

# Jadašifrid

Ahto Buldas

## Jadašifrid

Üritame edastada salastatud teateid pikkusega  $p(n)$  bitti, juhul kui võtme pikkus on  $n < p(n)$  bitti.

Selleks krüpteerime bitikaupa, kusjuures krüptogrammi  $i$ -s bitt on funktsioon ( $E$ ) võtmest  $x$ , indeksist  $i$  ja  $i$ -nda biti väärtusest (0/1). Eeldame, et igale bitile vastav krüptogramm on  $k(n)$ -bitine. Seega,

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

kus  $\ell(n) = \lceil \log_2 p(n) \rceil$  on indeksi  $i$  kodeerimiseks vajalike bittide arv. Krüptogrammist saab avateksti biti tagasi dekrüpteerimisalgoritmiga:

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

Et iga korrektne (st  $E$  abil saadud) krüptogramm oleks dešifreeritav, nõuame, et iga  $x \in \{0, 1\}^n$ , iga  $i \in \{0, 1\}^{\ell(n)}$  ja iga  $b \in \{0, 1\}$  korral

$$D(x, i, E(x, i, b)) = b.$$

Tähistuste kompaktsust silmas pidades kasutame edaspidi kirjapilti

$$E_x(i, m_i) = E(x, i, m_i) \quad \text{ja} \quad D_x(i, m_i) = D(x, i, m_i).$$

## Turvalisuse Definiitsioonid

Turvalise jadašifri defineerimiseks on mitmeid viise, mis põhinevad erinevatel ründestsenaariumidel. Ründed võivad olla aktiivsed ja passiivsed, sõltuvalt ründajale antud võimalustest. Järgnevalt käsitlemegi nelja erinevat ründestsenaariumi:

- Lihtne passiivne rünne,
- Üldine passiivne rünne,
- Lihtne valitud avatekstiga rünne, ja
- Üldine valitud avatekstiga rünne.

## Lihtne passiivne rünne

Ründe idee seisneb järgmises stsenaariumis. Genereeritakse juhuslikult ja ühtlaselt bitt  $b \in \{0, 1\}$ , arvutatakse avatekstele  $\overbrace{bb \dots b}^{p(n)}$  vastav krüptogramm, mille järgi ründaja püüab arvata ära biti  $b$ . Seega:

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

Rünne ise koosneb järgmistest sammudest:

- Valitakse  $x \leftarrow \{0, 1\}^n$
- Valitakse  $b \leftarrow \{0, 1\}$ . Olgu  $m^0 = 0^{p(n)}$ ,  $m^1 = 1^{p(n)}$ ,  $m = m^b = m_1 m_2 \dots m_{p(n)} \in \{0, 1\}^{p(n)}$ , ja

$$e = (E_x(1, m_1), \dots, E_x(p(n), m_{p(n)})) .$$

- Vastase  $A$  edukus defineeritakse järgmiselt:

$$\begin{aligned}\delta(n) &= |\Pr[A(e) = b] - \Pr[A(e) \neq b]| \\ &= 2 \cdot |\Pr[A(e) = b] - 1/2|\end{aligned}$$

Jadašiffer on  $S(n)$ -turvaline lihtsa passiivse ründe vastu, kui iga vastase aeg-edukus suhe on vähemalt  $S(n)$ .

## Näide turvalisest jadašifrist

Olgu  $g: \{0, 1\}^n \rightarrow \{0, 1\}^{p(n)}$  pseudojuhuarvude generaator, kus  $p(n)$  olgu maksimaalne bittide arv, mida on vaja krüpteerida. Olgu  $x \in \{0, 1\}^n$  võti, millest generaatori  $g$  abil arvutatakse võtmebittide bitijada  $g(x)$ . Sõnumi  $m = m_1 m_2 \dots m_{p(n)} \in \{0, 1\}^{p(n)}$  krüptogramm  $e = (e_1, \dots, e_i, \dots, e_{p(n)})$  arvutatakse järgmiselt:

$$e_i = E_x(i, m_i) = g(x)_i \oplus m_i. \quad (1)$$

**Teoreem:** Kui  $g$  on pseudojuhuarvude generaator, siis valemiga (1) defineeritud jadašiffer on turvaline lihtsa passiivse ründe vastu. Reduktsioon on lineaarne.

## Tõestus

Olgu  $X \leftarrow \{0, 1\}^n$  ja  $B \leftarrow \{0, 1\}$ . Olgu  $B^{p(n)} = \overbrace{BB \dots B}^{p(n)}$ . Olgu  $A$  vastane, mis murrab ülalkirjeldatud jadašifrit edukusega

$$\delta(n) = 2 \cdot \left| \Pr_{X,B} [A(g(X) \oplus B^{p(n)}) = B] - 1/2 \right|.$$

Konstrueerime oraakliga vastase  $S^A$ , mis murrab generaatorit  $g$  edukusega  $\delta(n)/2$ . Eeldame üldisust kitsendamata, et

$$\delta(n)/2 = \Pr_{X,B} [A(g(X) \oplus B^{p(n)}) = B] - 1/2. \quad (2)$$

Paneme tähele, et kui  $Z \leftarrow \{0, 1\}^{p(n)}$ , siis  $\Pr[A(Z \oplus B^{p(n)}) = B] - 1/2 = 0$ , sest  $Z \oplus B^{p(n)}$  on sõltumatu suurusest  $B$ , mis ise on ühtlase jaotusega.

Järelikult, kui defineerida (generaatori väljundit juhuslikust jadast eristav) vastane  $S^A: \{0, 1\}^{p(n)} \rightarrow \{0, 1\}$ , mis sisendi  $y \in \{0, 1\}^{p(n)}$  korral toimib

järgmiselt:

- $S^A$  genereerib juhusliku biti  $B \leftarrow \{0, 1\}$ .
- Kui  $A(y \oplus B^{p(n)}) = B$ , siis  $S^A$  väljastab 1, vastasel juhul 0.

Kui  $y = Z$ , siis  $\Pr[S^A(z) = 1] = 1/2$ . Kui aga  $y = g(X)$ , siis on vastavalt eeldusele (2) teada, et  $\Pr[S^A(y) = 1] = 1/2 + \delta(n)/2$ . Seega suudab vastane  $S^A$  eristada  $g$  väljundjada juhuslikust jadast edukusega  $\delta(n)/2$ , mis tähendabki, et reduktsioon on tõepoolest lineaarne.

## Üldine passiivne rünne

Lihtsa passiivse ründe kirjeldus on võrdlemisi kunstlik. Tegelikult me soovime, et ründaja ei saaks krüptogrammi järgi teada mitte mingisugust informatsiooni vastava avateksti kohta, isegi mitte ainsat bitti.

Ründajal peab olema krüptogrammi põhjal raske kindlaks teha ükskõik millist avateksti  $m$  omadust  $b(m)$ . Võib väljenduda ka nii, et ründaja ise valib sobiliku omaduse  $b$ , mida ta soovib krüptogrammi järgi tuvastama hakata.

Samuti eeldame, et omaduse  $b(m)$  tuvastamine peab olema raske avateksti  $m = m_1 m_2 \dots m_{p(n)} \in \{0, 1\}^{p(n)}$  suvalise (polünomiaalselt genereeritava) tõenäosusjaotuse korral.

## Formaalne Ründestsenaarium

Ülaloodud mõttekäiku silmas pidades tuleb eeldada, et vastane koosneb kolmest P-perest  $(P, A, b)$ , kus:

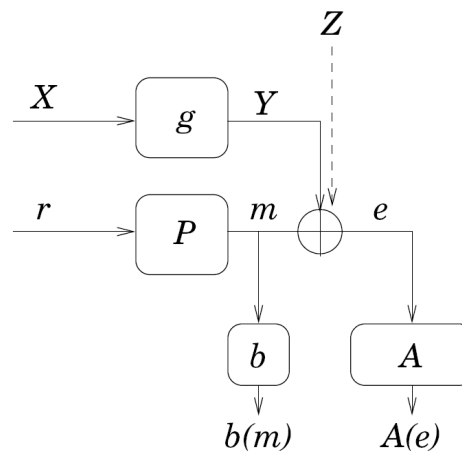
- $P: \{0, 1\}^{s(n)} \rightarrow \{0, 1\}^{p(n)}$  on P-pere, mille abil genereeritakse juhuslikult sõnum  $m = P(r)$ , kus  $r \leftarrow \{0, 1\}^{s(n)}$ .
- $b: \{0, 1\}^{p(n)} \rightarrow \{0, 1\}$  on bitt, mille väärtust (kohal  $m$ ) vastane ( $A$ ) püüab tuvastada.
- $A: (\{0, 1\}^{k(n)})^{p(n)} \rightarrow \{0, 1\}$  on vastane, mis püüab bitti arvutada, olles sisendiks saanud krüptogrammi  $e = (E_x(1, m_1), \dots, E_x(p(n), m_{p(n)}))$ .

Rünne ise toimub järgmiste etappide kaupa:

- Valitakse juhuslikult võti  $x \leftarrow \{0, 1\}^n$ .
- Valitakse juhuslikult  $r \leftarrow \{0, 1\}^{s(n)}$ .
- Arvutatakse  $m = P(r) = m_1 m_2 \dots m_{p(n)} \in \{0, 1\}^{p(n)}$ .

- Arvutatakse krüptogramm  $e = (E_x(1, m_1), \dots, E_x(p(n), m_{p(n)}))$ .
- Vastane  $A$ , saades sisendiks  $e$ , leiab  $A(e) \in \{0, 1\}$ .

Vastase  $(P, A, b)$  tööajaks loetakse kõigi kolme komponent-vastase tööaegade summat.



Intuitiivselt, mida paremini  $A(e)$  langeb kokku bitiga  $b(m)$ , seda edukamaks loetakse vastast  $(P, A, b)$ . Milline oleks aga matemaatiliselt kor-

rektne edukuse definitsioon? Selgub, et sobilikku viisi edukuse defineerimiseks ei ole sugugi nii lihtne leida. Alustame selgitusest, miks ei saa analoogiliselt eelnevaga defineerida edukusena suurust

$$\delta(n) = |\Pr[A(e) = b(m)] - \Pr[A(e) \neq b(m)]|$$

Asi on selles, et tänu algoritmide  $P$ ,  $A$  ja  $b$  “koostööle” võib saavutada suuruste  $A(e)$  ja  $b(m)$  kui tahes hea vastavuse. Ekstreemse näite saame, kui võtame funktsioonideks  $A$  ja  $b$  konstantsed funktsioonid. Sellisel juhul on alati  $\delta(n) = 1$ . Seega ei oleks nii defineeritud edukusega turvatingimus üldse saavutatav. Intuitiivselt me tahame, et vastane näitaks võimet ennustada neid bitte, mis sisaldavad kasvõi mingitki määramatust. Enne kui läheme turvatingimuse korrektse püstituse juurde, tutvume ühe tõenäosusteooria põhimõistega – *kovariatsiooniga*.

## Kovariatsioon ja selle omadused

Olgu  $X$  ja  $Y$  juhuslikud suurused. Suuruste  $X$  ja  $Y$  kovariatsiooniks  $\text{cov}(X, Y)$  nimetatakse suurust

$$\text{cov}(X, Y) = \mathbf{E}[X \cdot Y] - \mathbf{E}[X] \cdot \mathbf{E}[Y].$$

Intuitiivselt väljendab kovariatsioon seda, kui hästi suurus  $Y$  aitab ennustada suurust  $X$ . Juhul kui  $X$  ja  $Y$  on 0/1-suurused, siis on kovariatsioonil järgmised omadused:

- $\text{cov}(X, Y) = \Pr[X = 1, Y = 1] - \Pr[X = 1] \cdot \Pr[Y = 1]$ .
- $\text{cov}(X, Y) = 0$  parajasti siis kui suurused  $X$  ja  $Y$  on sõltumatud.
- Kui  $Y \leftarrow \{0, 1\}$  ja  $X = Y$ , siis on kovariatsioon  $\text{cov}(X, Y)$  maksimaalne, s.t. võrdne  $1/4$ .
- Üldisemalt, kui  $p = \Pr[X = 1]$ , siis maksimaalne kovariatsioon on  $p(1 - p)$ , mis saavutatakse parajasti siis kui  $X = Y$ .

Viimase lause põhjendamiseks võtame  $q_{11} = \Pr[Y = 1 \mid X = 1]$  ja  $q_{10} = \Pr[Y = 1 \mid X = 0]$ . Kolm suurust  $p$ ,  $q_{10}$  ja  $q_{0,1}$  määravad seose

$$\Pr[Y = 1] = pq_{11} + (1 - p)q_{10}$$

tõttu täielikult ära ka suuruse  $Y$  tõenäosusjaotuse. Samas võib suurusi  $q_{11}$  ja  $q_{10}$  valida suvaliselt. Avaldades kovariatsiooni  $\text{cov}(X, Y)$  nimetatud suuruste kaudu, saame

$$\text{cov}(X, Y) = pq_{11} - p \cdot (pq_{11} + (1 - p)q_{10}) = q_{11} \underbrace{(p - p^2)}_{\geq 0} + q_{10} \underbrace{(p^2 - p)}_{\leq 0},$$

millest on selge, et  $\text{cov}(X, Y)$  saavutab maksimumi parajasti siis kui  $q_{11} = 1$  ja  $q_{10} = 0$ . Suuruste  $X, Y$  väärtuste hulkade lõpikkusest järeldubki nüüd, et  $X = Y$ .

## Tingimuslik kovariatsioon.

Suuruste  $X$  ja  $Y$  tingimuslikuks kovariatsiooniks suuruse  $Z$  suhtes nimetatakse avaldist:

$$\text{cov}(X, Y | Z) = \mathbf{E}_Z[\mathbf{E}[X \cdot Y | Z] - \mathbf{E}[X | Z] \cdot \mathbf{E}[Y | Z]].$$

Intuitiivselt tähendab tingimuslik kovariatsioon mõõtu kui hästi aitab muutuja  $Y$  väärtuse teadmine ette ennustada muutuja  $X$  väärtust eeldusel, et muutuja  $Z$  väärtus on teada. Kui  $X$  ja  $Y$  on 0/1-suurused ja  $Z$  on suurus väärtuste piirkonnaga  $D$ , siis

$$\begin{aligned} \text{cov}(X, Y | Z) &= \sum_{z \in D} \Pr[Z = z] \cdot [\Pr[X = 1, Y = 1 | Z = z] - \\ &\quad - \Pr[X = 1 | Z = z] \cdot \Pr[Y = 1 | Z = z]]. \end{aligned}$$

Näiteks kui  $Z \leftarrow \{0, 1\}^n$  ja  $X, Y$  võrduvad mõlemad suuruse  $Z$  esimese bitiga  $Z_1 \in \{0, 1\}$ , siis  $\text{cov}(X, Y) = 1/4$ , kuid samas  $\text{cov}(X, Y | Z) = 0$ .

Viimase asjaolu intuiitivne põhjendus on see, et kuna  $X$  ja  $Y$  on mõlemad suuruse  $Z$  funktsioonid, siis peale  $Z$  väärtuse teadasaamist on teada ka  $X$  ja  $Y$  väärtus, mistõttu ei ole alust öelda, et  $Y$  aitab ennustada  $X$  väärtust.

## Turvalisus üldise passiivse ründe vastu

Defineerime ründaja edukuse  $\delta(n)$  kui kovariatsiooni  $\text{cov}(A(e), b(m))$  ja tõestame, et valemiga (1) defineeritud jadasiffer on turvaline üldise passiivse ründe vastu.

**Teoreem:** Kui  $g$  on pseudojuhuarvude generaator, siis ülaloodud jadašiffer on turvaline üldise passiivse ründe vastu. Reduktsioon on lineaarne.

**Tõestus:** Olgu  $(P, A, b)$  vastane, mis teostab üldist passiivset rünnet edukusega  $\text{cov}(A(e), b(m)) = \delta(n)$ . Näitame, et siis leidub vastane  $A' = S^{P,A,b}$ , mis edukusega vähemalt  $\delta(n)/2$  eristab generaatori  $g$  väljundit ühtlasest jaotusest.

Olgu  $Y = g(X)$ ,  $Z \leftarrow \{0, 1\}^{p(n)}$ ,  $e_Y = e = m \oplus Y$  ja  $e_Z = m \oplus Z$ . Paneme kõigepealt tähele, et kui üldises passiivses ründes võtta  $g(x)$

asemele ühtlane jaotus  $Z$ , siis on suurused  $A(e_Z)$  ja  $b(m)$  sõltumatud, mistõttu

$$\text{cov}(A(e_Z), b(m)) = 0.$$

Olgu  $p = \Pr[e(m) = 1]$ . Saame kaks võrdust.

$$\begin{aligned} \text{cov}(A(e_Y), b(m)) &= \Pr[A(e_Y) = b(m) = 1] - p \cdot \Pr[A(e_Y) = 1] = \delta(n), \\ \text{cov}(A(e_Z), b(m)) &= \Pr[A(e_Z) = b(m) = 1] - p \cdot \Pr[A(e_Z) = 1] = 0, \end{aligned}$$

millest alumise lahutamisel ülemisest saame, et

$$\begin{aligned} &\Pr[A(e_Y) = b(m) = 1] - \Pr[A(e_Z) = b(m) = 1] && (3) \\ &+ p \cdot [\Pr[A(e_Z) = 1] - \Pr[A(e_Y) = 1]] = \delta(n). \end{aligned}$$

Järgnevalt kirjeldame kahte vastast  $S_1^{P,A,b}$  ja  $S_2^{P,A,b}$ , millest vähemalt üks peab eristama jaotusi  $Z$  ja  $Y$  edukusega vähemalt  $\delta(n)/2$ .

Esimese vastase  $S_1^{P,A,b}$  töö (sisendi  $T \in \{0, 1\}^{p(n)}$  korral) on esitatav järgmiste sammudena:

- $S_1^{P,A,b}$  genereerib  $r \leftarrow \{0, 1\}^{s(n)}$ , arvutab  $m = P(r) \in \{0, 1\}^{p(n)}$  ja  $b(m)$ . Seejärel arvutab  $S_1^{P,A,b}$  krüptogrammi  $e_T = m \oplus T$  ja biti  $A(e_T)$ .
- Kui  $A(e_T) = b(m) = 1$ , siis  $S_1^{P,A,b}(T)$  tagastab 1, vastasel korral aga 0.

Teine vastane  $S_2^{P,A,b}$  käitub (sisendi  $T$  korral) järgmiselt:

- $S_2^{P,A,b}$  genereerib  $r \leftarrow \{0, 1\}^{s(n)}$  ja arvutab  $m = P(r) \in \{0, 1\}^{p(n)}$ .
- $S_2^{P,A,b}$  arvutab krüptogrammi  $e_T = m \oplus T$  ja tagastab biti  $A(e_T)$ .

Arvutades mõlemate vastaste  $S_1, S_2$  edukused (vastavalt  $\delta_1(n), \delta_2(n)$ ),

saame:

$$\begin{aligned}\delta_1(n) &= |\Pr[S_1^{P,A,b}(Y) = 1] - \Pr[S_1^{P,A,b}(Z) = 1]| \\ &= |\Pr[A(e_Y) = b(m) = 1] - \Pr[A(e_Z) = b(m) = 1]|; \\ \delta_2(n) &= |\Pr[S_2^{P,A,b}(Y) = 1] - \Pr[S_2^{P,A,b}(Z) = 1]| \\ &= |\Pr[A(e_Y) = 1] - \Pr[A(e_Z) = 1]|.\end{aligned}$$

Seosest (3) saame, et vähemalt üks suurustest  $\delta_1(n)$ ,  $\delta_2(n)$  peab olema  $\geq \delta(n)/2$ , millest järeldubki, et vähemalt üks vastastest  $S_1^{P,A,b}$ ,  $S_2^{P,A,b}$  on piisavalt edukas jaotuste  $Z$  ja  $Y$  eristamisel.

## Lihtne valitud avatekstiga rünne

Valitud avatekstiga ründes eeldatakse, et vastasel on piiratud aja jook-sul võimalik uurida krüpteerimisalgoritmi  $E$ . Seejärel valib vastane kaks avateksti ja olles saanud nende avatekstide krüptogrammide (järjekord tead-mata), püüab ära arvata kumb on kumb.

Vastane koosneb kolmest algoritmist  $M$ ,  $P$  ja  $A$ . Eeldame, et kõik kolm algoritmi on esitatavad P-peredena:

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

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

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

## Ründestsenaarium: lihtne valitud avatekstiga rünne

- Genereeritakse salajane võti  $x \leftarrow \{0, 1\}^n$  ja juhuslik  $r \leftarrow \{0, 1\}^{s(n)}$ .
- Algoritmi  $M$  abil luuakse sõnum  $m = m_1, \dots, m_{p(n)} \in \{0, 1\}^{p(n)}$  ja vastav krüptogramm  $e = (E_x(1, m_1), \dots, E_x(p(n), m_{p(n)}))$ , kasutades algoritmi  $E_x$  iteratiivselt iga  $j \in \{1, \dots, p(n)\}$  korral:

$$m_j = M(j, r; E_x(1, m_1), \dots, E_x(j-1, m_{j-1})) \quad (4)$$

- Algoritm  $P$ , sisendiga  $(r, e)$ , leiab kaks  $t(n)$ -bitist sõnumit  $(m^0, m^1)$ .
- Valitakse  $b \leftarrow \{0, 1\}$ , võetakse  $m' = m^b$  ja arvutatakse krüptogramm:

$$e' = (E_x(p(n) + 1, m'_1), \dots, E_x(p(n) + t(n), m'_{t(n)})).$$

- Vastane  $A$ , saades sisendiks  $(r, e, e')$ , püüab ära arvata, milline sõnumitest  $m^0, m^1$  on krüptogrammi  $e'$  originaal. Ründe edukus on:

$$\delta(n) = 2 \cdot |\Pr[A(r, e, e') = b] - 1/2|.$$

## Turvalisus

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

Oluline on tähele panna, et ehkki bitid  $m_1, \dots, m_{j-1}$  ei esine algoritmi  $M$  argumentide hulgas (vt valem (4)), on need bitid kaudselt välja arvutatavad, sest juhuarv  $r$  on algoritmile  $M$  teada. Samal põhjusel on algoritmile  $A$  teada sõnumid  $m, m^0$  ja  $m^1$ .

**Teoreem:** Kui  $g: \{0, 1\}^n \rightarrow \{0, 1\}^{p(n)+t(n)}$  on pseudojuhuarvude generaatore, siis valemiga  $e = m \oplus g(x)$  defineeritud jadašiffer on turvaline lihtsa valitud avatekstiga ründe vastu. Reduktsioon on lineaarne.

## Turvatõestus

Olgu  $(M, P, A)$  edukusega  $\delta = \delta(n)$ , nii et (lüh.  $p = p(n), t = t(n)$ ):

$$\Pr[A(r, g(X)_{\{1\dots p\}} \oplus m, g(X)_{\{p+1\dots p+t\}} \oplus m^b) = b] - \frac{1}{2} = \frac{\delta}{2},$$

kus  $m$  genereeritakse  $M$  abil ja  $m^0, m^1$  genereeritakse algoritmi  $P$  abil. Kui  $g(X)$  asendada jaotusega  $Z \leftarrow \{0, 1\}^{p+t}$ , siis

$$\Pr[A(R, Z_{\{1\dots p\}} \oplus m, Z_{\{p+1\dots p+t\}} \oplus m^b) = b] - \frac{1}{2} = 0,$$

sest algoritmi  $A$  kõik sisendid (kaasaarvatud  $Z_{\{p+1\dots p+t\}} \oplus m^b$ ) on sõltumatud suurusest  $b$ , mis ise on ühtlase jaotusega. Sellest tähelepanekust tulenevalt saab koostada oraakliga vastase  $S^{M,P,A}$ , mis eristab generaatori väljundjaotust  $g(X)$  ühtlasest jaotusest  $Z$ . Vastane  $S^{M,P,A}$  töötab sisendi  $y \in \{0, 1\}^{p+t}$  korral järgmiselt:

- $S^{M,P,A}$  genereerib  $r \leftarrow \{0, 1\}^{s(n)}$  ja kasutades algoritmi  $M$  arvutab sõnumi  $m \in \{0, 1\}^p$  ja sellele vastava krüptogrammi

$$e = y_{\{1\dots p\}} \oplus m .$$

- $S^{M,P,A}$  kasutab algoritmi  $P$  ja arvutab sõnumid  $(m_0, m_1) \leftarrow P(r, e)$ .
- $S^{M,P,A}$  genereerib  $b \leftarrow \{0, 1\}$  ja arvutab krüptogrammi

$$e' = y_{\{p+1,\dots,p+t\}} \oplus m^b .$$

- Kui  $A(r, e, e') = b$ , siis  $S^{M,P,A}$  väljastab 1, vastasel juhul 0.

Lihtne on veenduda, et kui  $y = Z$ , siis  $\Pr[S^{M,P,A}(y) = 1] = 1/2$ . Kui aga  $y = g(X)$ , siis  $\Pr[S^{M,P,A}(y) = 1] = 1/2 + \delta(n)/2$ . Seega suudab  $S^{M,P,A}$  eristada jaotusi  $g(X)$  ja  $Z$  edukusega  $\delta(n)/2$  ja et ka  $S^{M,P,A}$  tööaeg langeb praktiliselt kokku vastase  $(M, P, A)$  tööajaga, siis sellest järeldubki, et reduktsioon on lineaarne.

## Üldine valitud avatekstiga rünne

Lihtne valitud avatekstiga rünne arvestas ainult kindla ründestsenaariumiga. Tegelikult me sooviksime, et ründaja ei suudaks krüptogrammi põhjal avatekstit teada saada mitte mingisugust informatsiooni. Analoogiliselt üleminekuga lihtsalt passiivselt ründelt üldisele passiivsele ründele, defineerime üldise valitud avatekstiga ründes vastase kui neliku  $(M, P, b, A)$ , kus:

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

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

$$b: \{0, 1\}^{t(n)} \rightarrow \{0, 1\}$$

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

## Ründestsenaarium

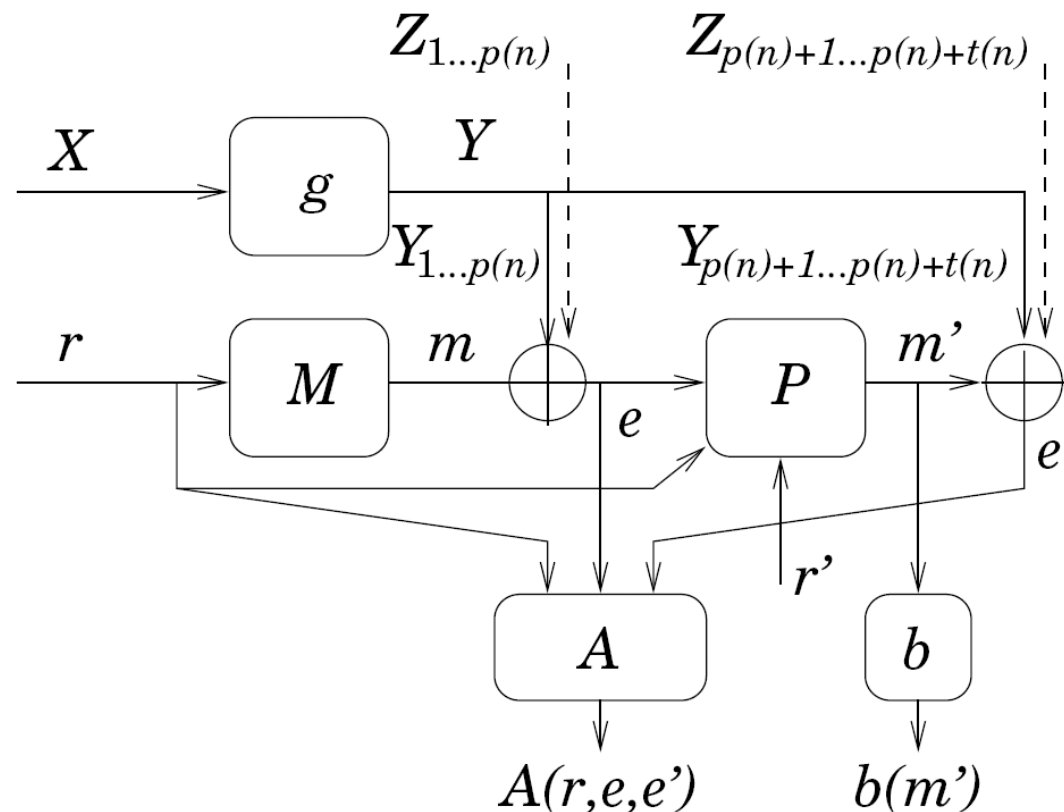
- Genereeritakse võti  $x \leftarrow \{0, 1\}^n$  ja juhuslik  $r \leftarrow \{0, 1\}^{s(n)}$ .
- Algoritmi  $M$  abil genereeritakse sõnum  $m = m_1, \dots, m_{p(n)} \in \{0, 1\}^{p(n)}$  ja vastav krüptogramm  $e = (E_x(1, m_1), \dots, E_x(p(n), m_{p(n)}))$ , kasutades algoritmi  $E_x$  musta kastina (oraaklina) ja valemit (4).
- Valitakse juhuslikult  $r' \leftarrow \{0, 1\}^{s(n)}$ .
- Algoritm  $P$ , sisendiga  $(r, r', e)$ , arvutab  $t(n)$ -bitise sõnumi  $m' = P(r, r', e)$ .
- Arvutatakse krüptogramm

$$e' = (E_x(p(n) + 1, m'_1), \dots, E_x(p(n) + t(n), m'_{t(n)})).$$

- Vastane  $A$ , saades sisendiks kolmiku  $(r, e, e')$ , püüab arvutada bitti  $b(m')$ . Vastase  $(M, P, b, A)$  edukuseks loetakse tingimuslikku kovariatsiooni:

$$\delta(n) = |\text{cov}(A(r, e, e'), b(m') \mid r, e)|.$$

**Teoreem:** Kui  $g: \{0, 1\}^n \rightarrow \{0, 1\}^{p(n)+t(n)}$  on pseudojuhuarvude generaator, siis valemiga  $e = m \oplus g(x)$  defineeritud jadašiffer on turvaline üldise valitud avatekstiga ründe vastu. Reduktsioon on lineaarne.



## Turvatõestus

Olgu  $(M, P, b, A)$  vastane, mis teostab üldist valitud avatekstiga rünnet edukusega  $\text{cov}(A(r, e, e'), b(m') \mid r, e) = \delta(n)$ . Näitame, et siis leidub vastane  $A' = S^{M, P, b, A}$ , mis edukusega vähemalt  $\delta(n)/2$  eristab generaatori  $g$  väljundit ühtlasest jaotusest. Olgu  $Y = g(X)$ ,  $Z \leftarrow \{0, 1\}^{p(n)+t(n)}$ , ja kasutame tähistusi:

$$\begin{array}{ll}
 e_Y = m \oplus Y_{\{1\dots p\}}, & e_Z = m \oplus Z_{\{1\dots p\}} \\
 m'_Y = P(r, r', e_Y), & m'_Z = P(r, r', e_Z) \\
 e'_Y = m'_Y \oplus Y_{\{p+1\dots p+t\}}, & e'_Z = m'_Z \oplus Z_{\{p+1, \dots, p+t\}} \\
 a_Y = A(r, e_Y, e'_Y), & a_Z = A(r, e_Z, e'_Z) \\
 p_Y(r, e) = \Pr_{R, Y}[R = r, e_Y = e] & p_Z(r, e) = \Pr_{R, Z}[R = r, e_Z = e].
 \end{array}$$

Kasutame edaspidi järgmisi lisaks järgmisi lühendatud tähistusi:

$$\begin{aligned}
 p(b \mid r, e) &= \Pr_{R' \leftarrow \{0,1\}^{s(n)}} [b(P(r, R', e)) = 1] \\
 p_Y(ab \mid r, e) &= \Pr[a_Y = b_Y = 1 \mid r, e] \\
 p_Z(ab \mid r, e) &= \Pr[a_Z = b_Z = 1 \mid r, e] \\
 p_Y(a \mid r, e) &= \Pr[a_Y = 1 \mid r, e] \\
 p_Z(a \mid r, e) &= \Pr[a_Z = 1 \mid r, e]
 \end{aligned}$$

Siis saab tingimusliku kovariatsiooni esitada kujul

$$\begin{aligned}
 c_Y &= \text{cov}(A(r, e_Y, e'_Y), b(m'_Y) \mid r, e) \\
 &= \sum_{r,e} p_Y(r, e) \cdot [p_Y(ab \mid r, e) - p(b \mid r, e) \cdot p_Y(a \mid r, e)] \\
 &= \delta(n).
 \end{aligned}$$

Kui võtta jaotuse  $g(X)$  asemele ühtlane jaotus  $Z$ , siis on suurused  $a_Z = A(r, e_Z, e'_Z)$  ja  $b(m'_Z)$  iga **fikseeritud  $r$  ja  $e$  korral** sõltumatud ja seetõttu

$$\begin{aligned} c_Z &= \text{cov}(A(r, e_Z, e'_Z), b(m'_Z) \mid r, e) \\ &= \sum_{r,e} p_Z(r, e) \cdot [p_Z(ab \mid r, e) - p_{r,e} \cdot p_Z(a \mid r, e)] = 0 . \end{aligned}$$

Arutledes analoogiliselt üldise passiivse ründe käsitlusega, saame võrdusest  $c_Y - c_Z = \delta(n)$ , et vähemalt üks suurustest

$$\begin{aligned} \delta_1(n) &= \sum_{r,e} p_Y(r, e) \cdot p_Y(ab \mid r, e) - \sum_{r,e} p_Z(r, e) \cdot p_Z(ab \mid r, e) \\ &= \Pr[a_Y = b_Y = 1] - \Pr[a_Z = b_Z = 1] \\ \delta_2(n) &= \sum_{r,e} p_Z(r, e) \cdot p(b \mid r, e) p_Z(a \mid r, e) - \\ &\quad \sum_{r,e} p_Y(r, e) \cdot p(b \mid r, e) p_Y(a \mid r, e) \end{aligned}$$

peab olema suuruselt vähemalt  $\delta(n)/2$ .

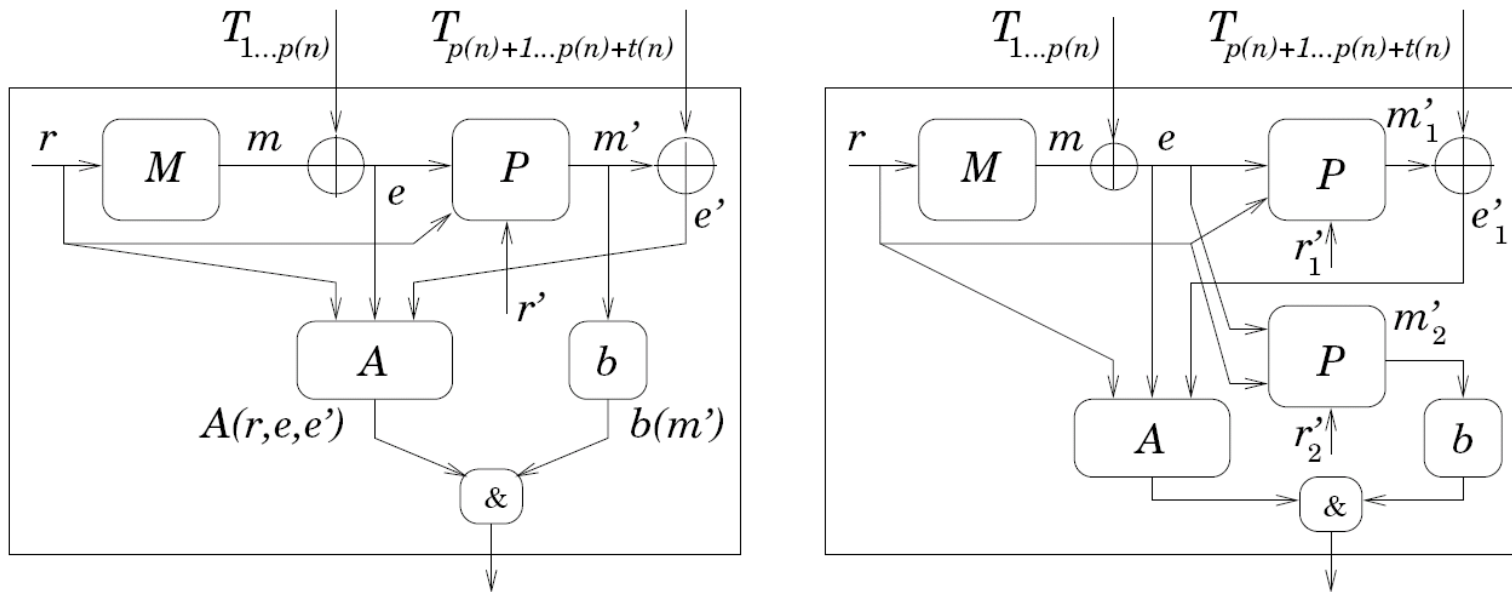
Nüüd defineerime kaks vastast  $S_1^{M,P,b,A}$  ja  $S_2^{M,P,b,A}$ , millest vähemalt üks peab eristama jaotusi  $Z$  ja  $Y$  edukusega vähemalt  $\delta(n)/2$ .

Vastane  $S_1^{M,P,b,A}$  käitub sisendi  $T \in \{0, 1\}^{p(n)+t(n)}$  korral järgmiselt:

- Genereerib  $r \leftarrow \{0, 1\}^{s(n)}$  ja  $r' \leftarrow \{0, 1\}^{s(n)}$ .
- Arvutab  $m \in \{0, 1\}^{p(n)}$ , kasutades  $M$  ja valemit (4).
- Arvutab krüptogrammi  $e = m \oplus T_{\{1, \dots, p(n)\}}$ .
- $P$  abil leiab  $m' = P(r, r', e)$  ja  $e' = m' \oplus T_{\{p(n), \dots, p(n)+t(n)\}}$ .
- $A$  abil leiab  $a = A(r, e, e')$  ja  $b$  abil  $b(m')$ .
- Kui  $a = b(m') = 1$ , siis  $S_1^{M,P,b,A}(T)$  väljastab 1, vastasel korral 0.

Vastane  $S_2^{M,P,b,A}$  käitub (sisendi  $T \in \{0, 1\}^{p(n)+t(n)}$  korral) järgmiselt:

- Genereerib  $r \leftarrow \{0, 1\}^{s(n)}$ .
- Arvutab  $m \in \{0, 1\}^{p(n)}$ , kasutades  $M$  ja valemit (4)
- Arvutab krüptogrammi  $e = m \oplus T_{\{1, \dots, p(n)\}}$ .
- Genereerib  $r'_1 \leftarrow \{0, 1\}^{s(n)}$ .
- $P$  abil leiab  $m'_1 = P(r, r'_1, e)$  ja  $e'_1 = m'_1 \oplus T_{\{p(n), \dots, p(n)+t(n)\}}$ .
- $A$  abil leitab  $a_1 = A(r, e, e'_1)$ .
- Genereerib  $r'_2 \leftarrow \{0, 1\}^{s(n)}$ .
- $P$  abil leiab  $m'_2 = P(r, r'_2, e)$  ja  $e'_2 = m'_2 \oplus T_{\{p(n), \dots, p(n)+t(n)\}}$ .
- $b$  abil leiab  $b_2 = b(m'_2)$ .
- Kui  $a_1 = b_2 = 1$ , siis  $S_2^{M,P,b,A}(T)$  väljastab 1, vastasel korral aga 0.



Vastased  $S_1^{M,P,b,A}$  (vasakul) ja  $S_2^{M,P,b,A}$  (paremal).

On lihtne veenduda, et vastase edukused on vastavalt  $\delta_1(n)$  ja  $\delta_2(n)$ , millest järeldub, et vähemalt üks neist vastastest on suuteline eristama jaotusi  $Y = g(X)$  ja  $Z$  edukusega vähemalt  $\delta(n)/2$ .