T-79.4001
Privacy amplification

Ari Nevalainen

ajnevala@cc.hut.fi

ALKUTILANNE

- Alkutilanne.
- Kaksi erikoistapausta.
- Yleinen tapaus.
- Yhteenveto.

ALKUTILANNE

- Alice ja Bob jakavat merkkijonon.

$$\vec{a} = \{a_1, a_2, \ldots, a_n\}$$

- Merkkijonosta on korjattu virheet käyttämällä korjausmatriisia H.
- Alice ja Bob tietävät virheiden esiintymistaajuuden.
- Eve tuntee korjausmatriisin ja sen avulla lasketut "syndromet".
- Even Rényi informaatio merkkijonosta $\vec{a}$ on korkeintaan t.

Eve tietää t bittiä

- Alice ja Bob tekevät uuden merkkijonon. $\vec{\alpha}^T = G\vec{a}^T$

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad \vec{a} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

$$\vec{\alpha} = \begin{pmatrix} a_1 + a_2 + a_3 & a_2 + a_3 + a_4 \end{pmatrix}$$

- Eve tietää: $\alpha_1 + \alpha_2 = a_1 + a_4$.
- G täytyy valita huolellisesti.

Eve tietää t bittiä

- Teoreema 5.2.1: $\vec{a} \in \mathbf{Z}_2^n$. Eve tietää t bittiä. Alice ja Bob valitsevat matriisin G joka generoi $[n, k]$ lineaarikoodin $C \subset \mathbf{Z}_2^n$, jonka minimipaino on w, ja laskevat uuden merkkijonon $\vec{\alpha}^T = G\vec{a}^T$. Jos $w > t$ niin Eve ei tiedä mitään $\vec{\alpha}$:sta.

Eve tietää t bittiä

- G_i on matriisin rivi i
  $\beta_i \in \mathbf{Z}_2$
  $\vec{c} \in C$
  $\sum_i \alpha_i = \beta_1\alpha_1 + \ldots + \beta_k\alpha_k$
  $= \beta_1 G_i \vec{a}^T + \ldots + \beta_k G_k \vec{a}^T$
  $=(\beta_1 G_1 + \ldots + \beta_k G_k)\vec{a}^T$
  $=\vec{c}^T \vec{a}^T$
- $w(\vec{c}) > t$
  Jokainen $\sum_i \vec{\alpha}_i$ sisältää Evelle tuntemattoman a_i.

Eve tietää pariteetteja.

- Eve tietää korjausmatriisin H ja lasketut "syndromet", jotka Alice ja Bob ovat vaihtaneet julkisella kanavalla.

$$\vec{S} = H\vec{a}^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix}$$

Eve tietää pariteetteja.

- "Syndromet" ovat summia joissa vain yksi tarkastusbitti on aina mukana

$$\begin{pmatrix} a_1 + a_2 + a_3 + a_5 \\ a_1 + a_2 + a_4 + a_6 \\ a_2 + a_3 + a_4 + a_7 \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

- Alice ja Bob tekevät uuden merkkijonon $\vec{\alpha}$ poistamalla bitit $a_5,\ a_6\ ja\ a_7$.
- Eve ei voi päätellä "syndromien" avulla mitään.

Eve tietää pariteetteja.

- Example: $\vec{a} = (1\ 1)$.
- Alice lähettää Bobille
  $H = (1\ 1)$
  $s = 0$.
- Poistamalla viimeisen 1 Bob muodostaa $\vec{\alpha} = 1$.
- Jos Eve tietää, että $\vec{a} \neq (0\ 0)$
- Eve voi päätellä, että $\vec{\alpha} = 1$.

Yleinen tapaus.

- Even tieto ei ole determinististä.

$$P((a_1 + a_6 + a_{17}) \equiv 0 (mod\ 2)) = 0.75$$

- Even Rényi informaatio on korkeintaan t bittiä.
- Alice ja Bob voivat arvioida t suuruuden olevan väärin vastaanotettujen bittien määrä.
- Alicen ja Bobin tavoite on pitää Even Shannon informaatio uudesta merkkijonosta $\vec{\alpha}$ mahdollisimman pienenä.

Yleinen tapaus.

- REFERENCES:
  Bennet, Brassard, Crépeau ja Mauer. Generalized Privacy Amplification. IEE Transactions on information theory, VOL. 41, NO. 6. November 1995.

Yleinen tapaus.

- Todennäköisyys sille, että kaksi riippumattomasti jakaumasta X saatua x ovat samat:

$$P_c(X) = \sum_{x \in X} P(x)^2$$

- Toisen kertaluvun Rényi entropia:

$$R(X) = -log_2(P_c(X)) = -log_2(E[P(X)])$$

- Esim: $X = \{1,0\}^k$, $P(\vec{x}_i = 1,0) = 0.5, 0.5$

$$R(X) = -log_2(\sum_{\vec{x} \in X} (P(\vec{x}))^2) = k$$

Yleinen tapaus.

- Shannon entropia:

$$H(x) = -E[log_2(P(X))]$$

- Jenssenin epäyhtälö konveksille funktiolle ϕ:

$$\phi(\frac{\sum a_i x_i}{\sum a_i}) \leq \frac{\sum a_i \phi(x_i)}{\sum a_i}$$

- $log_2(x)$ on konveksi funktio.
- $log_2(E[x]) \leq E[log_2(x)]$
- $R(x) \leq H(x)$

Yleinen tapaus.

- G on satunnaismuuttuja [k,n]binäärimatriisille
  $g : \{0,1\}^n \rightarrow \{0,1\}^k$

$$H(G(X)|G)$$

$$\geq R(G(X)|G)$$

$$\geq k - log_2(1 + 2^{k-R(X)})$$

$$\geq k - \frac{(2^{k-R(X)})}{ln(2)}$$

Yleinen tapaus.

$$R(G(X)|G) = \sum_g P(g) R(G(X)|G = g)$$

$$= \sum_g P(g)(-log_2(P_c(G(x)|G = g))$$

Jensen epäyhtälöstä:

$$\geq -log_2(\sum_g P(g) P_c(G(X)|G = g))$$

Yleinen tapaus.

$$\geq -log_2(\sum_g P(g)P_c(G(X)|G=g))$$

$$\geq -log_2(P_c(X)+(1-P_c(X))2^{-k})$$

- $P_c(X)$ on todennäköisyys, että $x_1 = x_2$, eli $G(x_1) = G(x_2)$.
- $(1-P_c(X))$ on todennäköisyys sille että $x_1 \neq x_2$ ja silti $G(x_1) = G(x_2)$.

  Tämä tapahtuu todennäköisyydellä $\frac{2^{n-k}}{2^n} = 2^{-k}$

Yleinen tapaus.

- Koska: $P_c(X) = 2^{log_2(P_c(X))} = 2^{-R(X)}$

$$\geq -log_2(P_c(X) + (1 - P_c(X))2^{-k})$$

$$= -log_2(2^{-R(X)} + (1 - 2^{-R(X)})2^{-k})$$

$$> -log_2(2^{-R(X)} + 2^{-k})$$

$$= -log_2(2^{-k}(1 + 2^{k-R(X)}))$$

$$= k - log_2(1 + 2^{k-R(X)})$$

Yleinen tapaus.

- Yhteensä:

$$H(G(X)|G) \geq k - \frac{2^{k-R(X)}}{ln(2)}$$

Yleinen tapaus.

- Eve salakuuntelee ja saa informaatiota $V = \varepsilon(A)$

$$\varepsilon : \{0,1\}^n \rightarrow \{0,1\}^t$$

$$\vec{v} \in \{0,1\}^t$$

$$c_v = |\vec{v} = \varepsilon(\vec{a} \in A)|$$

C_v on lukumäärä vektoreille $\vec{a}$ niin, että $\varepsilon(\vec{a}) = \vec{v}$

$$P(A = a | V = \vec{v}) = \frac{1}{c_v}$$

Yleinen tapaus.

- Törmäys todennäköisyys vektorille $\vec{a}$ kun $V = \vec{v}$

$$P_c(A|V = \vec{v}) = c_v(\frac{1}{c_v})^2 = \frac{1}{c_v}$$

$$R(A|V = \vec{v}) = log_2(c_v)$$

- Sijoitetaan yhtälöön:$H(G(X)|G) \geq k - \frac{2^{k-R(X)}}{ln(2)}$

  Saadaan:

$$H(G(A)|G, V = \vec{v}) \geq k - \frac{2^{k-log_2 c_v}}{ln(2)}$$

Yleinen tapaus.

- Alice ja Bob valitsevat:
  t=virheellisesti vastaanotettujen bittien määrä.
  s=varmuustekijä
- Alice ja Bob arpovat $[k = n - t - s, n]$matriisin G.
- Uusi merkkijono $\alpha = G(A)$
- $$H(\alpha|G, V = \vec{v}) \geq k - \frac{2^k}{c_v ln(2)}$$

Yleinen tapaus.

- Keskiarvona yli kaikkien $\vec{v}$ kun erilaisia vektoreit $\vec{a}$ on 2^n kpl,

$$P(\vec{v}) = c_v 2^{-n}$$

$$H(\alpha|G,V) = \sum_{\vec{v}\in\{0,1\}^t} P(\vec{v}) H(\alpha|G,V=\vec{v})$$

Yleinen tapaus.

- Yhteis informaatio:

$$I(\alpha; GV) = H(\alpha) - H(\alpha|GV)$$

$$\leq k - \sum_{\vec{v}\in\{0,1\}^t} P(\vec{v}) H(\alpha|G, V = \vec{v})$$

$$\leq \sum_{\vec{v}\in\{0,1\}^t} c_v 2^{-n} \frac{2^k}{c_v ln(2)}$$

$$\frac{2^{-n+t+k}}{ln(2)} = \frac{2^{-s}}{ln(2)}$$

Yleinen tapaus.

- s on varmuus tekijä Alicelle ja Bobille.
- Kun s kasvaa yhdellä niin yläraja informaatiolle, jonka Eve tietää, pienenee tekijällä 2.
- Even informaatio k-merkkijonosta $\vec{\alpha}$ on korkeintaan $\frac{2^{-s}}{ln(2)}$.
- $\frac{2^{-s}}{ln(2)}$ ei sisällä merkkijonon $\vec{a}$ pituutta n.

Yhteenveto.

- Even tieto n-mittaisesta merkkijonsta $\vec{a}$ ei ole determinististä.
- Alice ja Bob voivat arvioida Even informaation yläräjaksi väärin vastaanotettujen bittien määrän t.
- Valitaan varmuustekijä s.
- Arvotaan $[n-s-t, n]$ binääri matriisi G.
- Uusi salattu k-merkkijono on $\vec{\alpha}^T = G\vec{a}^T$.
- Uutta merkkijonoa voidaan generoida samalla nopeudella, kuin viestiä lähetetään. Tuloksena on one-time pad tasoinen salaus.
- Alicen ja Bobin saavuttama yksityisyys ei ole determinististä.