Adaptívne medové šifrovanie

Erika Szelleová

Školiteľ: doc. RNDr. Martin Stanek, PhD.

17. 06. 2020

Úvod

- Medové šifrovanie - angl. Honey Encryption
- Ari Juels and Thomas Ristenpart: “Honey encryption: Security beyond the brute-force bound” (2014)
- Útok s obnovou správy (Message recovery attack)
  - útočník dostane šifrový text, hľadá prislúchajúci otvorený text
  - má informáciu o očakávanej štruktúre otvoreného textu
  - skúša dešifrovať rôznymi kľúčmi
  - ak výstup z dešifrovacieho algoritmu zodpovedá danej štruktúre, prislúchajúci kľúč prehlási za správny
- cieľ:
  - pri dešifrovaní ľubovoľným nesprávnym kľúčom bude schéma vracať správne vyzerajúci otvorený text

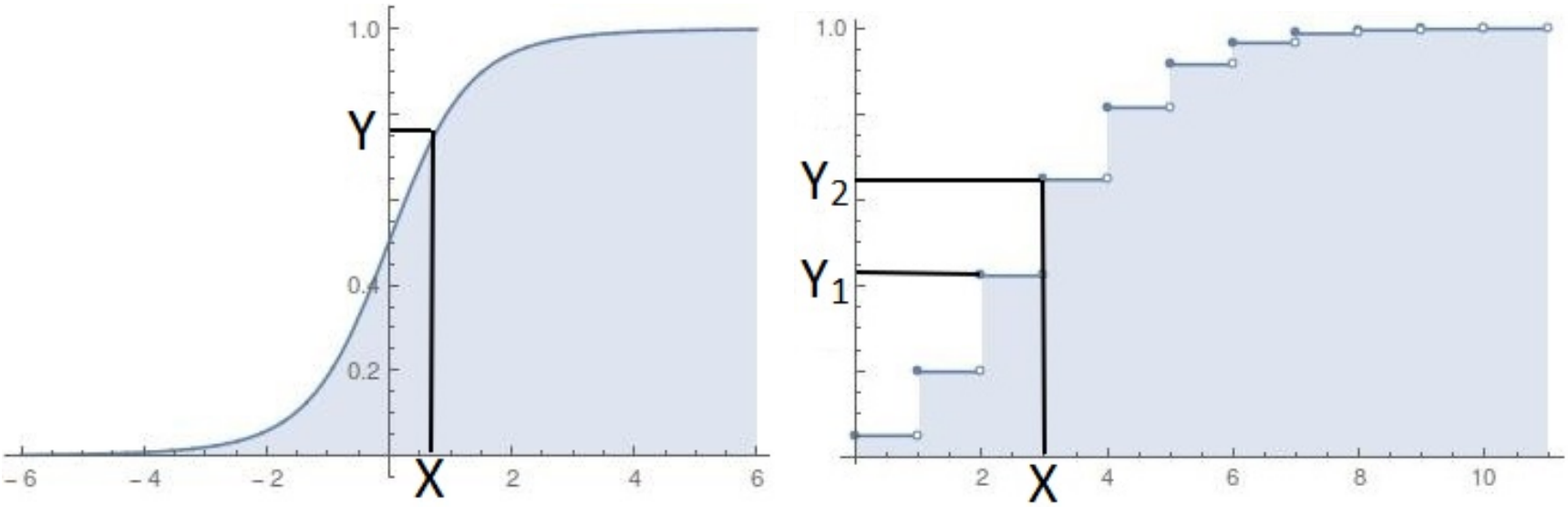
Medové šifrovanie - základné pojmy

- DTE - Distribution transforming encoder
  - kóder, kt. transformuje pravdepodobnostné rozdelenie svojich vstupov
- Schéma "Kóduj a šifruj" (DTE-and-encrypt)
  - symetrická schéma + špeciálny kóder a dekóder
  - kóder sa aplikuje pred šifrovaním, dekóder po dešifrovaní
  - nech p_m je pravdepodobnostné rozdelenie otvorených textov
  - pred šifrovaním: transformácia z rozdelenia p_m na rovnomerné rozdelenie na intervale $[0, 1)$
  - po dešifrovaní: transformácia z rovnomerného rozdelenia na intervale $[0, 1)$ späť na p_m
  - pozn.: kóder vracia rovnomerne rozdelené čísla s fixnou bitovou dĺžkou

Konštrukcia DTE

1. Spätné vzorkovanie (Inverse transform sampling)
   - všeobecná metóda konštrukcie DTE
   - vyžaduje znalosť distribučnej funkcie správ (alebo jej aproximácie)
2. Markovov model
   - trénuje sa pomocou vhodne zvoleného korpusu
3. Pravdepodobnostná bezkontextová gramatika
   - kompaktnejší model ako tie predošlé
   - ťažšie sa vytvára - vyžaduje hlbšiu analýzu

Konštrukcia DTE - spätné vzorkovanie



Obr.: Spätné vzorkovanie. Hodnote X priradíme hodnotu Y (v prípade spojitej náhodnej premennej) resp. náhodnú hodnotu z intervalu $(Y_1, Y_2]$ (v prípade diskrétnej náhodnej premennej)

Motivácia

- doterajšie výskumy vytvárali statické modely
  - na základe dopredu známeho rozdelenia otvorených textov
  - alebo pomocou trénovacej množiny (korpusu)
- modely sú príliš špecifické a ťažko sa vytvárajú nové
- niekedy nemáme vopred danú informáciu o štruktúre/rozdelení otvorených textov
- rozdelenie otvorených textov sa časom môže meniť

Cieľ práce

- modifikovať schému medového šifrovania aby sme dosiahli:
  1. **Adaptívnosť**. DTE schémy sa prispôsobuje rozdeleniu otvorených textov.
  2. **Univerzálnosť**. Schéma by mala vedieť pracovať s ľubovoľným priestorom otvorených textov, bez ohľadu na jeho rozdelenie.
  3. **Korektnosť**.
- výsledok: **adaptívne medové šifrovanie** (**AHE**)

Návrh schémy - Apriórne rozdelenie, aposteriórne rozdelenie, vierohodnosť

- v našej práci sme sa zaoberali iba s celočíselnými vstupmi
- zvolili sme si spätné vzorkovanie
- vychádzali sme z metód Bayesovskej štatistiky
- predpoklad: otvorené texty majú parametrické rozdelenie X_θ
- trénuje sa rozdelenie parametrov θ
- nech $\mathcal{D} = \{x, \cdots x_n\}$ je postupnosť otvorených textov a $f_{\mathcal{X}_\theta}$ je funkcia hustoty pre $\mathcal{X}_\theta$

Definícia (Apriórne rozdelenie, aposteriórne rozdelenie, vierohodnosť)

$$P[\theta|\mathcal{D}] \propto L(\mathcal{D}, \theta) \cdot P[\theta],$$

kde:

- $P[\theta]$ *sa nazýva* **apriórne rozdelenie parametrov**
- $P[\theta|\mathcal{D}]$ *je* **aposteriórne rozdelenie parametrov**
- $L(\mathcal{D}, \theta)$ *je* **vierohodnosť**: $L(\mathcal{D}, \theta) = \prod_{i=1}^{n} f_{\mathcal{X}_\theta}(x_i)$

Návrh schémy - konjugované apriórne rozdelenie

- pri kódovaní potom použijeme aposteriórne rozdelenie parametrov
  - zvolíme si zoznam parametrov na základe jeho rozdelenia (napr. náhodný výber, stredná hodnota)
- z tohto vzorca sa ľahko odvodí aj vzorec na sekvenčné trénovanie
- použili sme tzv. **konjugované apriórne rozdelenie**
- apriórne rozdelenie parametrov sa zvolí tak, aby to aposteriórne patrilo do rovnakej triedy parametrických rozdelení ako apriórne
- napr. ak otvorené texty majú normálne rozdelenie $\mathcal{N}(\mu, \sigma^2)$ a apriórne rozdelenie parametrov $(\mu, 1/\sigma^2)$ je normálno-gama rozdelenie, potom aj aposteriórne rozdelenie parametrov bude normálno-gama rozdelenie

Návrh schémy - DTE

- tri parametrické rozdelenia na popis otvorených textov:
  - normálne rozdelenie: $\mathcal{N}(\mu, \sigma^2)$
  - logaritmicko-normáne rozdelenie: $\texttt{LogNorm}(\mu, \sigma^2)$
  - gama rozdelenie: $\texttt{Gamma}(\alpha, \beta)$
- našli sme k nim vhodné konjugované apriórne rozdelenia
- model sa aktualizuje pred každým šifrovaním
- pri kódovaní sa zvolí buď náhodný zoznam parametrov alebo očakávané hodnoty parametrov
- model v DTE sa trénuje sekvenčne, ale pri kódovaní nemusíme použiť ten najaktuálnejší
  - pri kódovaní sa môže použiť staršia verzia modelu, ktorá sa pravidelne aktualizuje (napr. vždy po určitom počte šifrovaní)
- parametre modelu sa prenášajú v otvorenom tvare spolu so šifrovým textom

Implementácia

- implementované v jazyku Python
- použila sa špeciálna knižnica s možnosťou nastavenia výpočtovej presnosti
- symetrická šifra: DES, mód CFB
- každý vstup sa kóduje do bitovej postupnosti, ktorá obsahuje:
  - počet parametrov (jeden bajt)
  - zoznam parametrov (8 bajtov na jeden parameter)
  - šifrový text (v našom prípade 16 bajtov)

Bezpečnosť (1)

- nový pojem: **bezpečnosť voči sledovaniu správ**

Definícia (Bezpečnosť voči sledovaniu správ)

Majme adaptívnu schému medového šifrovania AHE a nech $T = \{\theta_i\}_{i=1}^{m}$ *je postupnosť zoznamov parametrov zo všetkých šifrových textov, ktoré sa doposiaľ šifrovali schémou AHE. S využitím tejto postupnosti a hry na obrázku 2 definujeme výhodu útočníka* $\mathcal{A}$ *nasledovne:*

$$\mathsf{Adv}^{\mathrm{mt}}_{AHE,T}(\mathcal{A}) = \Pr\left[MT^{\mathcal{A}}_{AHE,T} \rightarrow \mathsf{true}\right]$$

Bezpečnosť schémy voči sledovaniu správ sa potom definuje ako:

$$\mathsf{Adv}^{\mathrm{mt}}_{AHE,T} = \max_{\mathcal{A}} \mathsf{Adv}^{\mathrm{ahe}}_{AHE,T}(\mathcal{A})$$

Bezpečnosť (2)

$\mathrm{MT}^{\mathcal{A}}_{\mathrm{AHE},T}$

1 : $M \leftarrow_{p_m} \mathcal{M}$

2 : $K \leftarrow_{p_k} \mathcal{K}$

3 : $C \leftarrow_{\$} \mathrm{aheEncrypt}(M, K)$

4 : $M' \leftarrow \mathcal{A}(T, C)$

5 : **return** $M = M'$

Obr.: Hra definujúca bezpečnosť voči sledovaniu správ

- navrhli sme útok voči AHE schéme so špecifickými predpokladmi

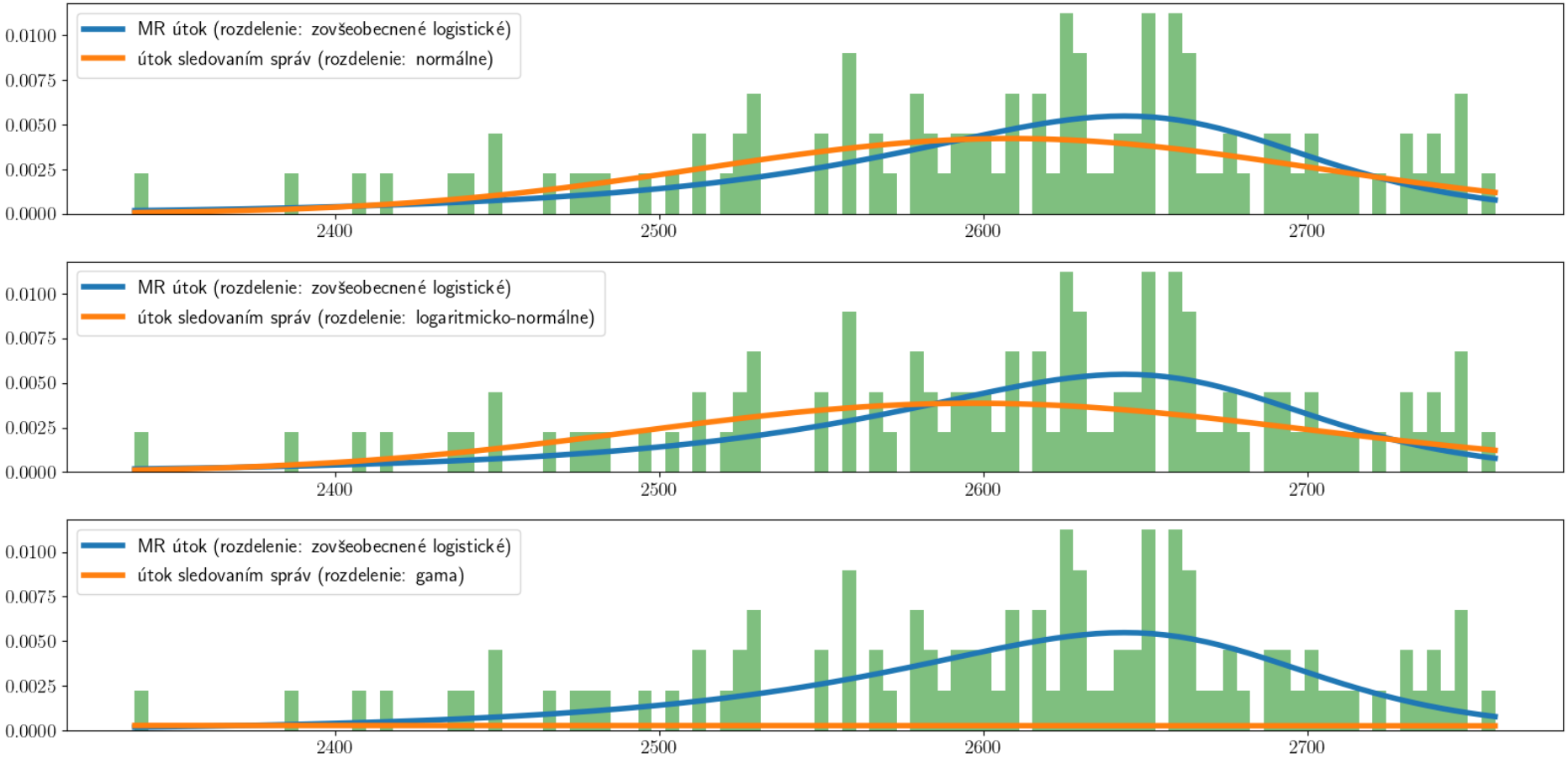
Experimenty - návrh

- navrhli sme dva útoky, ktoré aplikujú slovníkový útok na danú schému
- najprv sme zašifrovali niekoľko otvorených textov z trénovacej množiny
- náhodne si zvolíme otvorené texty spomedzi tých, ktoré už boli šifrované AHE schémou a zašifrujeme ich náhodným heslom
- útočník potom vytvára zoznamy hesiel utriedených podľa pravdepodobnosti
- pravdepodobnosť sa počíta zo združenej pravdepodobnosti hesla a otvoreného textu
- pravdepodobnosť otvoreného textu sa počíta dvomi spôsobmi:
  - frekvencia otvoreného textu v trénovacej množine
  - parametre použité v AHE schéme (zo šifrového textu)
- skúmame priemerné poradia správnych hesiel v zoznamoch

Experimenty - výsledky (1)

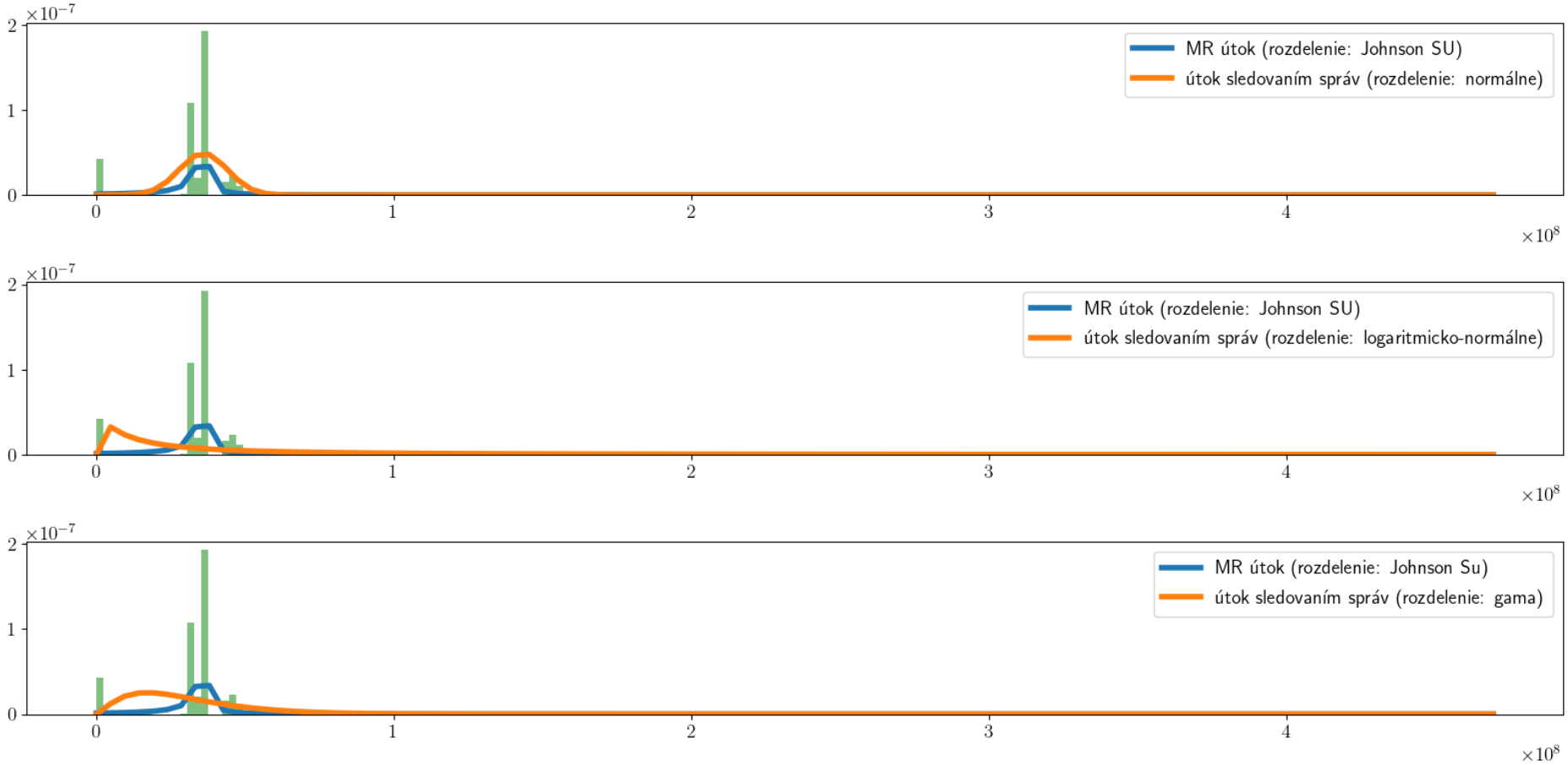
- rôzne počiatočné nastavenia, ktoré sme dosiahli kombináciou troch premenných
  - `sequential` - používa sa vždy najaktuálnejší model? [`true` / `false`]
  - `randomParams` - náhodné parametre či očakávaná hodnota parametrov? [`true` / `false`]
  - `modelType` - ktorým rozdelením sa modeluje priestor otvorených textov [`normal` / `lognormal` / `gamma`]
- tri rôzne trénovacie množiny
  - identifikačné čísla organizácií (IČO)
  - ELO hráčov zo šachového turnaja
  - generované dáta
- zoznam hesiel zo stránky PasteBin
- gama model bol najmenej vhodný na použitie v AHE schéme
- naša schéma je citlivá na vyčnievajúce sa hodnoty
- zvolené modely nie vždy sú vhodné na aproximáciu rozdelenia otvorených textov

Experimenty - výsledky (2)



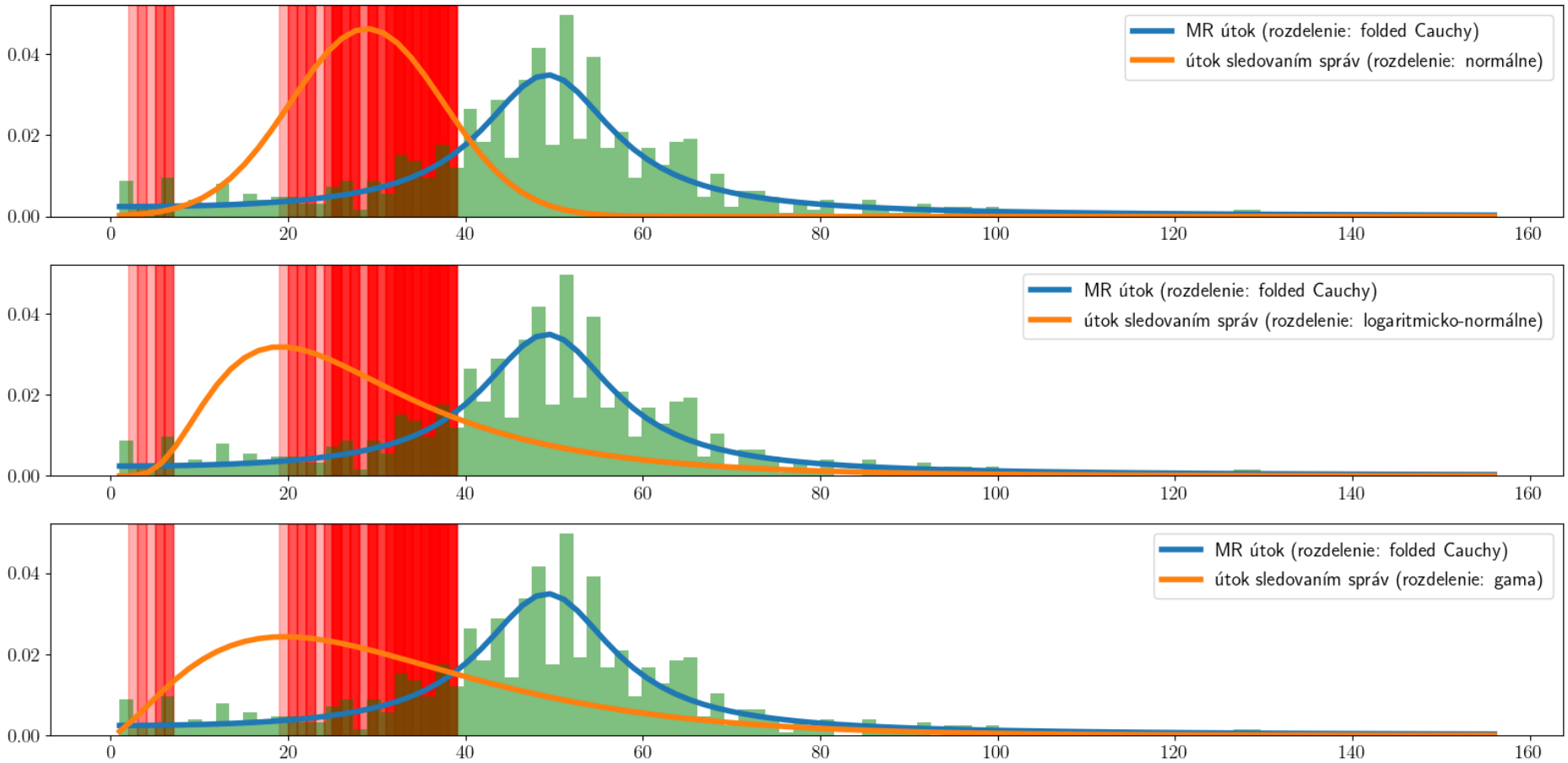
Obr.: Grafy aproximácií rozdelenia otvorených textov s histogramom všetkých dát pre databázu `chessResults.TB1` (`sequential` = `true`, `randomParams` = `false`)

Experimenty - výsledky (3)



Obr.: Grafy aproximácií rozdelenia otvorených textov s histogramom všetkých dát pre databázu `enviroportal` – `ipkz.ICO` (`sequential` = `true`, `randomParams` = `false`)

Experimenty - výsledky (4)



Obr.: Grafy aproximácií rozdelenia otvorených textov s histogramom všetkých dát pre databázu `generated` – `data.dataset1` (`sequential` = `true`, `randomParams` = `false`). Prvých 130 prvkov databázy (trénovaciu množinu) sme vyznačili červenou farbou.

Záver

- cieľom práce bolo navrhnúť adaptívnu schému medového šifrovania
- našli sme riešenie tohto problému s využitím Bayesovej vety
- navrhnutý algoritmus sme naimplementovali a vyskúšali s rôznymi vstupnými dátami
- zadefinovali sme nový pojem bezpečnosti - bezpečnosť voči sledovaniu správ - a navrhli sme útok voči schéme
- navrhli sme a vykonali sme niekoľko experimentov na otestovanie našej implementácie

Ďakujem za pozornosť!