

Plokkšifrid

Ahto Buldas

Motivatsioon

Jadašifritel on mitmeid puudusi, mis teevad nad paljudes olukordades eba-praktiliseks. Olulisimad probleemid on järgmised:

- **Sünkroniseermisvajadus.** Kui bitt läheb edastusel kaduma, siis ei saa vastuvõtja saatjast enam aru. Näiteks \oplus -tüüpi šifrite korral võivad võtmebitid minna “nihkesse” ja tulemusena üritab vastuvõtja kasutada vale võtmebitte.
- **Mahuline efektiivsus.** Ülalmainitud probleemist jagu saamiseks võib iga krüpteeritud biti varustada unikaalse indeksiga, mis ütleb vastuvõtjale, mitmenda biti krüptogrammiga on tegemist. See aga suurendab tunduvalt edastatava koodi mahtu – suur protsent edastatavast koodist on indeksid.
- **Arvutuslik efektiivsus.** Isegi kui kasutada indekseid, kulub vastuvõtjal võtmejada generaatori uuesti samasse olekusse viimiseks teatud aeg. Halvimal juhul tuleb alustada kõigi võtmebittide genereerimist otsast peale. Eriti oluliseks muutub probleem siis, kui sõnumeid edastatakse plokkide kaupa, kusjuures plokkide järjestus ei pruugi edastusel säilida.

Plokkšifri idee

Siit tuleneb vajadus krüpteerida andmeid suuremate tükide kaupa ja muuta võtmejada generaatorid selliseks, mis lubaks neid kiiresti ümber seada suvalise järjekorranumbriga biti dekrüpteerimiseks, s.t. i -nda võtmemärgi x_i arvutamine peaks olema võimalik efektiivselt arvutatava funktsiooniga indeksist $x_i = f_x(i)$, kus x on mingi fikseeritud pikkusega lähtevõti. See vajadus viib nn. *pseudojuhuslike funktsioonide generaatoriteni*. Osutub, et pseudojuhuslike funktsioonide generaatorit saab efektiivselt konstrueerida pseudojuhuarvude generaatorist.

Käesolevas loengus defineerime esmalt *plokkšifri* mõiste, seejärel esitame *pseudojuhusliku funktsiooni* mõiste ja selle konstruktsiooni lähtudes tavalisest pseudojuhuarvude generaatorist. Seejärel esitame plokkšifri konstruktsiooni lähtudes pseudojuhuslike funktsioonide generaatorist. Loengu lõpus uurime üht praktikas laialt kasutatavat võtet efektiivsete plokkšifrite konstrueerimiseks – nn *Feistel konstruktsiooni* ja uurime selle turvalisust.

Plokkšifri definitsioon

Plokkšiffer koosneb krüpteerimisalgoritmist E ja dekrüpteerimisalgoritmist D , mis mõlemad kasutavad parameetrina salajast võtit $x \in \{0, 1\}^n$. Eeldame, et kõik osalevad pooled salvestavad võtme x oma privaadmälusse ja seega on sobilik võtta turvaparameetriks n .

$$E: \{0, 1\}^n \times \{0, 1\}^{\ell(n)} \times \{0, 1\}^{q(n)} \rightarrow \{0, 1\}^{k(n)}$$
$$D: \{0, 1\}^n \times \{0, 1\}^{\ell(n)} \times \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{q(n)} .$$

Kasutame tähistusi $E_x(i, m) = E(x, i, m)$ ja $D_x(i, m) = D(x, i, m)$.

Korrektus: iga $x \in \{0, 1\}^n$, $i \in \{0, 1\}^{\ell(n)}$ ja $m \in \{0, 1\}^{q(n)}$ korral:

$$D_x(i, E_x(i, m)) = m .$$

Sõnumibloki $m \in \{0, 1\}^{q(n)}$ saatmiseks valitakse alati unikaalne indeks $i \in \{0, 1\}^{\ell(n)}$, mis ei ole esinenud ühegi varasema bloki krüpteerimisel. Seejärel arvutatakse $e = E_x(i, m)$ ja saadetakse avaliku kanali kaudu paar (i, e) .

Vastane (M, P, A) ja ründestsenaarium

$$M: \{0, 1\}^{\log(p(n))} \times \{0, 1\}^{\ell(n)} \times \{0, 1\}^{q(n)} \rightarrow \{0, 1\}^{k(n)}$$

$$P: \left(\{0, 1\}^{k(n)}\right)^{p(n)} \rightarrow \{0, 1\}^{\ell(n)+2q(n)}$$

$$A: \{0, 1\}^{s(n)} \times \left(\{0, 1\}^{k(n)}\right)^{p(n)} \rightarrow \{0, 1\} .$$

- Genereeritakse võti $x \leftarrow \{0, 1\}^n$ ja $r \leftarrow \{0, 1\}^{s(n)}$.
- M abil genereeritakse plokid $m = (m_1, \dots, m_{p(n)})$ ja vastavad krüptogrammide $e = (E_x(i_1, m_1), \dots, E_x(i_{p(n)}, m_{p(n)}))$, kasutades E_x oraaklina. See toimub iteratiivselt iga $j \in \{1, \dots, p(n)\}$ korral:

$$(i_j, m_j) = M(j, r; E_x(i_1, m_1), \dots, E_x(i_{j-1}, m_{j-1})) .$$

- $P(r, e)$, arvutab $\ell(n)$ -bitise indeksi $i' \notin \{i_1, \dots, i_{p(n)}\}$, ja kaks $q(n)$ -bitist sõnumit $m^0, m^1 \in \{0, 1\}^{q(n)}$.
- Valitakse juhuslik $b \leftarrow \{0, 1\}$ ja saadakse krüptogramm $e' = E_x(i', m^b)$.
- Vastane A , sisendiga (r, e, e') , püüab ära arvata bitti b .

Ründe edukus

Ründe edukus $\delta(n)$ defineeritakse järgmiselt:

$$\delta(n) = 2 \cdot \left| \Pr[A(r, e, e') = b] - \frac{1}{2} \right|.$$

Vastase (M, P, A) tööajaks $T(n)$ loetakse kõigi kolme algoritmi M , P ja A tööaegade summat, kusjuures algoritmi M tööajaks arvestatakse tema kõigi väljakutsete tööaegade summat. Öeldakse, et blokkšiffr on $S(n)$ -turvaline valitud avatekstiga ründe vastu, kui iga vastase (M, P, A) aeg-
edukus suhe $T(n)/\delta(n)$ on vähemalt $S(n)$.

Pseudojuhuslike funktsioonide generaatorid

Def.: Olgu $f: \{0, 1\}^n \times \{0, 1\}^{\ell(n)} \rightarrow \{0, 1\}^{k(n)}$ mingi \mathbf{P} -pere, kus esimene argument on salajane ja teine avalik, s.t. turvaparameter on n . Fikseeritud $x \in \{0, 1\}^n$ korral vaatleme $f(x, i)$ kui funktsiooni $f_x(i)$ argumentidiga i . Seega

$$f_x \in \text{Map} \left(\{0, 1\}^{\ell(n)}, \{0, 1\}^{k(n)} \right).$$

Olgu $X \leftarrow \{0, 1\}^n$ ja $F \leftarrow \text{Map} \left(\{0, 1\}^{\ell(n)}, \{0, 1\}^{k(n)} \right)$. Olgu A oraakliga vastane, mille väljund on ühebitine. Oraakli sisend on alati $\ell(n)$ -bitine, ja väljund $k(n)$ -bitine. Vastase A edukuseks pere f korral nimetatakse suurust

$$\delta(n) = \left| \Pr_X[A^{f^X}(n) = 1] - \Pr_F[A^F(n) = 1] \right|.$$

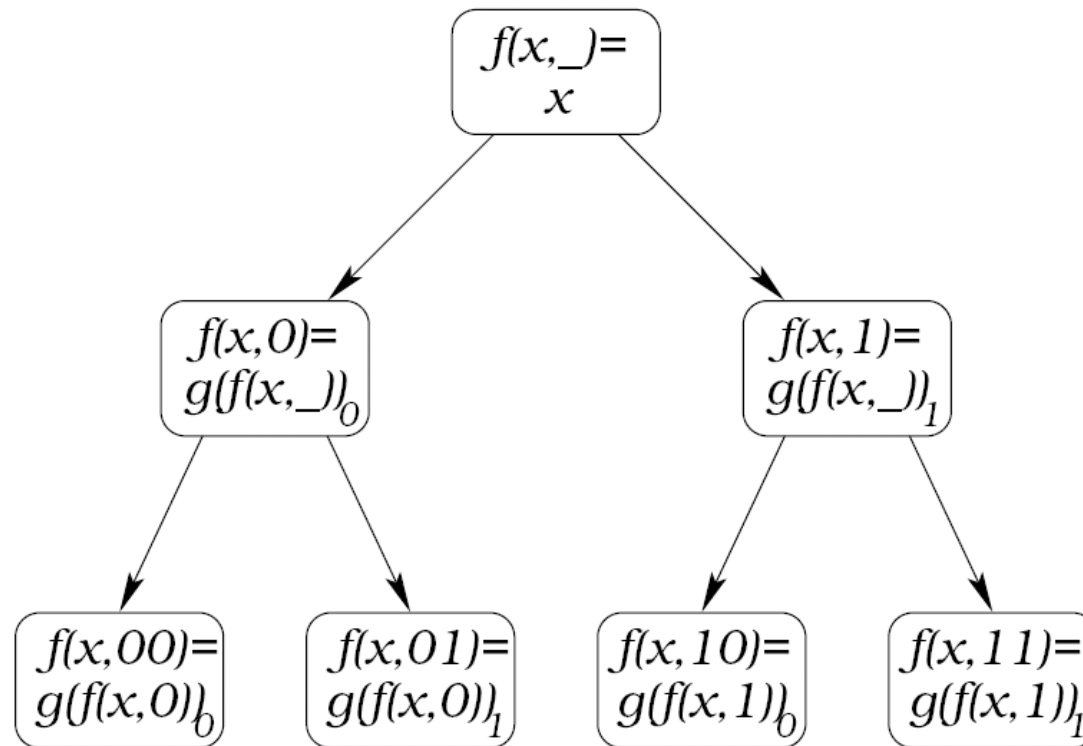
Öeldakse, et f on $S(n)$ -turvaline **pseudojuhuslike funktsioonide generaator**, kui iga vastase aeg-edukus suhe on vähemalt $S(n)$.

Seega, vastasele antakse musta kastina ette kas f_X või F ja ta peab kindlaks tegema kumba funktsioonidest must kast realiseerib. Järgnevalt näitame, et pseudojuhuslike funktsioonide generaatoreid saab konstrueerida pseudojuhuarvude generaatoritest.

Olgu $g: \{0, 1\}^n \rightarrow (\{0, 1\}^n)^2$ pseudojuhuarvude generaator, mis venitab sisendit kaks korda pikemaks. Edaspidi kasutame tähistust $g(x) = (g(x)_0, g(x)_1)$, kus $g(x)_0, g(x)_1 \in \{0, 1\}^n$. Konstrueerime g abil \mathbf{P} -pere $f: \{0, 1\}^n \times \{0, 1\}^{\leq \ell(n)} \rightarrow \{0, 1\}^{k(n)}$, kasutades rekursiivset definitsiooni, nii et iga $x \in \{0, 1\}^n$ korral: *

- $f(x, \perp) = x$,
- $f(x, i||0) = g(f(x, i))_0$
- $f(x, i||1) = g(f(x, i))_1$.

*Siin $\{0, 1\}^{\leq \ell(n)} = \bigcup_{i=0}^{\ell(n)} \{0, 1\}^i = \{\perp\} \cup \{0, 1\} \cup \{0, 1\}^2 \cup \dots \cup \{0, 1\}^{\ell(n)}$.



Teoreem: Kui g on pseudojuhuarvude generaator, siis f on pseudojuhuslike funktsioonide generaator. Reduktsioon on polünomiaalne.

Turvatõestus

Eristagu A primitiive f_X (kus $X \leftarrow \{0, 1\}^n$) ja $F \leftarrow \text{Map}(\{0, 1\}^{\ell(n)}, \{0, 1\}^n)$ edukusega $\delta(n)$ ja tööajaga $T(n)$. Olgu

$$q_0 = \Pr_X[A^{f_X}(n) = 1] \quad \text{ja} \quad q_1 = \Pr_F[A^F(n) = 1],$$

kusjuures eeldame üldisust kitsendamata, et $\delta(n) = q_0 - q_1$. Konstrueerime vastase S^A , mis eristab g väljundit ühtlasest jaotusest polünomiaalse reduktsiooni jaoks piisava edukus/aeg suhtega.

Olgu $m(n)$ maksimaalne oraakli väljakutsete arv, mida A^h teeb, kus h on suvaline funktsioon hulgast $\text{Map}(\{0, 1\}^{\ell(n)}, \{0, 1\}^n)$. Kuna $T(n)$ on halvima juhu tööaeg, siis $m(n) \leq T(n)$. Vastane S^A (saades sisendiks $z = (z_0, z_1) \in (\{0, 1\}^n)^2$ simuleerib A tööd, kasutades oraaklina teatud

“hübriidoraaklit” H , mis moodustatakse vastavalt sisendile z ja juhuarvule $k \leftarrow \{1, \dots, \ell(n) \cdot m(n)\}$.

Defineerime kõigepealt k -ndat järku ($k \in \{0, \dots, \ell(n)m(n)\}$) hübriidoraakli H_k järgmiselt. Olgu $s \in \{0, 1\}^n$ mingi konstant. Olgu p oraakli väljakutse järjekorranumber. Kirjeldame, kuidas käitub $H_k(i)$ sisendi $i = i_1 i_2 \dots i_n \in \{0, 1\}^{\ell(n)}$ korral. Eeldame, et oraakel H_k kasutab/arvutab massiivi

$$\chi: \{0, 1\}^{\leq \ell(n)} \rightarrow \{0, 1\}^n.$$

Massiivi esimene element algväärtustatakse $\chi(\square) := s$. Iga väljakutse arvutab teatud osa (mis võib ka tühi olla) massiivi χ elementidest, kusjuures varem (eelmiste väljakutsete ajal) arvutatud massiivi elemendid jäävad muutumatuks. See tähendab, me eeldame, et H_k “mäletab” kõiki oma eelmisi väljakutseid. Sisendi i korral arvutatakse järgmised elementide

paarid järgnevalt toodud järjestuses:

$$\begin{array}{ll}
 \chi(0) & \chi(1) \\
 \chi(i_1 0) & \chi(i_1 1) \\
 \chi(i_1 i_2 0) & \chi(i_1 i_2 1) \\
 \dots & \dots \\
 \chi(i_1 i_2 \dots i_{\ell(n)-1} 0) & \chi(i_1 i_2 \dots i_{\ell(n)-1} 1),
 \end{array}$$

kusjuures eelnevalt juba arvutatud paare enam ümber ei arvutata. Oraakli H_k väljundiks kohal i on alati $\chi(i)$.

Ükski oraakli väljakutse ei saa arvutada rohkem kui $\ell(n)$ uut paari. Seega kokku ei arvutata kunagi rohkem kui $\ell(n)m(n)$ uut paari. Oluline on märkida, et kui $(u||0, u||1)$ on uus paar, siis on väärtus $\chi(u)$ juba eelnevalt arvutatud.

Järgnevalt kirjeldame, kuidas $\chi()$ väärtuste arvutamine toimub. Oletame, et $(u||0, u||1)$ on järjekorras j -s uus paar. Kui $j \leq k$, siis genereeritakse

sõltumatult $\chi(u\|0) \leftarrow \{0, 1\}^n$ ja $\chi(u\|1) \leftarrow \{0, 1\}^n$. Kui aga $j > k$, siis võetakse

$$\chi(u\|0) = g(\chi(u))_0 \quad \text{ja} \quad \chi(u\|1) = g(\chi(u))_1.$$

Ehkki oraakli H_k väljund (erinevalt tavalisest funktsioonist) sõltub ka väljakutsete ajaloost, on lihtne veenduda, et lõppkokkuvõttes käitub H_k alati nagu mingi funktsioon $h \in \text{Map}(\{0, 1\}^{\ell(n)}, \{0, 1\}^n)$. Seega ei toimu ka arvutuses A^{H_k} kunagi rohkem kui $m(n)$ oraakli väljakutset.

On selge, et H_0 käitub identselt f_X -ga, kus $X \leftarrow \{0, 1\}^n$. Samuti on selge, et $H_{\ell(n)m(n)}$ on identne F -ga, kus $F \leftarrow \text{Map}(\{0, 1\}^{\ell(n)}, \{0, 1\}^n)$, sest kõik tema väärtused genereeritakse ühtlaselt ja juhuslikult. Olgu

$$p_k = \Pr[A^{H_k}(n) = 1].$$

Vastavalt äsjasele tähelepanekule $q_0 = p_0$ ja $q_1 = p_{\ell(n)m(n)}$, mistõttu võime kirjutada, et

$$(p_0 - p_1) + (p_1 - p_2) + \dots + (p_{\ell(n)m(n)-1} - p_{\ell(n)m(n)}) = q_0 - q_1 = \delta(n).$$

Seega, kui $k \leftarrow \{1, \dots, \ell(n)m(n)\}$, siis

$$\mathbf{E}_k[p_{k-1} - p_k] = \frac{\delta(n)}{\ell(n)m(n)}.$$

Defineerime iga $z = (z_0, z_1) \in (\{0, 1\}^n)^2$ korral oraakli H_k^z , mis käitub identselt oraakliga H_k , välja arvatud üks detail massiivi χ arvutamise skeemis, kus juhul $j = k$ (ja $(u||0, u||1)$ on j -s uus paar):

$$\chi(u||0) = z_0 \quad \text{ja} \quad \chi(u||1) = z_1.$$

Kui $z \leftarrow (\{0, 1\}^n)^2$, siis H_k^z käitub nagu H_k . Kui aga $z = g(x)$, kus $x \leftarrow \{0, 1\}^n$, siis H_k^z käitub nagu H_{k-1} (vt. Märkus). Järelikult kui defineerida vastane S^A sisendi $z = (z_0, z_1)$ korral järgmiselt:

- $S^A(z)$ genereerib juhuslikult $k \leftarrow \{1, \dots, \ell(n)m(n)\}$ ja
 - $S^A(z)$ tagastab väärtuse $A^{H_k^z}$,
- siis vastase S^A edukus on

$$\delta'(n) = \mathbf{E}_k [p_{k-1} - p_k] = \frac{\delta(n)}{\ell(n)m(n)}$$

ja tööaeg $T'(n) = n^{\mathcal{O}(1)} \cdot T(n)$, millest tulenevalt saame turvakao valemi:

$$\frac{T'(n)}{\delta'(n)} = \frac{n^{\mathcal{O}(1)} \ell(n) m(n) T(n)}{\delta(n)} = \underbrace{n^{\mathcal{O}(1)} \ell(n) \delta(n)}_{n^{\mathcal{O}(1)}} \cdot \underbrace{\frac{m(n)}{T(n)}}_{\leq 1} \cdot \left(\frac{T(n)}{\delta(n)} \right)^2,$$

mis on polünoomiaalne.

Märkus.

Kui aga $z = g(x) = (z_0, z_1)$ ja $x \leftarrow \{0, 1\}^n$, siis H_k^z käitub funktsioonina nagu H_{k-1} . See tuleneb asjaolust, et ehkki χ kui funktsioon on defineeritud kogu hulgal $\{0, 1\}^{\leq \ell(n)}$, siis oraakli H_k^z väljunditena esinevad vaid χ väärtused hulgal $\{0, 1\}^{\ell(n)}$. Kui $(u||0, u||1)$ on k -s uus paar, siis vastavalt kirjeldusele H_k^z defineerib $\chi(u||0) = z_0 = g(x)_0$ ja $\chi(u||1) = z_1 = g(x)_1$. Oluline on tähele panna, et mitte ükski H_k^z väljund ei sõltu suurus-est $\chi(u)$, mille rolli on endale võtnud suurus x . Järgnevast tabelist

Oraaklis H_{k-1} :	Oraaklis H_k^z :
$\chi(u) \leftarrow \{0, 1\}^n$	$x \leftarrow \{0, 1\}^n$
$\chi(u 0) = g(\chi(u))_0$	$\chi(u 0) = z_0 = g(x)_0$
$\chi(u 1) = g(\chi(u))_1$	$\chi(u 1) = z_1 = g(x)_1$

on näha, et “kriitilises osas” on oraaklite H_{k-1} ja H_k^z arvutuskeemid ident-
sed, mistõttu need kaks oraaklit ka käituvad identselt.

Ülesanne võrdsetest paaridest

Näita, et kui d -elemendilisest hulgast D valitakse juhuslikult ja ühtlase jaotusega elemendid i_1, \dots, i_p , siis tõenäosus, et vähemalt kaks neist on võrdsed ei ole kunagi suurem kui $\frac{p^2}{2d}$.

Tõestuseks kasutame tavalist loendamist. On selge, et iga indeksite paari $k \neq \ell$ korral on $\Pr[i_k = i_\ell] = \frac{1}{d}$. Et kokku on täpselt $\frac{p(p-1)}{2}$ paari, siis järelikult ei ole tõenäosus, et kaks elementi on võrdsed, kunagi suurem kui

$$\frac{p(p-1)}{2d} \leq \frac{p^2}{2d}.$$

Plokkšifri konstruktsioon

Defineerime plokkšifri, kasutades ehituskivina pseudojuhuslike funktsioonide generaatorit $f: \{0, 1\}^n \times \{0, 1\}^{\ell(n)} \rightarrow \{0, 1\}^n$. Defineerime plokkšifri, mis n -bitise ploki m teisendab krüptogrammiks:

$$e = E_x(i, m) = m \oplus f_x(i). \quad (1)$$

Loomulikult, $D_x(i, e) = E_x(i, e)$, sest $f_x(i) \oplus f_x(i) = 0$.

Teoreem: Kui f on pseudojuhuslike funktsioonide generaator, siis valemiga (1) defineeritud plokkšiffer on turvaline. Reduktsioon on lineaarne.

Turvatõestus

Olgu (M, P, A) vastane edukusega $\delta = \delta(n)$, nii et

$$\frac{\delta}{2} = \Pr[A(R, \underbrace{m_1 \oplus f_X(i_1)}_{E_X(i_1, m_1)}, \dots, \underbrace{m_p \oplus f_X(i_p)}_{E_X(i_p, m_p)}; \underbrace{m^B \oplus f_X(i')}_{e' = E_X(i', m^B)}) = B] - \frac{1}{2},$$

kus sõnumid m_1, \dots, m_p genereeritakse algoritmi M abil ja $(i', m^0, m_1) = P(R, e)$. Kui asendada ründes kasutatud väärtuste jada

$$(f_x(i_1), \dots, f_x(i_p), f_x(i'))$$

sõltumatult, ühtlaselt ja juhuslikult genereeritud jadaga (Z_1, \dots, Z_p, Z') , siis on

$$\Pr_{Z, R, B} [A(R, m_1 \oplus Z_1, \dots, m_p \oplus Z_p, m^B \oplus Z') = B] - \frac{1}{2} = 0,$$

sest vastase A kõik sisendid on sõltumatud bitist B . Sama teeb aga välja kui asendada pseudojuhuslike funktsioonide generaator f tõeliselt juhusliku funktsiooniga $F \leftarrow \text{Map} \left(\{0, 1\}^{\ell(n)}, \{0, 1\}^n \right)$ ja arvutada

$$Z_1 = F(i_1), Z_2 = F(i_2), \dots, Z_{p(n)} = F(i_p), Z' = F(i') .$$

Seega saab koostada järgmise oraakliga vastase \mathcal{A}^Φ , mis sisendi n korral püüab arvata, kas oraakel $\Phi = F \leftarrow \text{Map} \left(\{0, 1\}^{\ell(n)}, \{0, 1\}^n \right)$ või on $\Phi = f_X$, kus $X \leftarrow \{0, 1\}^n$. Vastane $\mathcal{A}^\Phi(n)$ töötab järgmiselt:

- Valib juhuslikult $r \leftarrow \{0, 1\}^{s(n)}$.
- Kasutades algoritmi M genereerib blokkide jada $m = (m_1, \dots, m_{p(n)})$ ja vastavate krüptogrammide jada

$$e = (m_1 \oplus \Phi(i_1), \dots, m_{p(n)} \oplus \Phi(i_p)) .$$

- Algoritm P , saades sisendiks paari (r, e) arvutab $\ell(n)$ -bitise indeksi $i' \in \{0, 1\}^{\ell(n)}$ ja kaks n -bitist sõnumit $m^0, m^1 \in \{0, 1\}^n$.

- Genereerib $b \leftarrow \{0, 1\}$.
- A abil, sisendiga (r, e, m^b) , arvutab biti $a = A(r, e, m^b) \in \{0, 1\}$.
- $A^\Phi(n)$ väljastab 1, kui $a = b$. Kui aga $a \neq b$, siis $A^\Phi(n)$ väljastab 0.

Vastase \mathcal{A}^Φ edukus on:

$$\Pr_X[\mathcal{A}^{f_X}(n) = 1] - \Pr_F[\mathcal{A}^F(n) = 1] = \left(\frac{1}{2} + \frac{\delta(n)}{2}\right) - \frac{1}{2} = \frac{\delta(n)}{2},$$

millest järeldub, et \mathcal{A}^Φ eristab pseudojuhuslikku funktsiooni tõeliselt juhuslikust funktsioonist edukusega vähemalt $\delta(n)/2$, millest järeldub, et reduktsioon on lineaarne.

Permutatsioonigeneraatorid

Inspireeritud praktiliste blokkšifrite (nagu näiteks DES) konstruktsioonidest.

Permutatsioonigeneraatoriks nimetatakse paari (g, \bar{g}) , kus

$$\begin{aligned} g &: \{0, 1\}^n \times \{0, 1\}^{\ell(n)} \rightarrow \{0, 1\}^{\ell(n)} \\ \bar{g} &: \{0, 1\}^n \times \{0, 1\}^{\ell(n)} \rightarrow \{0, 1\}^{\ell(n)}, \end{aligned}$$

kusjuures $g_k(x) = g(k, x)$ hulga $\{0, 1\}^{\ell(n)}$ permutatsioonid ja

$$\bar{g}_k(g_k(x)) = g_k(\bar{g}_k(x)) = x,$$

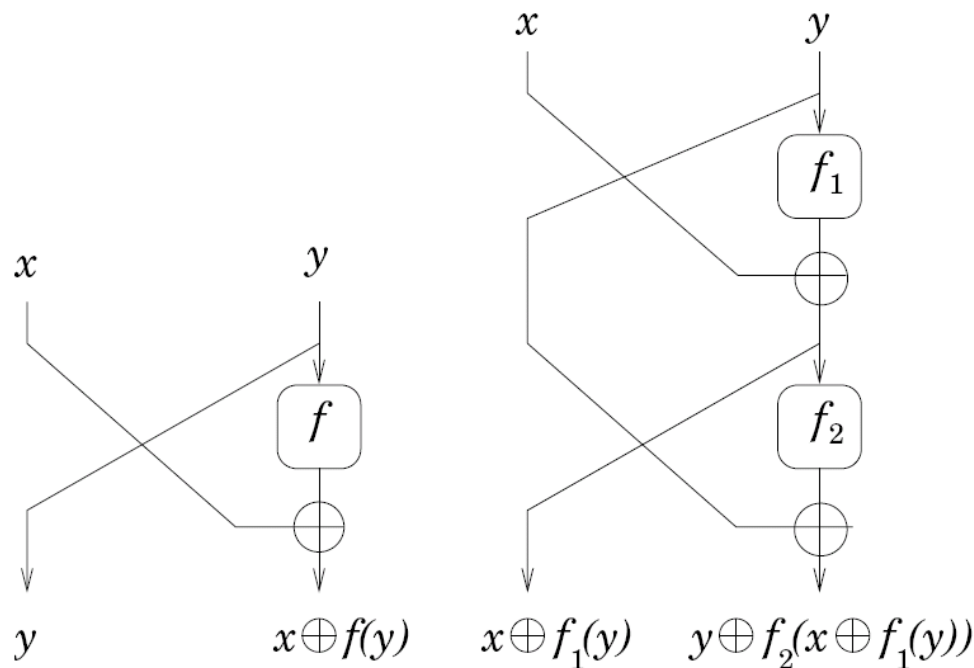
iga $x \in \{0, 1\}^{\ell(n)}$ korral. Praktilistes šifrites kasutatakse **itereerimist**, mistõttu on vaja, et $E_k(x)$ määramispiirkond langeks kokku tema väärtuste hulgaga.

Def.: Paari (g, \bar{g}) nimetatakse $S(n)$ -turvaliseks **pööratavaks pseudojuhuslike permutatsioonide generaatoriks**, kui funktsioon $g_k(x)$ on $S(n)$ -turvaline pseudojuhuslike funktsioonide generaator.

Feistel konstruktsioon

Võimaldab permutatsioonigeneraatorit konstrueerida pseudojuhuslikest funktsioonidest $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$. Olgu iga $(x, y) \in \{0, 1\}^{2n}$ korral:

$$\mathcal{F}^f(x, y) = (y, x \oplus f(y)) \quad \text{ja} \quad \overline{\mathcal{F}}^f(x, y) = (y \oplus f(x), x) .$$



Feisteli konstruktsiooni itereerimine

\mathcal{F}^f ja $\overline{\mathcal{F}}^f$ on teineteise pöördfunktsioonid, st iga $x, y \in \{0, 1\}^n$ korral:

$$\overline{\mathcal{F}}^f(\mathcal{F}^f(x, y)) = \mathcal{F}^f(\overline{\mathcal{F}}^f(x, y)) = (x, y) .$$

Itereeritud Feisteli konstruktsioon: Olgu $f_1, \dots, f_d: \{0, 1\}^n \rightarrow \{0, 1\}^n$.

Siis

$$\begin{aligned} \mathcal{F}^{f_1, \dots, f_d}(x, y) &= \mathcal{F}^{f_d}(\mathcal{F}^{f_1, \dots, f_{d-1}}(x, y)) \\ \overline{\mathcal{F}}^{f_1, \dots, f_d}(x, y) &= \overline{\mathcal{F}}^{f_1}(\mathcal{F}^{f_2, \dots, f_d}(x, y)). \end{aligned}$$

Näiteks kahekordne Feisteli konstruktsioon (Joon. vasakul) avaldub:

$$\mathcal{F}^{f_1, f_2}(x, y) = (x \oplus f_1(y), y \oplus f_2(x \oplus f_1(y))) .$$

Eesmärk: konstrueerida pööratav pseudojuhuslike permutatsioonide generaator g_k , kasutades pseudojuhuslike funktsioonide generaatorit f_k , nii et

$$g_k(x, y) = g_k^{(d)}(x, y) = \mathcal{F}^{f_{k_1}, \dots, f_{k_d}}(x, y),$$

kus $(k_1, \dots, k_d) = k \leftarrow (\{0, 1\}^n)^d$.

$g_k^{(1)}$ **ei ole pseudojuhuslik.** Piisab, kui mainida, et seosest $(x', y') = g_K^{(1)}(x, y) = \mathcal{F}^{f_K}(x, y) = (y, x \oplus f_K(y))$ järeldeb $x' = y$, või teisiti väljendudes, $\Pr_K[x' = y] = 1$. Samas, kui $F \leftarrow \text{Map}(\{0, 1\}^{2n}, \{0, 1\}^{2n})$ ja $(x', y') = F(x, y)$, siis seose $x' = y$ kehtimise tõenäosus

$$\Pr_F[x' = y] = 2^{-n}.$$

Siit järeldeb, et $g_K^{(1)}$ on lihtsasti eristatav päris-juhuslikust funktsioonist F .

$g_k^{(2)}$ ei ole pseudojuhuslik. Piisab, kui mainida, et seostest

$$(x'_1, y') = g_K^{(2)}(x_1, y) = (x_1 \oplus f_{k_1}(y), y \oplus f_{k_2}(x_1 \oplus f_{k_1}(y)))$$

$$(x'_2, y'') = g_K^{(2)}(x_2, y) = (x_2 \oplus f_{k_1}(y), y \oplus f_{k_2}(x_2 \oplus f_{k_1}(y)))$$

tuleneb seos $x'_1 \oplus x'_2 = x_1 \oplus x_2$. Kui aga $(x'_1, y) = F(x_1, y)$ ja $(x'_2, y) = F(x_2, y)$, kus $F \leftarrow \text{Map}(\{0, 1\}^{2n}, \{0, 1\}^{2n})$, siis

$$\Pr_F[x'_1 \oplus x'_2 = x_1 \oplus x_2] = 2^{-n} .$$

Siit järeldub, et ka $g_k^{(2)}$ on lihtsasti eristuv juhuslikust funktsioonist F .

Kolmekordse Feisteli struktuuri turvalisus

Eelnevate lihtsate näidete taustal, kus lihtsalt murti $g_k^{(1)}$ ja $g_k^{(2)}$, võib tunda üllatav, et $g_k^{(3)}$ osutub juba piisavalt eristamatuks tõeliselt juhuslikust funktsioonist.

Teoreem: Kui A on oraakliga vastane, mis väljastab ühe biti ja mis teeb ülimalt m oraakli väljakutset (oraaklid on tüüpi $\{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$), siis

$$\left| \Pr_{F_1, F_2, F_3} [A^{\mathcal{F}^{F_1, F_2, F_3}} = 1] - \Pr_{F_0} [A^{F_0} = 1] \right| \leq \frac{m^2}{2^n},$$

kus $F_1, F_2, F_3 \leftarrow \text{Map}(\{0, 1\}^n, \{0, 1\}^n)$ ja $F_0 \leftarrow \text{Map}(\{0, 1\}^{2n}, \{0, 1\}^{2n})$.

(Tõestust siin ei esitata)

Indeksivabad plokkšifrid

Seni konstrueeritud plokkšifrites oli iga krüpteeritud plokk varustatud uni-kaalse indeksiga. Kui aga ploki pikkus on piisavalt suur ja tõenäosus, et sama ploki krüpteeritakse mitu korda sama võtmega, on piisavalt väike, siis võib võtta krüptogrammi sõltuvaks ainult võtmest ja sõnumist endast. Sellises *indeksivabas* krüptosüsteemis on järgmised komponendid:

- *Võti* $x \in \{0, 1\}^n$.
- *Šifreerimisalgoritm* $E: \{0, 1\}^n \times \{0, 1\}^{q(n)} \rightarrow \{0, 1\}^{k(n)}$, mis avatekstist $m \in \{0, 1\}^{q(n)}$ ja võtmest x teeb $k(n)$ -bitise krüptogrammi $e = E(x, m) = E_x(m)$.
- *Dešifreerimisalgoritm* $D: \{0, 1\}^n \times \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{q(n)}$, mis $k(n)$ -bitisest krüptogrammist $e \in \{0, 1\}^{k(n)}$ ja võtmest x taastab $q(n)$ -bitise avateksti $m = D(x, e) = D_x(e)$.

Eeldatakse, et iga $x \in \{0, 1\}^n$ ja iga $m \in \{0, 1\}^{q(n)}$ korral kehtib seos

$$D_x(E_x(m)) = m .$$

Vastane (M, P, A) ja turvalisus

$$M: \{0, 1\}^{\log(p(n))} \times \{0, 1\}^{s(n)} \times (\{0, 1\}^{k(n)})^{\leq p(n)} \rightarrow \{0, 1\}^{q(n)}$$

$$P: \{0, 1\}^{s(n)} \times (\{0, 1\}^{k(n)})^{p(n)} \rightarrow (\{0, 1\}^{q(n)})^2$$

$$A: \{0, 1\}^{s(n)} \times (\{0, 1\}^{k(n)})^{p(n)} \times \{0, 1\}^{k(n)} \rightarrow \{0, 1\}$$

- Valitakse võti $x \leftarrow \{0, 1\}^n$ ja juhuarv $r \leftarrow \{0, 1\}^{s(n)}$.
- Algoritmi M abil genereeritakse plokid $m = (m_1, \dots, m_{p(n)})$ ja vastavate krüptogrammide $e = (E_x(m_1), \dots, E_x(m_{p(n)}))$, iteratiivselt:

$$m_j = M(j, r; E_x(m_1), E_x(m_2), \dots, E_x(m_{j-1})) .$$

- $P(r, e)$ väljastab $q(n)$ -bitised $m^0, m^1 \notin \{m_1, \dots, m_{p(n)}\}$.
- Valitakse juhuslikult $b \leftarrow \{0, 1\}$ ja arvutatakse krüptogramm $e' = E_x(m^b)$.
- Algoritm A , saades sisendiks kolmiku (r, e, e') , püüab ära arvata bitti b .

Ründe edukus on:

$$\delta(n) = 2 \cdot \left| \Pr[A(r, e, e') = b] - \frac{1}{2} \right| .$$

Indeksivaba plokkšifri konstruktsioon.

Olgu (g, \bar{g}) pööratav pseudojuhuslike permutatsioonide generaator, kus funktsioonid g ja \bar{g} on mõlemad tüüpi $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$. Olgu $x \leftarrow \{0, 1\}^n$ salajane võti. Defineerime krüpteerimis- ja dekrüpteerimis-funktsioonid järgmiselt:

$$e = E_x(m) = g_x(m), \quad m = D_x(e) = \bar{g}_x(e). \quad (2)$$

Teoreem: Kui (g, \bar{g}) on pööratav pseudojuhuslike permutatsioonide generaator, siis seostega (2) defineeritud indeksivaba blokkšifri on turvaline valitud avatekstiga ründe suhtes. Reduktsioon on lineaarne.

Turvatõestus

Olgu (M, P, A) vastane, mis teostab blokkšifrile (2) valitud avatekstiga rünnet edukusega $\delta(x)$, kusjuures eeldame üldisust kitsendamata, et

$$\Pr[A(r, e, e') = b] = \frac{1}{2} + \frac{\delta(n)}{2} . \quad (3)$$

Konstrueerime vastase S , mis emuleerib (komponent-) vastaseid M , P ja A , ja millele antakse oraaklina ette funktsioon $f' : \{0, 1\}^n \rightarrow \{0, 1\}^n$, nii et $S^{f'; M, P, A}$ eristab funktsioone

$$g_X \text{ kus } X \leftarrow \{0, 1\}^n ,$$

ja

$$F \leftarrow \text{Map} (\{0, 1\}^n, \{0, 1\}^n)$$

edukusega $\delta(n)/2$.

Vastane $S^{f';M,P,A}$ töötab järgmiselt:

- Genereerib juhuarvu $r \leftarrow \{0, 1\}^{s(n)}$.
- Emuleerides algoritmi M ja kasutades f' oraaklina, genereerib plokid $m = (m_1, \dots, m_p)$ ja vastavad krüptogrammid $e = (f'(m_1), \dots, f'(m_p))$:

$$m_j = M(j, r; f'(m_1), f'(m_2), \dots, f'(m_p)) .$$

- Emuleerides algoritmi P , genereeritakse avatekstid $(m^0, m^1) \leftarrow P(r, e)$.
- Valitakse juhuslikult $b \leftarrow \{0, 1\}$ ja arvutatakse “krüptogramm” $e' = f'(m^b)$.
- Emuleeritakse algoritmi A ja arvutatakse $a \leftarrow A(r, e, e')$
- Kui $a = b$, siis väljastatakse 1, vastasel juhul 0.

Et $m^b \notin \{m_1, \dots, m_{p(n)}\}$, siis $f' = F \leftarrow \text{Map}(\{0, 1\}^n, \{0, 1\}^n)$ korral ei sõltu algoritmi A ükski sisenditest r, e, e' suurusest B , millest järeljub, et

$$\Pr_{R,B,F} [S^{F;M,P,A} = 1] = \frac{1}{2} .$$

Kui aga sisendiks on funktsioon $g_X()$ (kus $X \leftarrow \{0, 1\}^n$), siis vastavalt eeldusele (3) saame, et

$$\Pr_{R,B,X} [S^{g_X;M,P,A}] = \frac{1}{2} + \frac{\delta(n)}{2} ,$$

millest tulenebki, et vastane $S^{f';M,P,A}$ eristab funktsioone g_X ja F edukusega $\delta(n)/2$. Et ka tööaeg ei erine oluliselt vastase (M, P, A) tööajast, siis on reduktsioon tõepoolest lineaarne.