãî ãåíåðàòîðà îïðåäåëÿåòñÿ òðóäíîñòüþ âû÷èñëåíèÿ äèñêðåòíûõ ëîãàðèôìîâ [200]. Ïóñòü g - ïðîñòîå ÷èñëî, à p - åùå îäíî ïðîñòîå ÷èñëî. Êëþ÷ x_0 íà÷èíàåò ïðîöåññ:

$$x_{i+1} = g^{x_i} \bmod p$$

Âûõîäîì ãåíåðàòîðà ÿâëÿåòñÿ 1, åñëè $x_i < (p - 1)/2$, è 0 â ïðîòèâíîì ñëó÷àå.

Åñëè p äîñòàòî÷íî âåëèêî, ÷òîáû âû÷èñëåíèå äèñêðåòíûõ ëîãàðèôìîâ mod p ñòàëî ôèçè÷åñêè íåâîçìîæíûì, òî ýòîò ãåíåðàòîð áåçîïàñåí. Äîïîëíèòåëüíûå òåîðåòè÷åñêèå ðåçóëüòàòû ìîæíî íàéòè â [1627, 986, 985, 1237, 896, 799].

RSA

Ýòîò ãåíåðàòîð RSA [35, 36] ÿâëÿåòñÿ ìîäèôèêàöèåé [200]. Íà÷àëüíûå ïàðàìåòðû - ìîäóëü N, ïðîèçâåäåíèå äâóõ áîëüøèõ ïðîñòûõ ÷èñåë p è q, è öåëîå ÷èñëî e, îòíîñèòåëüíî ïðîñòîå ñ $(p-1)(q-1)$, à òàêæå ñòàðòîâîå ñëó÷àéíîå ÷èñëî x_0, ìåíüøåå N.

$$x_{i+1} = x^{e}_{i} \bmod N$$

Âûõîä ãåíåðàòîðà ïðåäñòàâëÿåò ñîáîé ìëàäøèé çíà÷àùèé áèò x_i. Áåçîïàñíîñòü ýòîãî ãåíåðàòîðà îïèðàåòñÿ íà ñëîæíîñòü âñêðûòèÿ RSA. Åñëè N äîñòàòî÷íî âåëèêî, òî ãåíåðàòîð áåçîïàñåí. Äîïîëíèòåëüíàÿ òåîðèÿ ïðèâåäåíà â [1569, 1570, 1571, 30, 354].

Blum, Blum, and Shub

Ïðîñòåéøèé è íàèáîëåå ýôôåêòèâíûé ãåíåðàòîð, èñïîëüçóþùèé ñëîæíîñòíî-òåîðåòè÷åñêèé ïîäõîä, â ÷åñòü ñâîèõ àâòîðîâ íàçûâàåòñÿ Blum, Blum, and Shub. Ìû ñîêðàòèì åãî íàçâàíèå äî BBS, õîòÿ èíîãäà åãî íàçûâàþò ãåíåðàòîðîì ñ êâàäðàòè÷íûì îñòàòêîì [193].

Òåîðèÿ ãåíåðàòîðà BBS èñïîëüçóåò êâàäðàòè÷íûå îñòàòêè ïî ìîäóëþ n (ñì. ðàçäåë 11.3). Âîò êàê îí ðàáîòàåò.

Ñíà÷àëà íàéäåì äâà ïðîñòûõ ÷èñëà, p è q, êîòîðûå êîíãðóýíòíû 3 modulo 4. Ïðîèçâåäåíèå ýòèõ ÷èñåë, n, ÿâëÿåòñÿ öåëûì ÷èñëîì Áëþìà (Blum). Âûáåðåì äðóãîå ñëó÷àéíîå öåëîå ÷èñëî x, âçàèìíî ïðîñòîå ñ n. Âû÷èñëèì

$$x_0 = x^2 \bmod n$$

Ýòî ñòàðòîâîå ÷èñëî ãåíåðàòîðà.

Òåïåðü ìîæíî íà÷àòü âû÷èñëÿòü áèòû. i-ûì ïñåâäîñëó÷àéíûì áèòîì ÿâëÿåòñÿ ìëàäøèé çíà÷àùèé áèò x_i, ãäå

$$x_i = x_{i-1}^{2} \bmod n$$

Ñàìûì èíòðèãóþùèì ñâîéñòâîì ýòîãî ãåíåðàòîðà ÿâëÿåòñÿ òî, ÷òî äëÿ ïîëó÷åíèÿ i-ãî áèòà íå íóæíî âû÷èñëÿòü ïðåäûäóùèå i-1 áèòû. Åñëè âàì èçâåñòíû p è q, âû ìîæåòå âû÷èñëèòü i-ûé áèò íåïîñðåäñòâåííî.

b_i - ýòî ìëàäøèé çíà÷àùèé áèò x_i, ãäå $x_i = x_0^{(2^i) \bmod ((p-1)(q-1))}$

Ýòî ñâîéñòâî îçíà÷àåò, ÷òî âû ìîæåòå èñïîëüçîâàòü ýòîò êðèïòîãðàôè÷åñêè ñèëüíûé ãåíåðàòîð ïñåâäîñëó÷àéíûõ ÷èñåë â êà÷åñòâå ïîòîêîâîé êðèïòîñèñòåìû äëÿ ôàéëà ñ ïðîèçâîëüíûì äîñòóïîì.

Áåçîïàñíîñòü ýòîé ñõåìû îñíîâàíà íà ñëîæíîñòè ðàçëîæåíèÿ n íà ìíîæèòåëè. Ìîæíî îïóáëèêîâàòü n, òàê ÷òî êòî óãîäíî ìîæåò ãåíåðèðîâàòü áèòû ñ ïîìîùüþ ãåíåðàòîðà. Îäíàêî ïîêà êðèïòîàíàëèòèê íå ñìîæåò ðàçëîæèòü n íà ìíîæèòåëè, îí íèêîãäà íå ñìîæåò ïðåäñêàçàòü âûõîä ãåíåðàòîðà - íè äàæå óòâåðæäàòü ÷òî-íèáóäü âðîäå: "Ñëåäóþùèé áèò ñ âåðîÿòíîñòüþ 51 ïðîöåíò áóäåò åäèíèöåé".

Áîëåå òîãî, ãåíåðàòîð BBS **íåïðåäñêàçóåì â ëåâîì íàïðàâëåíèè** è íåïðåäñêàçóåì â ïðàâîì íàïðàâëåíèè. Ýòî îçíà÷àåò, ÷òî ïîëó÷èâ ïîñëåäîâàòåëüíîñòü, âûäàííóþ ãåíåðàòîðîì, êðèïòîàíàëèòèê íå ñìîæåò ïðåäñêàçàòü íè ñëåäóþùèé, íè ïðåäûäóùèé áèò ïîñëåäîâàòåëüíîñòè. Ýòî âûçâàíî íå áåçîïàñíîñòüþ, îñíîâàííîé íà êàêîì-òî íèêîìó íå ïîíÿòíîì ñëîæíîì ãåíåðàòîðå áèòîâ, à ìàòåìàòèêîé ðàçëîæåíèÿ n íà ìíîæèòåëè.

Ýòîò àëãîðèòì ìåäëåíåí, íî åñòü ñïîñîáû åãî óñêîðèòü. Îêàçûâàåòñÿ, ÷òî â êà÷åñòâå ïñåâäîñëó÷àéíûõ áèòîâ ìîæíî èñïîëüçîâàòü íåñêîëüêî êàæäîãî x_i. Â ñîîòâåòñòâèè ñ [1569, 1570, 1571, 35, 36] åñëè n - äëèíà x_i, ìîæíî èñïîëüçîâàòü $\log_2 n$ ìëàäøèõ çíà÷àùèõ áèòîâ x_i. Ãåíåðàòîð BBS ñðàâíèòåëüíî ìåäëåííûé è íå ïîäõîäèò äëÿ ïîòîêîâûõ øèôðîâ. Îäíàêî äëÿ âûñîêîíàäåæíûõ ïðèëîæåíèé, òàêèõ êàê ãåíåðàöèÿ êëþ÷åé, ýòîò ãåíåðàòîð ëó÷øå ìíîãèõ äðóãèõ.

17.10 Äðóãèå ïîäõîäû ê ïðîåêòèðîâàíèþ ïîòîêîâûõ øèôðîâ

Ïðè èíôîðìàöèîííî-òåîðåòè÷åñêîì ïîäõîäå ê ïîòîêîâûì øèôðàì ïðåäïîëàãàåòñÿ, ÷òî êðèïòîàíàëèòèê îáëàäàåò íåîãðàíè÷åííûìè âðåìåíåì è âû÷èñëèòåëüíîé ìîùíîñòüþ. Åäèíñòâåííûì ïðàêòè÷åñêè ðåàëèçîâàííûì ïîòîêîâûì øèôðîì, çàùèùåííûì îò òàêîãî ïðîòèâíèêà, ÿâëÿåòñÿ îäíîðàçîâûé áëîêíîò (ñì. ðàçäåë 1.5). Òàê êàê ïèñàòü áèòû â áëîêíîòå íå î÷åíü óäîáíî, åãî èíîãäà íàçûâàþò **îäíîðàçîâîé ëåíòîé**. Íà äâóõ ìàãíèòíûõ ëåíòàõ, íà îäíîé äëÿ øèôðîâàíèÿ, à íà äðóãîé äëÿ äåøèôðîâàíèÿ, äîëæåí áûòü çàïèñàí èäåíòè÷íûé ïîòîê êëþ÷åé. Äëÿ øèôðîâàíèÿ ïðîñòî âûïîëíÿåòñÿ XOR îòêðûòîãî òåêñòà ñ áèòàìè ëåíòû. Äëÿ äåøèôðîâàíèÿ

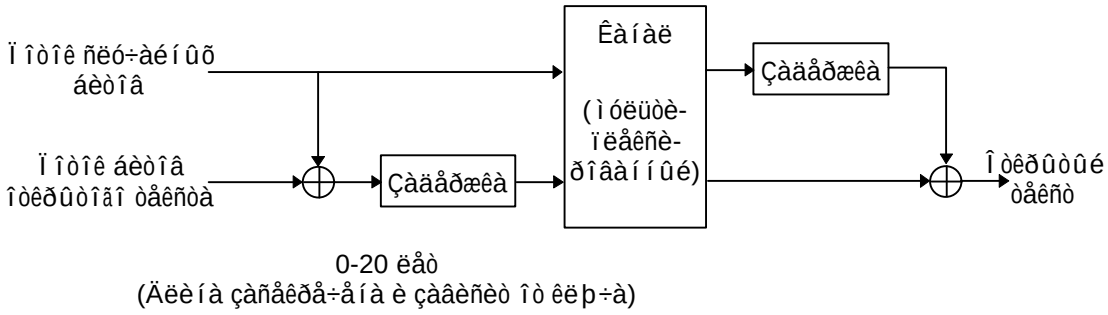
âûïîëíÿåòñÿ XOR øèôðîâåñòà ñ áèòàìè äóãîé, èäåíòè÷íîé ëåíòû. Îäèí è òîò æå ïîòîê êëþ÷åé íåëüçÿ èñïîëüçîâàòü ââàæäû. Òàê êàê áèòû ïîòîêà êëþ÷åé äâóõâåðíîé ñëó÷àéíû, ïðåäñêàçàòü ïîòîê êëþ÷åé íåâîçìîæíî. Åñëè ñæèãàòü ëåíòó ïîñëå èñïîëüçîâàíèÿ, òî áåçîïàñíîñòü áóäåò àáñîëþòíîé (ïðè óñëîâèè, ÷òî ó êîãî-òî äðóãîãî íåò êîïèè ëåíòû).

Äðóãîé èíôîðìàöèîííî-òåîðåòè÷åñêèé ïîòîêîâûé øèôð, ðàçðàáîòàííûõ Êëàóñîì Øíîððîì (Claus Schnorr) ïðåäïîëàãàåò, ÷òî êðèïòîàíàëèòèê èìååò äîñòóï ê îãðàíè÷åííîìó ÷èñëó áèòîâ øèôðîòåêñòà [1395]. Ðåçóëüòàòû ÿâëÿþòñÿ ñëèøêîì òåîðåòè÷åñêèìè results è íå èìåþò ïðàêòè÷åñêîãî çíà÷åíèÿ. Ïîäîáíîñòè ìîæíî íàéòè [1361, 1643,1193].

Ñ ïîìîùüþ ðàíäîìèçèðîâàííîãî ïîòîêîâîãî øèôðà êðèòîãðàô ïûòàåòñÿ ñäåëàòü ðåøåíèå ïðîáëåìû, ñòîÿùåé ïåðåä êðèïòîàíàëèòèêîì, ôèçè÷åñêè íåâîçìîæíûì. Äëÿ ýòîãî, ñîõðàíÿÿ íåíóëåâîé ðàçìåð ñåêðåòíîãî êëþ÷à, êðèïòîãðàô çíà÷èòåëüíî óâåëè÷èâàåò êîëè÷åñòâî áèòîâ, ñ êîòîðûìè ïðèäàòñÿ èìåòü äåëî êðèïòîàíàëèòèê. Ýòî ìîæåò áûòü ñäåëàíî çà ñ÷åò èñïîëüçîâàíèÿ ïðè øèôðîâàíèè è äøèôðîâàíèè áîëüøîé îïóáëèêîâàííîé ñëó÷àéíîé ñòðîêè. Êëþ÷ æå óêàçûâàåò, êàêèå ÷àñòè ñòðîêè áóäóò èñïîëüçîâàíû ïðè øèôðîâàíèè è äåøèôðîâàíèè. Êðèïòîàíàëèòèê, íå çíàþùèé êëþ÷à, ïðèäåòñÿ ïåðåáèðàòü ñëó÷àéíûå êîìáèíàöèè ÷àñòåé ñòðîêè. Áåçîïàñíîñòü òàêîãî øèôðà ìîæíî âû÷èñëèòü ñ ïîìîùüþ ñðåäíåãî ÷èñëà áèòîâ, êîòîðûå äîëæíû áûòü ïîäîáðàíû ïðè øèôðîâàíèè è äåøèôðîâàíèè ïðîòèâíèêîì, ïðåæäå, ÷åì âåðîÿòíîñòüíîðìàëèçóþùèé êëþ÷ çíà÷èòåëüíî óäó÷øèòñÿ ïî ñðàâíåíèþ ñ âåðîÿòíîñòüþ ïðîñòîãî óãàäûâàíèÿ.

Øèôð "Ðèï âàí Âèíêëü"

Äæåéìñ Ìàññåé (James Massey) è Èíãåìàð Èíãåìàðñîí (Ingemar Ingemarsson) ïðåäëîæèëè øèôð "Ðèï âàí Âèíêëü" [1011], íàçâàííûé òàê, ïîòîìó ÷òî ïîëó÷àòåëü, ÷òîáû íà÷àòü äåøèôðîâàíèå, äîëæåí ïîëó÷èòü 2^n áèòîâ øèôðîòåêñòà. Àëãîðèòì, ïîêàçàííûé íà 7-é, ïðîñò â ðåàëèçàöèè, ãàðàíòèðîâàíî áåçîïàñåí è ñîâåðøåííî íåïðàêòè÷åí. Ïðîñòî âûïîëíèòå XOR îòêðûòîãî òåêñòà ñ ïîòîêîì êëþ÷åé è çàâåðæèòå ïîòîê êëþ÷åé íà âðåìÿ îò 0 äî 20 ëåò - òî÷íàÿ çàâåðæêà ÿâëÿåòñÿ ÷àñòüþ êëþ÷à. Ï ñëîâàì Ìàññåÿ: "Ì íîãî ëåãêî äîêàçàòü, ÷òî âðàæåñêîì óêðûòûé øèôðà ìîæíî âûðàçèòü ñ ïîìîùüþ ñðåäíåãî ÷èñëà áèòîâ, êîòîðûå äîëæíû áûòü ïîäîáðàíû ïðè øèôðîâàíèè è äåøèôðîâàíèè ñ ïîìîùüþ ïîäõîäÿùåãî ïðîòîêîëà." Ðàçâèòèå ýòîé èäåè ìîæíî íàéòè â [1577, 755].



Ðèñ. 17-10. Øèôð "Ðèï âàí Âèíêëü".

Ðàíäîìèçèðîâàííûé ïîòîêîâûé øèôð Äèôôè

Ýòà ñõåìà âïåðâûå áûëà ïðåäëîæåíà Óèòôèëäîì Äèôôè [1362]. Èñïîëüçóåòñÿ 2^n ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé. Êëþ÷ ïðåäñòàâëÿåò ñîáîé ñëó÷àéíóþ *n*-áèòîâóþ ñòðîêó. Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ Àëèñà èñïîëüçóåò *k*-óþ ñëó÷àéíóþ ñòðîêó êàê îäíîðàçîâûé áëîêíîò. Çàòåì îíà ïîïðàâëÿåò øèôðîâêñò è 2^n ñëó÷àéíûõ ñòðîê ïî 2^n+1 ðàçëè÷íûì êàíàëàì ñâÿçè.

Áîá çíàåò *k*-, ïîýòîìó îí ìîæåò ëåãêî âû÷èñëèòü, êàêîé èç îäíîðàçîâûõ áëîêíîòîâ èñïîëüçîâàòü äëÿ äåøèôðîâàíèÿ ñîîáùåíèÿ. Åâà îñòàåòñÿ òîëüêî ïððáëèðàòü ñëó÷àéíûå ïîñëåäîâàòåëüíîñòè, ïîêà íå íàéäåò ïðàâèëüíûé îäíîðàçîâûé áëîêíîò. Äëÿ âñêðûòèÿ ïîòðåáóåòñÿ ïðîâåðèòü íåêîòîðûå ÷èñëî áèòîâ, ïî ïîðÿäêó ðàâíî $O(2^n)$. Ðþ ïîåë óêàçàë, ÷òî, åñëè âû îòïðàâëÿåòå *n* ñëó÷àéíûõ ñòðîê âì åñòî2^n, è åñëè êëþ÷ èñïîëüçóåòñÿ äëÿ çàäàíèÿ ëèíåéíîé êîìáèíàöèè ýòèõ ñëó÷àéíûõ ñòðîê, áåçîïàñíîñòü îñòàåòñÿ íà ïðæíåì óðîâíå.

Ðàíäîìèçèðîâàííûé ïîòîêîâûé øèôð Ìàóðåðà

Óåëè Ìàóðåð (Ueli Maurer) îïèñàë ñõåìó, îñíîâàííóþ íà âû÷èñëåíèè XOR îòêðûòîãî òåêñòà ñ íåñêîëüêèì áîëüøèì îòêðûòûì ïîñëåäîâàòåëüíîñòüì ñëó÷àéíûõ áèòîâ [1034, 1029, 1030]. Êëþ÷ ÿâëÿåòñÿ íàáîðîì ñòàðòîâûõ ïîçèöèé â êàæäîé ïîñëåäîâàòåëüíîñòè. Ì îæíî äîêàçàòü, ÷òî òàêîé øèôð ïî÷òè áåçîïàñåí, ñ âåðîÿòíîñòüþ âçëîìà îïðåäåëÿòñÿ îáúåì ïàìÿòè, èìåþùåéñÿ â ðàñïîðÿæåíèè âçëîìùèêà, íåçàâèñèìî îò äîñòóïíîé âû÷èñëèòåëüíîé ìîùíîñòè. Ìàóðåð óòâåðæäàë, ÷òî ýòà ñõåìà ñòàíîâèòñÿ ïðàêòè÷íîé ïðè 100 ðàçëè÷íûõ ïîñëåäîâàòåëüíîñòÿõ äëèíîé 10^{20} ñëó÷àéíûõ áèòîâ êàæäàÿ. Îäíàì èç ñïîñîáîâ ïîëó÷èòü ðàê ìíîãî áèòîâ ÿâëÿ-

åòñÿ îöèôðîâêà ïîâåðõíîñòè Ëóíû.

17.11 Øèôðû ñ êàñêàäîì íåñêîëüêèõ ïîòîêîâ

Åñëè ïðîèçâîäèòåëüíîñòü íå âàæíà, òî íåò ïðè÷èí âûáèðàòü íåñêîëüêî ïîòîêîâûõ øèôðîâ è îáúåäèíÿòü èõ â êàñêàä. Äëÿ ïîëó÷åíèÿ øèôðîòåêñòà ïðîñòî âûïîëíèòå XOR âûõîäà êàæäîãî ãåíåðàòîðà ñ îòêðûòûì òåêñòîì. Ðåçóëüòàò Óåëëè Ìàóðåðà (ñì. ðàçäåë 15.7) ïîêàçûâàåò, ÷òî åñëè ãåíåðàòîðû èñïîëüçóþò íåçàâèñèìûå êëþ÷è, òî áåçîïàñíîñòü êàñêàäà ïî êðàéíåé ìåðå íå ìåíüøå áåçîïàñíîñòè ñàìîãî ñèëüíîãî àëãîðèòìà êàñêàäà, à ñêîðåå âñåãî è íàìíîãî áîëüøå.

Ïîòîêîâûå øèôðû îáúåäèíÿþòñÿ òåìè æå ñïîñîáàìè, ÷òî è áëî÷íûå (ñì. ãëàâó 15). Ïîòîêîâûå øèôðû ìîæíî îáúåäèíèòü â êàñêàä (ñì. ðàçäåë 15.7) ñ äðóãèìè ïîòîêîâûìè øèôðàìè èëè ñ áëî÷íûìè øèôðàìè.

Ëîâêèì òðþêîì ÿâëÿåòñÿ èñïîëüçîâàíèå îäíîãî àëãîðèòìà, ïîòîêîâîãî èëè áëî÷íîãî, äëÿ ÷àñòîãî îáíîâëåíèÿ êëþ÷à áûñòðîãî ïîòîêîâîãî àëãîðèòìà (êîòîðûì ìîæåò áûòü è áëî÷íûé àëãîðèòì â ðåæèìå OFB). Áûñòðûé àëãîðèòì ìîæåò áûòü ñëàáûì, òàê êàê êðèïòîàíàëèòèê íèêîãäà íå ïîëó÷èò äîñòàòî÷íî îòêðûòîãî òåêñòà, çàøèôðîâàííîãî îäíèì êëþ÷îì.

Ñóùåñòâóåò ñïîñîá ðàçìåíÿòü ðàçìåð âíóòðåííåãî ñîñòîÿíèÿ áûñòðîãî àëãîðèòìà (êîòîðûé ìîæåò âëèÿòü íà áåçîïàñíîñòü) íà ÷àñòîòó ñìåíû êëþ÷à. Ñìåíà êëþ÷à äîëæíà áûòü îòíîñèòåëüíî ÷àñòîé, íå ñòîèò èñïîëüçîâàòü äëÿ ýòîãî àëãîðèòìû ñ äëèííîé ïðîöåäóðîé óñòàíîâêè êëþ÷à. Êðîìå òîãî, ñìåíà êëþ÷à íå äîëæíà çàâèñåòü îò âíóòðåííåãî ñîñòîÿíèÿ áûñòðîãî àëãîðèòìà.

17.12 Âûáîð ïîòîêîâîãî øèôðà

Åñëè èçó÷åíèå ïîòîêîâûõ øèôðîâ è äàåò êàêîé-ëèáî ðåçóëüòàò, òàê ýòî ïîÿâëåíèå ñ ïóãàþùåé ðåãóëÿðíîñòüþ âñå íîâûõ ñïîñîáîâ âñêðûòèÿ. Òðàäèöèîííî ïîòîêîâûå øèôðû îïèðàëèñü íà áîëüøóþ ìàòåìàòè÷åñêóþ òåîðèþ. Ýòó òåîðèþ ìîæíî áûëî èñïîëüçîâàòü äëÿ äîêàçàòåëüñòâà ïîëîæèòåëüíûõ êà÷åñòâ øèôðà, íî åå æå ìîæíî áûëî èñïîëüçîâàòü äëÿ ïîèñêà íîâûõ ñïîñîáîâ âñêðûòèÿ øèôðà. Ïî ýòîé ïðè÷èíå ëþáîé ïîòîêîâûé øèôð, îñíîâàííûé òîëüêî íà LFSR, âûçûâàåò ìîå áåñïîêîéñòâî.

ß ïðåäïî÷èòàþ ïîòîêîâûå øèôðû, ñïðîåêòèðîâàííûå ïîäîáíî áëî÷íûì øèôðàì: íåëèíåéíûå ïðåîáðàçîâàíèÿ, áîëüøèå S-áëîêè, è ò.ä. Áîëüøå âñåãî ìíå íðàâèòñÿ RC4, à çàòåì SEAL. Ìíå áû î÷åíü õîòåëîñü óâèäåòü ðåçóëüòàòû êðèïòîàíàëèçà ïðåäëîæåííûõ ìíîé ãåíåðàòîðîâ, îáúåäèíÿþùèõ LFSR è FCSR. Ýòà îáëàñòü êàæåòñÿ âåñüìà ïðèâëåêàòåëüíîé äëÿ èçó÷åíèÿ âîçìîæíîñòè èñïîëüçîâàíèÿ â ðåàëüíûõ ðàçðàáîòêàõ. Èëè äëÿ ïîëó÷åíèÿ ïîòîêîâîãî øèôðà ìîæíî èñïîëüçîâàòü áëî÷íûé øèôð â ðåæèìå OFB èëè CFB.

Â 14-é äëÿ ñðàâíåíèÿ ïðèâåäåíû âðåìåííûå ñîîòíîøåíèÿ äëÿ íåêîòîðûõ àëãîðèòìîâ.

Òàáë. 17-3.
Ñêîðîñòè øèôðîâàíèÿ íåñêîëüêèõ ïîòîêîâûõ øèôðîâ íà i486SX/33 ÌÃö

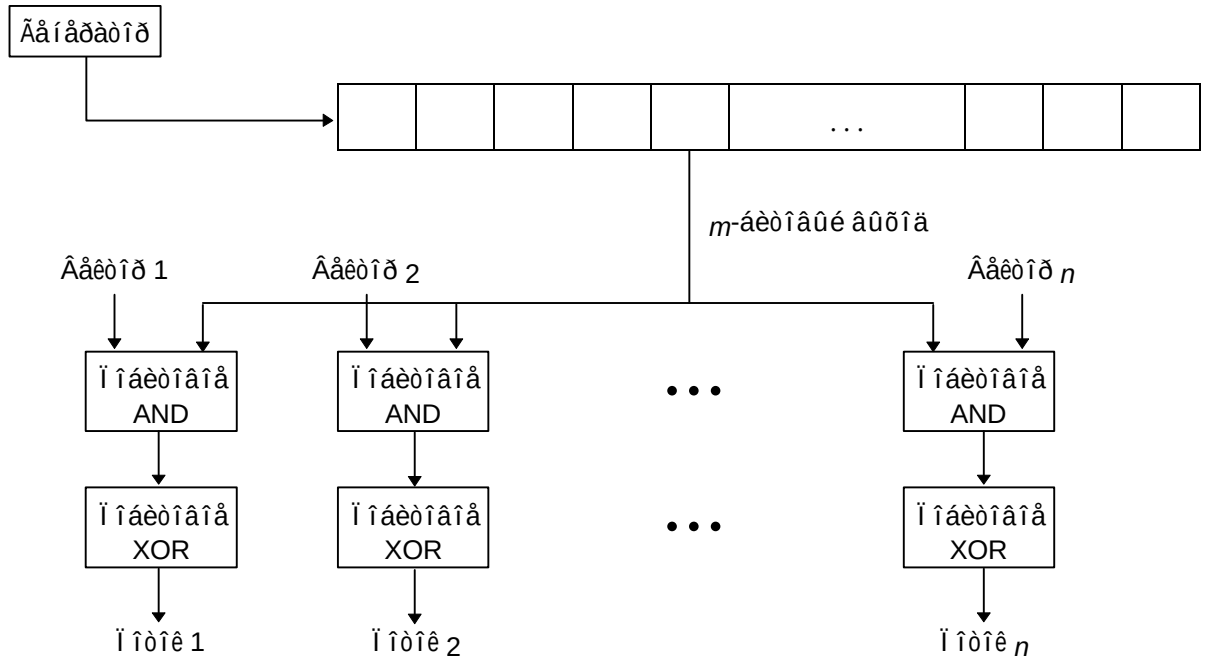
Àëãîðèòì	Ñêîðîñòü øèôðîâàíèÿ (Ìáàéò/ñ)
A5	5
PIKE	62
RC4	164
SEAL	381

17.13 Ãåíåðàöèÿ íåñêîëüêèõ ïîòîêîâ èç îäíîãî ãåíåðàòîðà ïñåâäîñëó÷àéíîé ïîñëåäîâàòåëüíîñòè

Åñëè íóæíî çàøèôðîâàòü íåñêîëüêî êàíàëîâ ñâÿçè ïðè ïîìîùè îäíîãî áëîêà - íàïðèìåð, ìóëüòèïëåêñîðà - ïðîñòûì ðåøåíèåì ÿâëÿåòñÿ èñïîëüçîâàíèå äëÿ êàæäîãî ïîòîêà ñâîåãî ãåíåðàòîðà ïñåâäîñëó÷àéíîé ïîñëåäîâàòåëüíîñòè. Ïðè ýòîì âîçíèêàþò äâå ñëåäóþùèõ ïðîáëåìû: íóæíà äîïîëíèòåëüíàÿ àïïàðàòóðà, è âñå ãåíåðàòîðû äîëæíû áûòü ñèíõðîíèçèðîâàíû. Ïðîùå áûëî áû èñïîëüçîâàòü îäèí ãåíåðàòîð.

Îäíî èç ðåøåíèé - òàêòèðîâàòü ãåíåðàòîð íåñêîëüêî ðàç. Åñëè íóæíî òðè íåçàâèñèìûõ ïîòîêà, òàêòèðóéòå ãåíåðàòîð òðè ðàçà è îòïðàâüòå ïî îäíîìó áèòó â êàæäûé ïîòîê. Ýòîò ìåòîä ðàáîòàåò, íî ìîãóò áûòü ñëîæíîñòè ïðè ïîëó÷åíèè áîëüøîé ÷àñòîòû. Íàïðèìåð, åñëè âû ìîæåòå òàêòèðîâàòü ãåíåðàòîð òîëüêî â òðè ðàçà áûñòðåå òàêòèðîâàíèÿ ïîòîêà äàííûõ, âû ñìîæåòå ñîçäàòü òîëüêî òðè ïîòîêà. Äðóãèì ñïîñîáîì ÿâëÿåòñÿ èñïîëüçîâàíèå îäíîé è òîé æå ïîñëåäîâàòåëüíîñòè äëÿ êàæäîãî êàíàëà, âîçìîæíî ñ ïåðåìåííîé âðåìåííîé çàäåðæêîé. Ýòî íåáåçîïàñíî.

Äåéñòâèòåëüíî óäà÷íàÿ èäåÿ [1489], çàïàòåíòîâàííàÿ NSA, ïîêàçàíà íà 6-é. Çàïèñûâàéòå âûõîä âàøåãî ëþáèìîãî äåíåðàòîðà â ïðîñòîé *m*-áèòîâûé ñäâèãîâûé ðåãiñòð. Ïî êàæäîìó òàêòîâîìó èìïóëüñó ñäâèãàéòå ðåãiñòð íà îäèí áèò âïðàâî. Çàòåì äëÿ êàæäîãî âûõîäíîãî ïîòîêà âû÷èñëèòå AND ðåãiñòðà ñ äðóãèì *m*-áèòîâûì âåêòîðîì, ðàññìàòðèâàåìûì êàê óíèêàëüíûé èäåíòèôèêàòîð äëÿ âûáðàííîãî âûõîäíîãî ïîòîêà, çàòåì îáúåäèíèòå ñ ïîìîùüþ XOR âñå áèòû, ïîëó÷àÿ âûõîäíîé áèò äëÿ ýòîãî ïîòîêà. Åñëè òðåáóåòñÿ ïîëó÷èòü ïàðàëëåëüíî íåñêîëüêî âûõîäíûõ ïîòîêîâ, äëÿ êàæäîãî âûõîäíîãî ïîòîêà íóæíî èñïîëüçîâàòü îòäåëüíûé âåêòîð è ëîãè÷åñêèé ìàññèâ XOR/AND.



Ðèñ. 17-11. Ãåíåðàòîð íåñêîëüêèõ áèòîâ.

Ñóùåñòâóåò ðÿä âåùåé, êîòîðûå íóæíî îòñëåæèâàòü. Åñëè ëþáîé èç ýòèõ ïîòîêîâ ÿâëÿåòñÿ ëèíåéíîé êîìáèíàöèåé äðóãèõ ïîòîêîâ, òî ñèñòåìà ìîæåò áûòü âçëîìàíà. Íî åñëè âû äîñòàòî÷íî àêòóàòíû, îïèñàííûé ñïîñîá ÿâëÿåòñÿ ïðîñòûì è áåçîïàñíûì ñïîñîáîì ðåøåíèÿ ïðîáëåì.

17.14 Ãåíåðàòîðû ðåàëüíûõ ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé

Èíîãäà êðèòîãðàôè÷åñêè áåçîïàñíûå ïñåâäîñëó÷àéíûå ïîñëåäîâàòåëüíîñòè íåäîñòàòî÷íî õîðîøè. Â êðèòîãðàôèè âàì ìîãóò ïîíàäîáèòüñÿ äåéſòâèòåëüíî ñëó÷àéíûå èñëà. Ïðåäïîëîæèì, ÷òî ïðèõîäèò â ãîëîâó - ýòî ãåíåðàöèÿ êëþ÷åé. Ïðåðàñíî ìîæíî ãåíåðèðîâàòü ñëó÷àéíûå êðèïòîãðàôè÷åñêèå êëþ÷è, èñïîëüçóÿ ãåíåðàòîð ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé, íî åñëè âðàã äîáóäåò êîïèþ ýòîãî ãåíåðàòîðà è ãëàâíûé êëþ÷, îí ñìîæåò ñîçäàòü òå æå êëþ÷è è âçëîìàòü âàøó êðèïòîñèſòåìó, íåçàâèñèìî îò íàäåæíîñòè âàøèõ äëãîðèòìîâ. Ïîñëåäîâàòåëüíîñòü, âûäàâàåìóþ ãåíåðàòîðîì ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé, âîñïðîèçâåñòè íåâîçìîæíî. Íèêòî, äàæå âû ñàìè, íå ñìîæåò âîñïðîèçâåñòè ïîñëåäîâàòåëüíîñòü áèòîâ, âûäàâàåìóþ ýòèìè ãåíåðàòîðàìè.

Êðóïíîé ôëîñîôñêîé ïðîáëåìîé ÿâëÿåòñÿ âîïðîñ î òîì, äàþò ëè ýòè ìåòîäû äåíòàêòèôèöèðîâàííî ñëó÷àéíûå áèòû, âûäàâàåìûå ïîñëåäîâàòåëüíîñòè, ïîñëåäîâàòåëüíîñòè, ïîëó÷åííûå ïîñëåäîâàòåëüíûì ïóòåì. Íèêòî, äàæå âû ñàìè, íå ñìîæåò âîñïðîèçâåñòè ïîñëåäîâàòåëüíîñòü áèòîâ, âûäàâàåìóþ ýòèìè ãåíåðàòîðàìè.

Äëÿ ëþáîãî ãåíåðàòîðà äéſòâèòåëüíî ñëó÷àéſûõ ïîñëåäîâàòåëüíîñòè âàæíû âîïðîſſì ÿâëÿåòſſ åãî ïðîâåðêà. Íà ýòó òåìó ſóùåſſòâóåò ìíîæåſſòâî ëèòåðàòóðû. Òåſſòû íà ſëó÷àéſſſòü ìîæſſ íàéòè â [863, 99]. Ìàóðåð ïîêàçàë, ÷òî âſå ýòè òåſſòû ìîæſſ ïîëó÷èòü èç ïîïûòêè ſæàòü ïîſſåſſíîſòü ìîæſſ íàéòè â [1031, 1032]. Åſſëè ſëó÷àéſàÿ ïîſſåſſíîſòü ſæèìàåſſſÿ, òî îſà íå ÿâëÿåſſſÿ ïî íàſòîÿùàìó ſëó÷àéſſé.

Â ëþáîì ſëó÷àå, âſå, ÷òî ìû èſſåì â ýòîſ îáëàſòè, âî ſſíîſſì ſòſſſèſſÿ ſ ÷åðſſé ſàſèſ. Äëàſſûì ſſſſåſſſòſſ ÿâëÿåſſſÿ ſåſſåðſàöèÿ ïſſëåſſſòſàſòåëüſſſſòè áèòſâ, êſòſðóþ íå ſſſæåſſ óſàſàſòü âſø ïðſòèâſèſ. Ýſſ ſſðſçäſ áſſëåå òðóſàſàÿ çſàſà÷à, ÷åſ êſæåſòÿ. ß íå ſſſſ äſêſçſòü, ÷òſ ëþáſé èç ſſſèſàſſſûſ ſſòſſſſſ ſſåſſåðåðóſò ſëó÷àéſûå áèòû. Ðåçóëüſòàòſſ èſ ðſáſſòû ÿâëÿþſÿ ſſſëåſſſòſàſòåëüſſſſòè áèòſâ, êſòſðóå íåâſçſſſſſſ ëåſêſ âſſſïðſèçâåſſòè. Ïſſäðſáſſſſòè ſſæſſ íſéòè â [1375, 1376, 511].

Òàáëèöû RAND

Äàâſû ſſſſſſ, â 1955 ſſſſó, êſſſſſà êſſſüþſåðû âſſå åùå áûëè â ſſâſéſêó, Rand Corporation èçſſſëſà êſèſſó, ſſſſåðæſâøóþ ſèëëèſſ ſëó÷àéſûſ öèôð [1289]. Èſ ſåſſſ ſſèſſûâſſÿſ òſê:

Ñëó÷àéíûå öèôðû ýòîé êíèãè áûëè ïîëó÷åíû ïðè ïîìîùè ðàíäîìèçàöèè îñíîâíîé òàáëèöû, ñãåíåðèðîâàííîé ýëåêòðîííîé ðóëåòêîé. Âêðàòöå, èñòî÷íèê èìóëüñîâ, âûâîä èëè ñîì ñëó÷àéíîé ÷àñòîòû â ñðåäíåì îêîëî 100000 èìóëüñîâ â ñåêóíäó, îòêðûâàëñÿ ðàç â ñåêóíäó èìïóëüñîì ïîñòóïàëè èìïóëüñû ÷åðåç 5-ðàçðÿäíûé áèíàðíûé ñ÷åò÷èê. Ïî ñóòè ìàøèíà ÿâëÿëàñü êîëåñîì ðóëåòêè ñ 32-ïîçèöèÿìè, êîòîðîå â ñðåäíåì äåëàëî îêîëî 3000 îáîðîòîâ çà âûáðîñ è âûäàâàëî îäíî ÷èñëî â ñåêóíäó. Èñïîëüçîâàëñÿ äâîè÷íî-äåñÿòè÷íûé ïðåîáðàçîâàòåëü, êîòîðûé ïðåîáðàçîâûâàë 20 èç 32 ÷èñåë (îñòàâøèñÿ ââåíäåíòàì îòáðàñûâàþòñÿ) è îñòàâëÿë òîëüêî ïîñëåäíèå 20 ÷èñåë, êîòîðûå è ïóñêàëèñü â îáîðîò. Ýòî ïîñëåäíåå öèôðû ïîïàäàëè â êîìïüþòåð IBM, îáðàçóÿ â êîíöå êîíöîâ òáëèöó ïðîáèòûõ êàðòî÷åê ñëó÷àéíûõ öèôð.

Â êíèãå ðàññìàòðèâàëèñü è ðåçóëüòàòû ðàçëè÷íûõ ïðîâåðîê äàííûõ íà ñëó÷àéíîñòü. Â íåé òàêæå ïðåäëàãàëñÿ ñïîñîá, êàê èñïîëüçîâàòü ýòó êíèãó äëÿ âûáîðà ñëó÷àéíîãî ÷èñëà:

Ñòðîêè òàáëèöû öèôð íóìåðóþòñÿ îò 00000 äî 19999. Ïðè èñïîëüçîâàíèè òàáëèöû íóæíî ñíà÷àëà âûáðàòü ñëó÷àéíóþ ñòàðòîâóþ ïîçèöèþ. Îáû÷íî ïðîöåäóðîé äëÿ ýòîãî ÿâëÿåòñÿ ñëåäóþùåå: îòêðîéòå ýòó êíèãó íà ïðîèçâîëüíîé ñòðàíèöå òàáëèöû öèôð è, çàêðûâ ãëàçà, âûáåðèòå ïÿòèðàçðÿäíîå ÷èñëî. Ýòî ÷èñëî ïîñëå çàìåíû ïåðâîé öèôðû îñòàòîê îò äåñÿòè åå íà 2 îïðåäåëÿåò ñòàðòîâóþ ñòðîêó. Îñòàòîê îò äåëåíèÿ äâóõ öèôð ñîñòàâà îò ïåðâîíà÷àëüíî âûáðàííîãî ïÿòèðàçðÿäíîãî ÷èñëà íà 50 çàäàåò ñòàðòîâûé ñòîëáåö â ñòàðòîâîé ñòðîêå. ×òîáû çàìèòüñÿ îò îêðûòèÿ êíèãè âñå âðåìÿ íà ïâíîé ñòðàíèöå è åñòåñòâåííûì îáðàçîì ïîðåçàòü ïîçèöèè ïÿòèðàçðÿäíîå ÷èñëî íà ïîëîñêå ïîä èãëîé. ×òîáû çàìèòèëè îò îêðûòèÿ êíèãè âñå âðåìÿ íà ïâíîé ñòðàíèöå è åñòåñòâåííûì îáðàçîì ïîçèöèè ïÿòèðàçðÿäíîå ÷èñëî äîëæíî áûòü ïîìå÷åíî è íå äîëæíî áûëüøå èñïîëüçîâàòüñÿ äëÿ ýòîé öåëè.

Ãëàâíûì ñîäåðæàíèåì ýòîé êíèãè áûëà "Òàáëèöà ñëó÷àéíûõ öèôð". Öèôðû ïðèâîäèëèñü ïÿòè ðàçðÿäíûìè ãðóïïàìè - "10097 32533 76520 13586 . . ." - ïî 50 â ñòðîêå è ïî ïÿòüäåñÿò ñòðîê íà ñòðàíèöå. Òàáëèöà çàíèìàëà 400 ñòðàíèö è, çà èñêëþ÷åíèåì îñíîâíîé âûäà÷è ýêçåìïëÿðîâ ñòðàíèöå 283, âûäàëÿäåøåé êàê "69696", áûëà äîñòàòî÷íî ñëó÷íûì ÷òåíèåì. Â êíèãó òàêæå âõîäèëà òàáëèöà 100000 íîðìàëüíûõ îòêëîíåíèé.

Èíòåðåñíûì â êíèãå RAND ÿâëÿþòñÿ íå ìèëëèîíû ñëó÷àéíûõ öèôð, à òî, ÷òî îíè áûëè ñîçäàíû äî êîìïüþòåðíîé ðåâîëþöèè. Âî ìíîãèõ êðèïòîãðàôè÷åñêèõ äèãîðèòìàõ èñïîëüçóþòñÿ ïðîèçâîëüíûå êíîñòàíòû - òàê íàçûâàåìûå "ìàãè÷åñêèå ÷èñëà". Âûáîð ìàãè÷åñêèõ ÷èñåë èç òàáëèö RAND ãàðàíòèðîâàë, ÷òî îíè íå áûëè âûáðàíû ñïåöèàëüíî ïî êàêèì-òî æóëüíè÷åñêèì ïðè÷èíàì. Òàê, íàïðèìåð, áûëî ñäåëàíî â Khafre.

Èñïîëüçîâàíèå ñëó÷àéíîãî øóìà

Ëó÷øèì ñïîñîáîì ïîëó÷èòü áîëüøîå êîëè÷åñòâî ñëó÷àéíûõ áèòîâ ÿâëÿåòñÿ èçâëå÷åíèå èõ èç åñòåñòâåííîé ñëó÷àéíîñòè ðåàëüíîãî ìèðà. ×àñòî òàêîé ìåòîä òðåáóåò ñïåöèàëüíîé àïïàðàòóðû, íî ýòî òðþê ìîæíî ïðèìåíèòü è â êîìïüþòåðàõ.

Íàéäèòå ñîáûòèå, êîòîðîå ñëó÷àéíîñòü ðåãóëÿðíî, íî ñëó÷àéíî: àòìîñôåðíûé øóì, ïðåîäîëåâàþùèé êàêîé-òî ïîðîã, ðåáåíîê, ïàäàþùèé, ó÷àñü õîäèòü. Èçìåðüòå éíòåðâàë ìåæäó îáíèì ïîâîáíûì ñîáûòèåì è ñîáûòèåì, ñëåäóþùèì çà íèì. Çàïèøèòå. Èçìåðüòå âðåìåííîé éíòåðâàë ìåæäó âòîðûì è òðåòüì ñîáûòèåì. Ñíîâà çàïèøèòå. Åñëè ïåðâûé âðåìåííîé éíòåðâàë áîëüøå âòîðîãî, âûõîäíûì áèòîì áóäåò 1. Åñëè âòîðîé éíòåðâàë áîëüøå ïðåäûäóùåãî, òî âûõîäíûì ñîáûòèåì áóäåò 0. Ñäåëàéòå ýòî ñíîâà äëÿ ñëåäóþùåãî ñîáûòèÿ.

Áðîñüòå ñòðåëó äàðòñ â ïðåå÷åíü êîòèðîâîê Íüþ-Éîðêñêîé ôîíäîâîé áèðæå â ìåñòíîé ãàçåòå. Ñðàâíèòå êîòèðîâêó àêöèè, â êîòîðóþ âû ïîïàëè, ñ êîòèðîâêîé àêöèè ïðÿìî íàä íåé. Åñëè áîëüøå òà, â êîòîðóþ âû ïîïàëè, âûõîä ðàâåí 0, à åñëè ìåíüøå - 1.

Ïîâòîðèòå ê êîìïüþòåðó ñ÷åò÷èê Åéãåðà, ïîäñ÷èòàéòå êîëè÷åñòâî èìïóëüñîâ çà ôèêñèðîâàííûé èíòåðâàë âðåìåíè è âîçüìèòå ìèíóñ îäíó éåíü. Èëè èçìåðüòå âðåìÿ ìåæäó ïîñëåäíèìè äâóìÿ ïîñëåäîâàòåëüíûìè òèêàìè ticks. (Òàê êàê ðàäèîàêòèâíûé èñòî÷íèê ðàñïàäàåòñÿ, ñðåäíåå âðåìÿ ìåæäó ïîñëåäíèìè äâóìÿ ïîñëåäîâàòåëüíûìè òèêàìè íåïðåðûâíî ÷åòûðíàäöàòü - òàêîé êàê ïëóòîíèé. Åñëè âû íåçíàêîìû ñ äîñòàòî÷íî ñëîæíûì ïîíÿòèåì, ïðîñòî çàáóäüòå îá ýòîì ÿâëÿåòñÿ. [535]. Êîìàð÷åñêèé (Òàê êàê ðàäèîàêòèâíûé èçîòîï [67]. Ì. Ãüþä (M. Gude) ïîñòðîèë ãåíåðàòîð ñëó÷àéíûõ ÷èñåë, îïèñàâ ñõåìó ñ äâóõ ìåòàëëè÷åñêèõ ïëàñòèí, ðàçäåë¸ííûõ òîíêèì ñëîåì äèýëåêòðèêà. Ïîäàâàÿ íà ýòè ÿâëåíèå [67]. Ì. Ãüþä (M. Gude) ïîñòðîèë ãåíåðàòîð ñëó÷àéíûõ ÷èñåë, îïèñàâ ñõåìó ñ äâóõ ìåòàëëè÷åñêèõ ïëàñòèí, ðàçäåë¸ííûõ òîíêèì ñëîåì äèýëåêòðèêà. Äâóõîé ãåíåðàòîð ñëó÷àéíûõ ÷èñåë åíåðãèþ ïîòîê ñëó÷àéíûõ áèòîâ, èñïîëüçóÿ íåñòàáèëüíîñòü ÷àñòîòû ñâîáîäíîãî êîëåáàòåëüíîãî êîíòóðà [535]. Êîì ìåð÷åñêèé ìåæäóíàðîäíûé êîíöåðí AT&T ãåíåðàòîðó ñëó÷àéíûõ ÷èñåë, îïèñàâ ñõåìó ñ äâóõ ìåòàëëè÷åñêèõ ïëàñòèí, ðàçäåë¸ííûõ òîíêèì ñëîåì äèýëåêòðèêà. Äâóõîé ãåíåðàòîð ñëó÷àéíûõ ÷èñåë ñ 32-ïîçèöèÿìè, êîòîðîå â ñðåäíåì îêîëî 3000 îáîðîòîâ çà âûáðîñ è âûäàâàëî îäíî ÷èñëî â ñåêóíäó. Èñïîëüçîâàëñÿ äâîè÷íî-äåñÿòè÷íûé ïðåîáðàçîâàòåëü, êîòîðûé ïðåîáðàçîâûâàë 20 èç 32 ÷èñåë (îñòàâøèñÿ ââåíäåíòàì îòáðàñûâàþòñÿ) è îñòàâëÿë òîëüêî ïîñëåäíèå 20 ÷èñåë, êîòîðûå è ïóñêàëèñü â îáîðîò. Ýòî ïîñëåäíåå öèôðû ïîïàäàëè â êîìïüþòåð IBM, îáðàçóÿ â êîíöå êîíöîâ òáëèöó ïðîáèòûõ êàðòî÷åê ñëó÷àéíûõ öèôð.

Â êíèãå ðàññìàòðèâàëèñü è ðåçóëüòàòû ðàçëè÷íûõ ïðîâåðîê äàííûõ íà ñëó÷àéíîñòü. Â íåé òàêæå ïðåäëàãàëñÿ ñïîñîá, êàê èñïîëüçîâàòü ýòó êíèãó äëÿ âûáîðà ñëó÷àéíîãî ÷èñëà:

Ñòðîêè òàáëèöû öèôð íóìåðóþòñÿ îò 00000 äî 19999. Ïðè èñïîëüçîâàíèè òàáëèöû íóæíî ñíà÷àëà âûáðàòü ñëó÷àéíóþ ñòàðòîâóþ ïîçèöèþ. Îáû÷íî ïðîöåäóðîé äëÿ ýòîãî ÿâëÿåòñÿ ñëåäóþùåå: îòêðîéòå ýòó êíèãó íà ïðîèçâîëüíîé ñòðàíèöå òàáëèöû öèôð è, çàêðûâ ãëàçà, âûáåðèòå ïÿòèðàçðÿäíîå ÷èñëî. Ýòî ÷èñëî ïîñëå çàìåíû ïåðâîé öèôðû îñòàòîê îò äåëåíèÿ äâóõ öèôð íà 2 îïðåäåëÿåò ñòàðòîâóþ ñòðîêó. Îñòàòîê îò äåëåíèÿ äâóõ öèôð íà ñòðàíèöå 283, âûäàëÿäåøåé êàê "69696", áûëà äîñòàòî÷íî ñëó÷íûì ÷òåíèåì. Â êíèãó òàêæå âõîäèëà òàáëèöà 100000 íîðìàëüíûõ îòêëîíåíèé.

Èíòåðåñíûì â êíèãå RAND ÿâëÿþòñÿ íå ìèëëèîíû ñëó÷àéíûõ öèôð, à òî, ÷òî îíè áûëè ñîçäàíû äî êîìïüþòåðíîé ðåâîëþöèè. Âî ìíîãèõ êðèïòîãðàôè÷åñêèõ äèãîðèòìàõ èñïîëüçóþòñÿ ïðîèçâîëüíûå êîíñòàíòû - òàê íàçûâàåìûå "ìàãè÷åñêèå ÷èñëà". Âûáîð ìàãè÷åñêèõ ÷èñåë èç òàáëèö RAND ãàðàíòèðîâàë, ÷òî îíè íå áûëè âûáðàíû ñïåöèàëüíî ïî êàêèì-òî æóëüíè÷åñêèì ïðè÷èíàì. Òàê, íàïðèìåð, áûëî ñäåëàíî â Khafre.

Èñïîëüçîâàíèå ñëó÷àéíîãî øóìà

Ëó÷øèì ñïîñîáîì ïîëó÷èòü áîëüøîå êîëè÷åñòâî ñëó÷àéíûõ áèòîâ ÿâëÿåòñÿ èçâëå÷åíèå èõ èç åñòåñòâåííîé ñëó÷àéíîñòè ðåàëüíîãî ìèðà. ×àñòî òàêîé ìåòîä òðåáóåò ñïåöèàëüíîé àïïàðàòóðû, íî ýòî òðþê ìîæíî ïðèìåíèòü è â êîìïüþòåðàõ.

Íàéäèòå ñîáûòèå, êîòîðîå ñëó÷àéíîñòü ðåãóëÿðíî, íî ñëó÷àéíî: àòìîñôåðíûé øóì, ïðåîäîëåâàþùèé êàêîé-òî ïîðîã, ðåáåíîê, ïàäàþùèé, ó÷àñü õîäèòü. Èçìåðüòå éíòåðâàë ìåæäó îáíèì ïîâîáíûì ñîáûòèåì è ñîáûòèåì, ñëåäóþùèì çà íèì. Çàïèøèòå. Èçìåðüòå âðåìåííîé éíòåðâàë ìåæäó âòîðûì è òðåòüì ñîáûòèåì. Ñíîâà çàïèøèòå. Åñëè âòîðîé éíòåðâàë áîëüøå âòîðîãî, âûõîäíûì áèòîì áóäåò 1. Åñëè âòîðîé éíòåðâàë áîëüøå ïðåäûäóùåãî, òî âûõîäíûì áèòîì áóäåò 0. Ñäåëàéòå ýòî ñíîâà äëÿ ñëåäóþùåãî ñîáûòèÿ.

Áðîñüòå ñòðåëó äàðòñ â ïðåå÷åíü êîòèðîâîê Íüþ-Éîðêñêîé ôîíäîâîé áèðæå â ìåñòíîé ãàçåòå. Ñðàâíèòå êîòèðîâêó àêöèè, â êîòîðóþ âû ïîïàëè, ñ êîòèðîâêîé àêöèè ïðÿìî íàä íåé. Åñëè áîëüøå òà, â êîòîðóþ âû ïîïàëè, âûõîä ðàâåí 0, à åñëè ìåíüøå - 1.

Ïîâòîðèòå ê êîìïüþòåðó ñ÷åò÷èê Åéãåðà, ïîäñ÷èòàéòå êîëè÷åñòâî èìïóëüñîâ çà ôèêñèðîâàííûé èíòåðâàë âðåìåíè è âîçüìèòå ìèíóñ îäíó éåíü. Èëè èçìåðüòå âðåìÿ ìåæäó ïîñëåäíèìè äâóìÿ ïîñëåäîâàòåëüíûìè òèêàìè ticks. (Òàê êàê ðàäèîàêòèâíûé èñòî÷íèê ðàñïàäàåòñÿ, ñðåäíåå âðåìÿ ìåæäó ïîñëåäíèìè äâóìÿ ïîñëåäîâàòåëüíûìè òèêàìè íåïðåðûâíî ÷åòûðíàäöàòü - òàêîé êàê ïëóòîíèé. Åñëè âû íåçíàêîìû ñ äîñòàòî÷íî ñëîæíûì ïîíÿòèåì, ïðîñòî çàáóäüòå îá ýòîì ÿâëÿåòñÿ. [535]. Êîì ìåð÷åñêèé (Òàê êàê ðàäèîàêòèâíûé èçîòîï [67]. Ì. Ãüþä (M. Gude) ïîñòðîèë ãåíåðàòîð ñëó÷àéíûõ ÷èñåë, îïèñàâ ñõåìó ñ äâóõ ìåòàëëè÷åñêèõ ïëàñòèí, ðàçäåë¸ííûõ òîíêèì ñëîåì äèýëåêòðèêà. Äâóõîé ãåíåðàòîð ñëó÷àéíûõ ÷èñåë åíåðãèþ ïîòîê ñëó÷àéíûõ áèòîâ, èñïîëüçóÿ íåñòàáèëüíîñòü ÷àñòîòû ñâîáîäíîãî êîëåáàòåëüíîãî êîíòóðà [439]. Îí èçìåðÿåò âðåìÿ, íóæíîå äëÿ ÷òåíèÿ äèñêà, è èñïîëüçóåò èçìåíåíèÿ ýòîãî âðåìåíè â êà÷åñòâå èñòî÷íèêà ñëó÷àéíûõ ÷èñåë. Äàííûå ôëüòðóþòñÿ, ÷òîáû óäàëèòü ñòðóêòóðó, âûçâàííóþ êâàíòîâàíèåì, çàòåì ê âåêòîðàì ÷èñëè ïðèìåíÿþòñÿ áûñòðûå ïðåîáðàçîâàíèÿ Ôóðüå. Ýòî óñòðàíÿåò ñìåùåíèå è êîððåëÿöèþ. Íàêîíåö, â êà÷åñòâå ñëó÷àéíûõ áèòîâ èñïîëüçóþòñÿ ñïåêòðàëüíûå óãëû ÷àñòîò â äèàïàçîíå (0, π), íîðìàëèçîâàííûå íà åäèíè÷íûé èíòåðâàë.

Áîëüøàÿ ÷àñòü èçìåíåíèé ñîîðíîñòè âðàùåíèÿ äèñêà âûçâàíà òóðáóëåíòíîñòüþ âîçäóõà, êîòîðàÿ è ÿâëÿåòñÿ èñòî÷íèêîì ñëó÷àéíîñòè â ñèñòåìå. Õîòÿ íàäî ó÷åñòü ñëåäóþùåå. Åñëè âû âûäåëèòå íà âûõîä ñëåøêîì íîãî áèòîâ, òî âû èñïîëüçóåòå â êà÷åñòâå ãåíåðàòîðà ñëó÷àéíûõ ÷èñåë áûñòðîå ïðåîáðàçîâàíèå Ôóðüå è ðàñêðóòêà ïîëó÷èòü îïðåäåëåííóþ ïðåäñêàçóåìîñòü. È ëó÷øå ñíîâà è ñíîâà ÷èòàòü îäèí è òîò æå äèñêîâûé áëîê, ÷òîáû âàì íå ïðèøëîñü ôèëüòðîâàòü ñòðóêòóðó, èñòî÷íèêîì êîòîðîé ÿâëÿåòñÿ ïëàíèðîâùèê äèñêà. Ðåàëèçàöèÿ òàêîé ñèñòåìû ïîçâîëÿëà ïîëó÷àòü îêîëî 100 áèòîâ â ìèíóòó [439].

Èñïîëüçîâàíèå òàéìåðà êîìïüþòåðà

Åñëè âàì íóæåí îäèí ñëó÷àéíûé áèò (èëè äàæå íåñêîëüêî), âîñïîëüçóéòåñü ìëàäøèì çíà÷àùèì áèòîì ëþáîãî ðåãèñòðà òàéìåðà. Â ñèñòåìå UNIX îí ìîæåò áûòü íå ñëèøêîì ñëó÷àéíûì èç-çà ðàçëè÷íîé âîçìîæíîé ñèíõðîíèçàöèè, íî íà íåêîòîðûõ ïðåñíîâëíûõ êîìïüþòåðàõ ýòî ðàíòàåò.

Íå ñòîèò èçâëåêàòü òàêèì îáðàçîì ñëèøêîì ìíîãî áèòîâ. Âûïîëíåíèå ìíîãî ðàç îäíîé è òîé æå ïðîöåäóðû ïîñëåäîâàòåëüíî ìîæåò ëåãêî ñìåñòèòü áèòû, äåíåðèðîâàííûå ýòèì ñïîñîáîì. Íàïðèìåð, åñëè âûïîëíåíèå êàæäîé ïðîöåäóðû ãåíåðàöèè áèòà çàíèìàåò ÷åòíî òèêîâ òàéìåðà, íà âûõîäå âàøåãî äåíåðàòîðà áóäåò áåñêîíå÷íàÿ ïîñëåäîâàòåëüíîñòü îäèíàêîâûõ áèòîâ. Åñëè âûïîëíåíèå êàæäîé ïðîöåäóðû äåíåðàöèè áèòà çàíèìàåò íå÷åòíî òèêîâ òàéìåðà, íà âûõîäå âàøåãî äåíåðàòîðà áóäåò áåñêîíå÷íàÿ ïîñëåäîâàòåëüíîñòü ÷åðåäóþùèõñÿ îäèíàêîâûõ áèòîâ. Äàæå åñëè çàâèñèìîñòü íå òàê î÷åâèäíà, ïîëó÷àþùèéñÿ áèòîâûé ïîòîê áóäåò äàëåê îò ñëó÷àéíîãî. Îäèí ãåíåðàòîð ñëó÷àéíûõ ÷èñåë ðàíòàåò ñëåäóþùèì îáðàçîì [918]:

> Íàø ãåíåðàòîð äèñêðåòèçèðóåò ñëó÷àéíûõ ÷èñåë . . . ðàíòàåò, óñòàíàâëèâàÿ áóäèëüíèê è çàòåì áûñòðî èíèöèàëèçèðóÿ ðåãèñòð ñ÷åò÷èêà ïðîöåññîðà äî òåõ ïîð, ïîêà íå ïðîèçîéäåò ïðåðûâàíèå. Äàëåå âû ïîëó÷àåòå XOR ñîäåðæèìîãî ðåãèñòðà è ñîäåðæèìîãî áàéòà âûõîäíîãî áóôåðà (äàííûå ðåãèñòðà óñëîæíÿò äî 8 áèòîâ). Ïîñëå òîãî, êàê áóäåò çàïîëíåí êàæäûé áàéò âûõîäíîãî áóôåðà, áóôåð ïîâòîðÿåòñÿ äàëüíîñòü îäèíàêîâûõ áèòîâ. Åñëè âûïîëíåíèå êàæäîé ïðîöåäóðû åñòåñòâåííûì îáðàçîì ïðèâîäèò ê ñëó÷àéíîñòè ÷åòíî òèêîâ òàéìåðà, íà âûõîäå âàøåãî äåíåðàòîðà áóäåò áåñêîíå÷íàÿ ïîñëåäîâàòåëüíîñòü ÷åðåäóþùèõñÿ îäèíàêîâûõ áèòîâ. Äàæå åñëè çàâèñèìîñòü íå òàê î÷åâèäíà, ïîëó÷àþùèéñÿ áèòîâûé ïîòîê áóäåò äàëåê îò ñëó÷àéíîãî. Îäèí ãåíåðàòîð ñëó÷àéíûõ ÷èñåë ðàíòàåò ñëåäóþùèì îáðàçîì [918]:
>
> Íàø ãåíåðàòîð äèñêðåòèçèðóåò ñëó÷àéíûõ ÷èñåë . . . ðàíòàåò, óñòàíàâëèâàÿ áóäèëüíèê è çàòåì áûñòðî èíèöèàëèçèðóÿ ðåãèñòð ñ÷åò÷èêà ïðîöåññîðà äî òåõ ïîð, ïîêà íå ïðîèçîéäåò ïðåðûâàíèå. Äàëåå âû ïîëó÷àåòå XOR ñîäåðæèìîãî ðåãèñòðà è ñîäåðæèìîãî áàéòà âûõîäíîãî áóôåðà, áóôåð ïîâòîðÿåòñÿ äàëüíîñòü îäèíàêîâûõ áèòîâ. Åñëè âûïîëíåíèå êàæäîé ïðîöåäóðû ãåíåðàòîðà áóäåò çàíèìàåò íå÷åòíî òèêîâ òàéìåðà, íà âûõîäå âàøåãî äåíåðàòîðà áóäåò áåñêîíå÷íàÿ ïîñëåäîâàòåëüíîñòü ÷åðåäóþùèõñÿ îäèíàêîâûõ áèòîâ. Äàæå åñëè çàâèñèìîñòü íå òàê î÷åâèäíà, ïîëó÷àþùèéñÿ áèòîâûé ïîòîê áóäåò äàëåê îò ñëó÷àéíîãî. Îäèí ãåíåðàòîð ñëó÷àéíûõ ÷èñåë ðàíòàåò ñëåäóþùèì îáðàçîì [918]:

Ýòî ìåòîä î÷åíü ÷óâñòâèòåëåí ê ñëó÷àéíîñòè ñèñòåìíûõ ïðîöåññîâ è ââîäíî-âûâîäíûõ ìåòîäîâ. Ïðè òàêîì ïîäõîäå ïîëó÷åííûå ïîñëåäîâàòåëüíîñòè ìîãóò ñîäåðæàòü ñèñòåìíûå øóìû, ïîâòîðíûå øàáëîíû ñëó÷àéíûõ äàííûõ è äàæå ïîëíîñòüþ ïîâòîðÿòüñÿ ïîñëå íåêîòîðîãî ïåðèîäà âðåìåíè. Ýòî ïðèâîäèò ê ýôôåêòó ïåðâîíà÷àëüíîãî ïîäáîðà ïîêîëåíèé, êîãäà ïîòîìêè ïîëó÷àþò ìåíüøå ïîëåçíîé èíôîðìàöèè, ÷åì èõ ðîäèòåëè. Çàòåì âåñü ïðîöåññ ïîâòîðÿåòñÿ òðè ðàçà. Íàêîíåö ïîñëå ïðåîáðàçîâàíèé äâà ñàìûõ ñëó÷àéíûõ áèòà ðåãèñòðà ñ÷åò÷èêà ïîâòîðÿþòñÿ íà êàæäûé ñèìâîë áóôåðà. Òî åñòü ïðîèñõîäèò 4*n* ïðåîáðàçîâàíèé, äëÿ *n* - ÷èñëî íóæíûõ ñëó÷àéíûõ áèòîâ.

Ýòîò ìåòîä î÷åíü ÷óâñòâèòåëåí ê ñëó÷àéíîñòè ñèñòåìíûõ ïðåðûâàíèé è êâàíòîâàíîñòè òàéìåðà. Ïðè òåñòèðîâàíèè íà ðåàëüíûõ UNIX-ìàøèíàõ ðåçóëüòàò áûë î÷åíü íåïëîõ.

Èçìåðåíèå ñêðûòîãî ñîñòîÿíèÿ êëàâèàòóðû

Ïðîöåññ ïå÷àòàíèÿ è ñëó÷àéí, è íåñëó÷àéí. Î í äîñòàòî÷íî íåñëó÷àéí, ÷òîáû åãî ìîæíî áûëî èñïîëüçîâàòü äëÿ èäåíòèôèêàöèè ïå÷àòàþùåãî ÷åëîâåêà, íî îí äîñòàòî÷íî ñëó÷àéí, ÷òîáû åãî ìîæíî áûëî èñïîëüçîâàòü äëÿ ãåíåðàòîðà ñëó÷àéíûõ áèòîâ. Èçìåðüòå âðåìÿ ìåæäó ïîñëåäîâàòåëüíûìè íàæàòèÿìè êëàâèø, çàòåì âîñïîëüçóéòåñü ìëàäøèìè çíà÷àùèìè áèòàìè ýòèõ èçìåðåíèé. Ýòè áèòû îêàçûâàþñÿ äîñòàòî÷íî ñëó÷àéíûìè. Ýòîò ìåòîä íå ðàáîòàåò íà UNIX-òåðìèíàëàõ, òàê êàê íàæàòèÿ êëàâèø ïðèâîäÿò íåêîòîðîå âðåìÿ, ÷òî îíè ìîãóò ïîïàñòü â ñëåäóþùèé âàøåé ïðîãðàììå, ïðîïóñêàÿ ÷åðåç ôèëüòðû è äðóãèå ìåõàíèçìû, íî ýòî áóäåò ðàíòàòü íà áîëüøèíñòâå ïðîãðàììíûõ êîìïüþòåðîâ.

Â èäåàëå âû äîëæíû ïî êàæäîìó íàæàòèþ êëàâèøè ãåíåðèðîâàòü òîëüêî îäèí áèò. Èñïîëüçîâàíèå áîëüøåãî êîëè÷åñòâà áèòîâ ìîæåò ñìåñòèòü ðåçóëüòàòû â çàâèñèìîñòè îò íàâûêîâ ìàøèíèñòêè. Õîòÿ íàòóðàëüíàÿ ïîñëåäîâàòåëüíîñòü 100 ñëîâ â ìèíóòó èëè îêîëî òîãî, åñëè åñòü âðåìÿ äëÿ ãåíåðàòîðà êëþ÷à, ãëóïî ïðîñòî ìàøèíèñòêè ïå÷àòàòü òåêñò 100 ñëîâ â ìèíóòó ðåçóëüòàòû ðàçíûõ ïîëüçîâàòåëåé áîëåå ïîõîæè íà áîëüøèíñòâî ïðîãðàìì, íî ýòî áóäåò ðàíòàòü íà áîëüøèíñòâå ïî÷òîâûõ ãåíåðàòîðàõ â êà÷åñòâå îñíîâû äëÿ ïîïûòêè ê ïîýòè÷åñêîìó ðàçëè÷åíèþ.

Ñìåùåíèÿ è êîððåëÿöèè

Ãëàâíîé ïðîáëåìîé ïîäîáíûõ ñèñòåì ÿâëÿþòñÿ âîçìîæíûå çàêîíîìåðíîñòè â ãåíåðèðóåìîé ïîñëåäîâàòåëüíîñòè. Èñïîëüçóåìûå ôèçè÷åñêèå ïðîöåññû ìîãóò áûòü íåëèíåéíûìè, íî ìåæäó ôèçè÷åñêèì ïðîöåññîì è êîìïüþòåðîì íàõîäÿòñÿ ðàçëè÷íûå èíòóèöèîííûå ìîäåëè, ïðèáëèæàþùèå ýòè ïðîöåññû. Ýòè èíòóèöèîííûå ìîäåëè ëåãêî ïðåîáðàçîâàòü â ãåíåðàòîðû ïñåâäîñëó÷àéíûõ áèòîâ, êîòîðûå áóäóò ïðîõîäèòü ìíîãî òåñòîâ íà ñëó÷àéíîñòü. Ýòè èíòóèöèîííûå ìîäåëè ìîãóò ïîìî÷ü ïîíÿòü ïðèíöèïû ðàáîòû ýòèõ ãåíåðàòîðîâ è ïîìî÷ü ïðåäñêàçàòü èõ ñëàáûå ìåñòà.

Ñïîñîáîì óñòðàíèòü **ñìåùåíèå**, èëè îòêëîíåíèå, ÿâëÿþùèõ XOR íåñêîëüêèõ áèòîâ äðóã ñ äðóãîì. Åñëè ñëó÷àéíûé áèò ñìåùåí ê 0 íà âåëè÷èíó *e*, òî âåðîÿòíîñòü 0 ìîæíî çàïèñàòü êàê:

$P(0) = 0.5 + e$

XOR äâóõ èç òàêèõ áèòîâ äàåò:

$P(0) = (0.5 + e)^2 + (0.5 - e)^2 = 0.5 + 2e^2$

Òå æå âû÷èñëåíèÿ äëÿ XOR 4 áèòîâ äàþò:

$P(0) = 0.5 + 8e^4$

XOR *m* áèòîâ ýêñïîíåíöèàëüíî ñõîäèòñÿ ê ðàâíîé âåðîÿòíîñòè 0 è 1. Åñëè èçâåñòíî ìàêñèìàëüíîå ñìåùåíèå, êîòîðîå äîïóñêàåòñÿ â âàøåì ïðèëîæåíèè, âû ìîæåòå âû÷èñëèòü, ñêîëüêî áèòîâ âàì íóæíî îáúåäèíèòü ñ ïîìîùüþ XOR, ÷òîáû óìåíüøèòü ñìåùåíèå äî ýòîãî çíà÷åíèÿ.

Åùå ëó÷øå ðàññìàòðèâàòü áèòû ïî ïàðíî. Åñëè 2 áèòà îäèíàêîâû îòáðîñüòå èõ è âçãëÿíèòå íà ñëåäóþùóþ ïàðó. Åñëè 2 áèòà ðàçëè÷íû, èñïîëüçóéòå ïåðâûé áèò â êà÷åñòâå âûõîäà ãåíåðàòîðà. Ýòî ïîëíîñòüþ óñòðàíÿåò ñìåùåíèå. Äðóãèå ìåòîäû óìåíüøåíèÿ ñìåùåíèÿ èñïîëüçóþò ðàñïðåäåëåíèå ïåðåõîäîâ ñæàòèå è áûñòðîå ïðåîáðàçîâàíèå Ôóðüå [511].

Ïîòåíöèàëüíîé ïðîáëåìîé îáîèõ ìåòîäîâ ÿâëÿåòñÿ òî, ÷òî ïðè íàëè÷èè **êîððåëÿöèè** ìåæäó ñîñåäíèìè áèòàìè ýòè ìåòîäû óâåëè÷èâàþò ñìåùåíèå. Îäíèì èç ñïîñîáîâ èñïðàâèòü ýòî ÿâëÿåòñÿ èñïîëüçîâàíèå íåñêîëüêèõ ñëó÷àéíûõ èñõîäíûõ áèòîâ. Âîçüìèòå äâà ñëó÷àéíûõ èñõîäíûõ áèòà è âûïîëíèòå XOR áèòîâ äðóã ñ äðóãîì èëè âîçüìèòå äâà ñëó÷àéíûõ èñõîäíûõ áèòà è âçãëÿíèòå íà èõ áèòû ïî ïàðíî.

Íàïðèìåð, âîçüìèòå ðàäèàòîðíûé èñòî÷íèê è ïðèñâîéòå ñ÷åò÷èê Åéãåðà ê âàøåìó êîìïüþòåðó. Âîçüìèòå ïàðó øóìÿùèõ äèîäîâ è çàïèñûâàéòå â êà÷åñòâå ñîáòèé êàæäûé ïðåâûøåíèå îïðåäåëåííîãî çíà÷åíèÿ. Èçìåðüòå àòìîñôåðíûé øóì. Èçâëåêèòå èç êàæäîãî èñòî÷íèêà ñëó÷àéíûé áèò è âûïîëíèòå èõ XOR äðóã ñ äðóãîì, ïîëó÷àÿ ñëó÷àéíûé áèò. Âîçìîæíîñòè áåñêîíå÷íû.

Îäíî òî, ÷òî ãåíåðàòîð ñëó÷àéíûõ ÷èñåë ñìåùåí íà îäÿçàòåëüíî îçíà÷àåò åãî ïðåäñêàçóåìîñòü. Ýòî òîëüêî îçíà÷àåò, ÷òî îí ìåíåå áåçîïàñåí. Íàïðèìåð, ðàññìîòðèì ïðîáëåìó Àëèñû, ãåíåðèðóþùåé 168-áèòîâûé êëþ÷ äëÿ òðîéíîãî DES. A âñå, ÷òî ó íåå åñòü, - ýòî ãåíåðàòîð ñëó÷àéíûõ áèòîâ ñî ñìåùåíèåì ê 0: ñ âåðîÿòíîñòüþ 55 ïðîöåíòîâ îí âûäàåò íóëè è ñ âåðîÿòíîñòüþ 45 ïðîöåíòîâ - åäèíèöû. Ýòî îçíà÷àåò, ÷òî ýíòðîïèÿ íà áèò êëþ÷à ñîñòàâèò òîëüêî 0.99277 (äëÿ èäåàëüíîãî ãåíåðàòîðà îíà ðàâíà 1). Ìýëîðè, ïûòàÿñü ðàñêðûòü êëþ÷, ìîæåò îïòèìèçèðîâàòü âûïîëíÿåìûå ãåíåðàòîðû ñëåäóþùåé ãðóïïû ñèñòåì, ïîñòðîåííûõ íà ðàâíî 1). Ìýëîðè, ïûòàÿñü ðàñêðûòü êëþ÷, ìîæåò îïòèìèçèðîâàòü âûïîëíÿåìûå ãåíåðàòîðû ñëåäóþùåé ãðóïïû ñèñòåì, ïîñòðîåííûõ íà ðàâíî 2^{109} ïîïûòîê. Ïðè îòñóòñòâèè ñìåùåíèÿ Ìýëîðè ïîòðåáóåòñÿ 2^{111} ïîïûòîê. Ïîëó÷åííûé êëþ÷ ìîæåò áûòü íåïðàâèëüíûì, íî ýòî ïðàêòè÷åñêè íåîòëè÷èì.

Èçâëå÷åíèå ñëó÷àéíîñòè

Â îáùåì ñëó÷àå ëó÷øèé ñïîñîá âåíåðèðîâàòü ñëó÷àéíûå ÷èñëà - íàéòè áîëüøîå êîëè÷åñòâî êàæóùèõñÿ ñëó÷àéíûì îñíîâûâàÿ è èçâëå÷ü ñëó÷àéíîñòü èç íèõ. Ýòà ñëó÷àéíîñòü ìîæåò õðàíèòüñÿ â íàêîïèòåëå è èçâëåêàòüñÿ ïðè íåîáõîäèìîñòè. .Îäíîíàïðàâëåííûå õýø-ôóíêöèè ïðåðàñíî ïîäõîäÿò äëÿ ýòîãî. Îíè áûñòðû, ïîýòîìó âû ìîæåòå ïðîóñêàòü áèòû ÷åðåç íèõ, íå ñëèøêîì çàâiòÿñü î ïðîçâîäèòåëüíîñòè è ïîäîáðàòü íàáîð áèòîâ, êîòîðûé íàèáîëåå âåðîÿòíûå ñ÷èòàëà ñëó÷àéíûìè. Ïîïðîáóéòå õýøèðîâàòü ïî÷òè âñå, ÷òî âàì êàæåòñÿ õîòü ÷óòü-÷óòü ñëó÷àéíûì. Íàïðèìåð:

— Êîïèÿ êàæäîãî íàæàòèÿ íà êëàâèøè

— Êîìàíäû ìûøè

— Íîìåð ñåêòîðà, âðåìÿ äíÿ è çàäåðæêà ïîèñêà äëÿ êàæäîé äèñêîâîé îïåðàöèè

— Äåéñòâèòåëüíîå ïîëîæåíèå ìûøè

— Íîìåð òåêóùåé ñòðîêè ðàçâåðòêè ìîíèòîðà

— Ñîäåðæàíèå äéñêâèòåëüíîé âûâîäèìîé íà ýêðàí èçîáðàæåíèÿ

— Ñîäåðæàíèå FAT-òàáëèö, òàáëèö ÿäðà, è ò.ä.

— Âðåìåíà äîñòóïà/èçìåíåíèÿ /dev/tty

— Çàãðóçêà ïðîöåññîðà

— Âðåìåíà ïîñòóïëåíèÿ ñåòåâûõ ïàêåòîâ

— Âûõîä ìèêðîôîíà

— /dev/audio áåç ïðèñòàèíåíííãî ìèêðîôîíà

Åñëè âàøà ñèñòåìà èñïîëüçóåò ðàçëè÷íûå êðèñòàëëû-îñöèëëÿòîðû äëÿ ñâîåãî ïðîöåññîðà è ÷àñîâ, ïîïûòàéòåñü ñ÷èòûâàòü âðåìÿ äíÿ â ïëîòíî öèêëå. Â íåêîòîðûõ (íî íå âñåõ) ñèñòåìàõ ýòî ïðèâåäåò ê ñëó÷àéíûì êîëåáàíèÿì ôàçû ìåæäó äâóìÿ îñöèëëÿòîðàìè.

Òàê êàê ñëó÷àéíîñòü â ýòèõ ñîâûòèÿõ îïðåäåëÿåòñÿ ñèíõðîíèçàöèåé îñöèëëÿòîðîâ, èñïîëüçóéòå ÷àñû ñ êâàðöåâûì ìåõàíèçìîì âðåìåíè. Â ñòàíäàðòíîì PC èñïîëüçóåòñÿ ìèêðîñõåìà òàéìåðà Intel 8254 (ëèê ýêâèâàëåíòíàÿ), ðàáîòàþùàÿ íà òàêòîâîé ÷àñòîòå 1.1931818 ÌÃö, ïîýòîìó íåïîñðåäñòâåííî ñ÷èòûâàíèå ðåãèñòðà ñ÷åò÷èêà äàñò ðàçðåøåíèå â 838 íàíîñåêóíä. ×òîáû èçáåæàòü ñìåùåíèÿ ðåçóëüòàòîâ, íå èñïîëüçóéòå â êà÷åñòâå èñòî÷íèêà ñîáûòèé ïðåðûâàíèå òàéìåðà. Âîò êàê âûãëÿäèò ýòîò ïðîöåññ íà ÿçûêå C ñ MD5 (ñì. ðàçäåë 18.5) â êà÷åñòâå õýø-ôóíêöèè:

```
char Randpool[16];

/* ×àñòî âûçûâàåòñÿ äëÿ øèðîêîãî ìíîæåñòâà ñëó÷àéíûõ èëè ïſåóñëó÷àéíûõ ñèñòåìíûõ ñîáûòèé äëÿ to
churn the randomness pool . Òî÷íûé ôîðìàò è äëèíà randevent íå èìåþò çíà÷åíèÿ, ïîêà åãî ñîäðæàíèå
```

```
ÿâëÿåòñÿ â íåêîòîðîé ìåðå ÷åì-òî íåïðåäñêàçóåìûì. */
   void churnrand(char *randevent,unsigned lnt randlen) {
        MD5_CTX md5;
        MD5Init(&md5);
        MD5Update(&md5, Randpool , sizeof(Randpool));
        MD5Update(&md5 , randevent , randlen );
        MD5Final(Randpool,&md5);
   }
```

Ïîñëå äîñòàòî÷íûõ âûçîâîâ churnrand() íàêîïëåíèÿ äîñòàòî÷íîé ñëó÷àéíîñòè â Randpool, ìîæíî ãåíåðèðîâàòü èç ýòîãî ñëó÷àéíûå áèòû. MD5 ñíîâà ñòàíîâèòñÿ ïîëåçíîé, â ýòîò ðàç â êà÷åñòâå ãåíåðàòîðà ïñåâäîñëó÷àéíîãî áàéòîâîãî ïîòîêà, ðàáîòàþ ùåãî â ðåæèìå ñ÷åò÷èêà.

```
   long Randcnt;
   void genrand(char *buf,unsigned int buflen) {
        MD5_CTX md5;
        char tmp[16];
        unsigned int n;
        while(buflen != 0) {
                /* Ïóë õýøèðóåòñÿ ñ÷åò÷èêîì */
                MD5Init(&md5);
                MD5Update(&md5, Randpool, sizeof(Randpool));
                MD5Update(&md5,(unsigned char *)&Randcnt,sizeof(Randcnt));
                MD5Final(tmp,&md5);
                Randcnt++; /* Èíêðåìåíòèðóåì ñ÷åò÷èê */
                /*Êîïèðóåì 16 èëè çàïðîøåííîå ÷èñëî áàéòîâ, åñëè îíî ìåíüøå 16, â áóôåð ïîëüçîâàòåëÿ*/
                n = (buflen < 16) ? buflen : 16;
                memcpy(buf, tmp, n);
                buf += n ;
                buflen -= n;
        }
   }
```

Ïî ìíîãèì ïðè÷èíàì õýø-ôóíêöèÿ èìååò êëþ÷åâîå çíà÷åíèå. Âî ïåðâûõ îíà îáåñïå÷èâàåò ïðîñòîé ñïîñîá äåíåðèðîâàòü ïðîèçâîëüíîå êîëè÷åñòâî ïñåâäîñëó÷àéíûõ, íå âûçûâàÿ âñÿêèé ðàç churnrand(). Íà äåëå, êîãäà çàïàñ â íàêîïèòåëå ïîäîáàëè ê êîíöó, ñèñòåìà ïîñòåïåííî ïðåðàùàåòñÿ ñëó÷àéíîñòè ê ïðàêòè÷åñêîé. Â ýòîì ñëó÷àå ñòàíîâèòñÿ *òåîðåòè÷åñêè* âîçìîæíûì èñïîëüçîâàòü ðåçóëüòàò âûçîâà genrand() äëÿ îïðåäåëåíèÿ ïðåäûäóùåãî èëè ïîñëåäóþùåãî ðåçóëüòàòà. Íî äëÿ ýòîãî ïîòðåáóåòñÿ èíâåðòèðîâàòü MD5, ÷òî âû÷èñëèòåëüíî íåâîçìîæíî.

Ýòî âàæíî, òàê êàê ïðîöåäóðà íåçâåñòíî, ÷òî äëåàòñÿ ïîòî ñëó÷àéíûìè, êîòîðûå îíà âîçâðàùåò. Îäíî âûçîâ ïðîöåäóðû ìîæåò ãåíåðèðîâàòü ñëó÷àéíå ÷èñëî äëÿ ïðîïîêëà, êîòîðîå ïîñûëàòñÿ â ÿâíîì âèäå, âîçìîæíî â îòâåò íà ïðÿìîé çàïðîñ âçëîìùèêà. À ñëåäóþùèé âûçîâ ìîæåò ãåíåðèðîâàòü ñåêðåòíûé êëþ÷ äëÿ ñîâñåì äðóãîãî ñåàíñà ñâÿçè, â ñóòü êîòîðîãî è õî÷åò ïðîíèêíóòü âçëîìùèê. Î÷åâèäíà âàæíîñòü òîãî, ÷òîáû âçëîìùèê íå ñìîã ïîëó÷èòü ñåêðåòíûé êëþ÷, èñïîëüçóÿ ïîäîáíóþ ñõåìó äåéñòâèé.

Íî îñòàåòñÿ îäíà ïðîáëåìà. Ïðæäå, ÷åì â ïåðâûé ðàç áóäåò âûçâàíà genrand() â ìàññèâå Randpool[] äîëæíî áûòü íàêîïëåíî äîñòàòî÷íî ñëó÷àéíûõ äàííûõ. Åñëè ñèñòåìà êàêîå-òî âðåìÿ ðàáîòàëà ñ ëîêàëüíûì ïîëüçîâàòåëåì, ÷òî-òî ïå÷àòàþùèì íà êëàâèàòóðå, òî ïðîáëåì íåò. Íî êàê íàñ÷åò íåçàâèñèìî ñèñòåì, êîòîðàÿ ïðåäíàçíà÷åíà äëÿ ðàáîòû ñ ïîëüçîâàòåëåì, ÷òî-òî ïå÷àòàþùèì íà êëàâèàòóðå, íå îáðàùàÿ âíèìàíèÿ íè íà êàêèå äàííûå êëàâèàòóðû èëè ìûøè?

Íî åñòü îäíà òðóäíîñòü. Â êà÷åñòâå ÷àñòè÷íîãî ðåøåíèÿ ìîæíî ïîòðåáîâàòü, ÷òîáû ïîñëå ñàìîé ïåðâîé çàãðóçêè îïåðàöèîííîé ñèñòåìû íà êëàâèàòóðå è ñîçäàë íà äèñêå ñòàðòîâûéôàéë ïåðâ âûãðóçêîé îïåðàöèîííîé ñèñòåìû, ÷òîáû â õîäå ïåðåçàãðóçêè èñïîëüçîâàëèñü ñëó÷àéíûå äàííûå, ïåðåäàííûå â Randseed[]. Íî íå ñîõðàíÿéòå íàïîñðåäñòâåííî ñàì Randseed[]. Âçëîìùèê, êîòîðîìó óäàñòñÿ çàïîëó÷èòü ýòîò ôàéë, ñìîæåò îïðåäåëèòü âñå ðåçóëüòàòû genrand() ïîñëå ïîñëåäíåãî îáðàùåíèÿ ê churnrand() ïðåæäå, ÷åì ýòîò ôàéë áóäåò ñîçäàí.

Ðåøåíèåì ýòîé ïðîáëåìû ÿâëÿåòñÿ õýøèðîâàíèå ìàññèâà Randseed[] ïåðåä ñîõðàíåíèåì, ìîæåò äàæå âûçîâîì genrandO. Ïðè ïåðåçàãðóçêå ñèñòåìû âû ñ÷èòûâàåòå äàííûå èç ñòàðòîâîãî ôàéëà, ïåðåäàåòå èõ

churnrand(), à çàòåì íåìåäëåííî ñòèðàåòñÿ èõ. Ê ñîæàëåíèþ ýòî íå óñòðàíÿåò óãðîçû òîãî, ÷òî çëîóìûøëåííèê äîáóäåò ôàéë ìåæäó ïåðåçàãðóçêàìè è èñïîëüçóåò åãî äëÿ ïðåäñêàçàíèÿ áóäóùèõ çíà÷åíèé ôóíêöèè genrand(). ß íå âèæó èíîãî ðåøåíèÿ ýòîé ïðîáëåìû êðîìå, êàê ïîäæäàòü íàêîïëåíèÿ äîñòàòî÷íîãî êîëè÷åñòâà ñëó÷àéíûõ ñîáûòèé, ñëó÷èâøèõñÿ ïîñëå ïåðåçàãðóçêè, ïðåæäå, ÷åì ïîçâîëèòü genrand() âûäàâàòü ðåçóëüòàòû.