MTAT.07.007 Krüptograafia kraadiõppeseminar

Kinnistus- ja krüpteerimisskeemide omavaheline vastavus

Liina Kamm
Tartu Ülikool
kamm@ut.ee

Ülevaade

- Kinnistusskeemid ja omadused
- Krüpteerimisskeemid ja turvalisus
- Krüpteerimis- ja kinnistusskeemide vaheline vastavus
- Omaduste vastavus
- Uurime välja, mis selle keerulise notatsiooni taga ikkagi tegelikult on :)

Kinnistusskeemid

- Saatja, saaja

- Skeemi komponendid

  - Ülesseadmine $\mathsf{pk} \leftarrow \mathsf{Gen}$

  - Kinnistus $\mathsf{Com}_{\mathsf{pk}} : \mathcal{M} \times \mathcal{R} \rightarrow \mathcal{C} \times \mathcal{D}$

  - Avamine $\mathsf{Open}_{\mathsf{pk}} : \mathcal{C} \times \mathcal{D} \rightarrow \mathcal{M} \cup \{\perp\}$

Kinnistusskeemide omadused

- Peitvus
- Siduvus
- Eraldatavus
- Mitte-deformeeritavus

Peitvus

Kinnistusskeem on (t, ε)-peitev, kui t-ajas töötav vastane $A = (A_1, A_2)$ saavutab eelise

$$\mathsf{Adv}^{\mathsf{hid}}_{\mathsf{Com}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ (c_s, d_s) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s, r) : \\ A_2(\sigma, c_s) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Täielik
- Statistiline

Siduvus

Kinnistusskeem on (t, ε)-siduv, kui t-ajas töötav vastane A saavutab eelise

$$\mathsf{Adv}^{\mathsf{bind}}_{\mathsf{Com}}(A) = \Pr\left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen}, (c, d_0, d_1, \sigma) \leftarrow A(\mathsf{pk}) : \\ \bot \neq \mathsf{Open}_{\mathsf{pk}}(c, d_0) \neq \mathsf{Open}_{\mathsf{pk}}(c, d_1) \neq \bot\end{array}\right] \leqslant \varepsilon \ .$$

- Täielik
- Statistiline

Krüpteerimisskeemid

- Saatja, saaja

- Skeemi komponendid

  - ⋆ Ülesseadmine $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
  - ⋆ Krüpteerimine $\mathsf{Enc}_{\mathsf{pk}} : \mathcal{M} \times \mathcal{R} \rightarrow \mathcal{E}$
  - ⋆ Dekrüpteerimine $\mathsf{Dec}_{\mathsf{sk}} : \mathcal{E} \rightarrow \mathcal{M} \cup \{\perp\}$

Krüpteerimisskeemide turvalisus

- Eristamatus valitud tavateksti ründe all (IND-CPA turvalisus)

- Eristamatus valitud kohanduva krüptoteksti ründe all (IND-CCA2 turvalisus)

IND-CPA turvalisus

Kinnistusskeem on (t, ε)-IND-CPA turvaline, kui t-ajas töötav vastane $A = (A_1, A_2)$ saavutab eelise

$$\mathsf{Adv}^{\mathsf{ind-cpa}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : A_2(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Lihtsamalt
- Tuleb tuttav ette?

IND-CCA2 turvalisus

Kinnistusskeem on (t, ε)-IND-CCA2 turvaline, kui t-ajas töötav vastane $A = (A_1, A_2)$ saavutab eelise

$$\mathsf{Adv}^{\mathsf{ind-cca2}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : \\ A_2^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ ,$$

kus $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$ on dekrüpteerimisoraakel.

- Eeldatakse, et A_2 ei lase oraaklil avada krüptoteksti e
- Lihtsamalt

Eraldatavus

- Uus funktsioon $\mathsf{Extr}_{\mathsf{sk}} : \mathcal{C} \to \mathcal{M}$

Kinnistusskeem on (t, ε)-eraldatav, kui t-ajas töötav vastane A saavutab eelise

$$\mathsf{Adv}^{\mathsf{extr}}(A) = \Pr\left[\begin{array}{l}(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}^*, (c, d) \leftarrow A(\mathsf{pk}) : \\ \mathsf{Extr}_{\mathsf{sk}}(c) \neq \mathsf{Open}_{\mathsf{pk}}(c, d) \neq \perp\end{array}\right] \leqslant \varepsilon \ ,$$

kus Gen ja Gen^* poolt väljastatud avalike võtmete pk jaotus langeb kokku.

- Selline skeem on vaid arvutuslikult peitev

- Funktsioon $\mathsf{Extr}_{\mathsf{sk}}$ ei tohi liiga kaua töötada

Krüpteerimis- ja kinnistusskeemide vaheline vastavus

- Krüpteerimisskeem $\mathcal{E}nc = (\mathsf{Gen}_{\mathcal{E}nc}, \mathsf{Enc}, \mathsf{Dec})$
- Kinnistusskeem $\mathcal{C}om = (\mathsf{Gen}_{\mathcal{C}om}, \mathsf{Gen}^*_{\mathcal{C}om}, \mathsf{Com}, \mathsf{Open}, \mathsf{Extr})$
- Krüpteerimisskeemist kinnistusskeem
- Kinnistusskeemist krüpteerimisskeem

Krüpteerimisskeemist kinnistusskeem

- Meil on olemas $\mathcal{E}nc = (\mathsf{Gen}_{\mathcal{E}nc}, \mathsf{Enc}, \mathsf{Dec})$
- Mida on vaja?
  - ⋆ Ülesseadmine
  - ⋆ Kinnistus
  - ⋆ Avamine

Kinnistusskeemist krüpteerimisskeem

- Meil on olemas $\mathcal{C}om = (\mathsf{Gen}_{\mathcal{C}om}, \mathsf{Gen}^*_{\mathcal{C}om}, \mathsf{Com}, \mathsf{Open}, \mathsf{Extr})$

- Mida on vaja?
  - ⋆ Ülesseadmine
  - ⋆ Krüpteerimine
  - ⋆ Dekrüpteerimine

IND-CPA turvalisus ja peitvus

$$\mathsf{Adv}^{\mathsf{ind-cpa}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : A_2(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

ja

$$\mathsf{Adv}^{\mathsf{hid}}_{\mathsf{Com}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ (c_s, d_s) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s, r) : \\ A_2(\sigma, c_s) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Samaväärsed?

IND-CPA turvalisus ja peitvus

$$\mathsf{Adv}^{\mathsf{ind-cpa}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : A_2(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

ja

$$\mathsf{Adv}^{\mathsf{hid}}_{\mathsf{Com}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ (c_s, d_s) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s, r) : \\ A_2(\sigma, c_s) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Samaväärsed? Jah!

Deformeeritavus

- Sisukad muudatused
- Vahendusrünne

$$Alice \xrightarrow{x} Eve \xrightarrow{x+y} Bob$$

- Homomorfsed kinnistusskeemid

$$\mathsf{Com}_{\mathsf{pk}}(m_1; r_1) \circ \mathsf{Com}_{\mathsf{pk}}(m_2; r_2) = \mathsf{Com}_{\mathsf{pk}}(m_1 + m_2; r_1 + r_2)$$

Mitte-deformeeritavus

- Mitte-deformeeritavus avamise suhtes
  - ⋆ Vastane ei saa muuta kinnistust nii, et ta seda avada suudaks
- Mitte-deformeeritavus kinnistuse suhtes
  - ⋆ Vastane ei saa olemasoleva kinnistuse põhjal uut kinnistust luua
- Mitte-deformeeritavus kinnistuse suhtes on tugevam eeldus

Mitte-deformeeritavus avamise suhtes (mäng)

$\mathcal{G}^{A}_{\mathsf{nm-open}}$

$\mathsf{pk} \leftarrow \mathsf{Gen}$

$(m_0, m_1, \sigma_1) \leftarrow A_1(\mathsf{pk})$

$s \leftarrow \{0, 1\}$

$(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s)$

$(\hat{c}_1, \ldots, \hat{c}_n, \sigma_2) \leftarrow A_2(c, \sigma_1)$

$(\hat{d}_1, \ldots, \hat{d}_n) \leftarrow A_3(d, \sigma_2)$

$y_i \leftarrow \mathsf{Open}_{\mathsf{pk}}(\hat{c}_i, \hat{d}_i), i = (1, \ldots, n)$

halt if $c \in (\hat{c}_1, \ldots, \hat{c}_n) \vee \perp \in (y_1, \ldots, y_n)$

if $A_4(m_1, y_1, \ldots, y_n, \sigma_2) = s$, return 1

else return 0

Mitte-deformeeritavus avamise suhtes

Kinnistusskeem on (t, ε)-mitte-deformeeritav avamise suhtes kui t-ajas töötav vastane $A = (A_1, A_2, A_3, A_4)$, kes mängib mängu $\mathcal{G}_{\mathsf{nm-open}}$ saavutab eelise

$$\mathsf{Adv}^{\mathsf{nm}}_{\mathcal{C}om}(A) = \left|2 \cdot \Pr\left[\mathcal{G}^A = s\right] - 1\right| \leq \varepsilon \ .$$

- Mitte-deformeeritavusest avamise suhtes järelduvad nii peitvus kui siduvus

Mitte-deformeeritavus kinnistuse suhtes (mäng)

$\mathcal{G}^{A}_{\mathsf{nm-com}}$

- $\mathsf{pk} \leftarrow \mathsf{Gen}$
- $(m_0, m_1, \sigma_1) \leftarrow A_1(\mathsf{pk})$
- $s \leftarrow \{0, 1\}$
- $(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s)$
- $(\widehat{c}_1, \ldots, \widehat{c}_n, \sigma_2) \leftarrow A_2(c, \sigma_1)$
- $(y_1, \ldots, y_n) \leftarrow \mathsf{Extr}_{\mathsf{sk}}(\widehat{c}_1, \ldots, \widehat{c}_n)$
- halt if $c \in (\widehat{c}_1, \ldots, \widehat{c}_n)$
- if $A_4(m_1, y_1, \ldots, y_n, \sigma_2) = s$, return 1
- else return 0

Mitte-deformeeritavus kinnistuse suhtes

Kinnistusskeem on (t, ε)-mitte-deformeeritav avamise suhtes kui t-ajas töötav vastane $A = (A_1, A_2, A_4)$, kes mängib mängu $\mathcal{G}_{\mathsf{nm-com}}$ saavutab eelise

$$\mathsf{Adv}^{\mathsf{nm}}_{\mathcal{C}om}(A) = \left|2 \cdot \Pr\left[\mathcal{G}^A = s\right] - 1\right| \leq \varepsilon \ ,$$

kus Extr on selline arvutatav funktsioon, et kui $(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(x)$, siis $\mathsf{Extr}_{\mathsf{pk}}(c) = x$

- Mitte-deformeeritavusest kinnistuse suhtes järeldub mitte-deformeeritavus avamise suhtes

IND-CCA2 turvalisus ja mitte-deformeeritavus

- IND-CCA2 turvalisusest järeldub mitte-deformeeritavus
- Vastupidine ei kehti

Tänan!