

# **О доверительном оценивании практической секретности для некоторых вероятностных моделей**

**Кирилл Царегородцев  
Марина Скоробогатова**

Компания «Актив»

# Содержание раздела

- 1 Введение
- 2 Схема Бернулли
- 3 Дельта-метод
- 4 Монотонное преобразование
- 5 Параметрический бутстрэп
- 6 Марковская цепь фиксированного порядка

# Практическая секретность

- Пусть некоторый генератор выдает последовательность **независимых** двоичных строк, используемых в качестве ключей в СКЗИ:  $(K_1, K_2, K_3, \dots)$ ,  $K_i \in \{0, 1\}^{klen}$ .
- Рассматривается следующая процедура определения ключа в ходе множественного эксперимента — **алгоритм усеченного опробования**:
  - противник упорядочивает ключи  $K \in \{0, 1\}^{klen}$  в порядке неубывания их вероятностей:  $p_1 \geq p_2 \geq \dots \geq p_{2^{klen}}$ ;
  - для каждого экземпляра СКЗИ противник перебирает некоторую долю  $\pi_0$  ключевого множества  $\{0, 1\}^{klen}$ , начиная с наиболее вероятного ключа;
  - если после перебора доли ключевого множества правильный ключ не был найден, противник переходит к следующему экземпляру шифраппаратуры и вновь начинает перебор доли ключей, начиная с наиболее вероятного.
- Практическая секретность (ключей/распределения): средняя трудоемкость алгоритма усеченного опробования.

# История вопроса

- Понятие введено и происследовано в работах [1] ; подробно рассмотрен случай схемы Бернулли (независимые, одинаково распределенные двоичные знаки).
- Работы [2] : связь между критериями секретности в квантовой и классической криптографии.
- Работа [3] : неравенства на допустимые отклонения распределения ключей от равномерного распределения на  $\{0, 1\}^{klen}$ , при выполнении которых практическая секретность ключа все ещё остается высокой.

---

[1] И. М. Арбеков, «Критерии секретности ключа»; I. M. Arbekov, «Lower bounds for the practical secrecy of a key».

[2] С. Н. Молотков, «Одноразовый блокнот, сложность перебора ключей и практическая секретность квантовой криптографии»; И. М. Арбеков и С. Н. Молотков, «Различимость квантовых состояний и трудоемкость по Шеннону в квантовой криптографии»; I. M. Arbekov и S. N. Molotkov, «Shannon unicity distance,  $\varepsilon$ -secrecy criterion and Holevo information in quantum cryptography».

[3] В. О. Дрелихов, «О практической безопасности ключа».

## История вопроса-2

- Работы [4] : обобщение ситуации на случай, когда порождаемые двоичные знаки могут быть зависимы.
- Работа [5] : методика оценки практической секретности для мгновенных значений стационарных гауссовских процессов.

---

[4] В. О. МIRONKIN и М. М. Михайлов, «Об энтропии последовательной процедуры опробования дискретной вероятностной схемы»; А. С. Логачев и В. О. МIRONKIN, «О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа».

[5] D. S. Bogdanov, «On the practical secrecy of keys formed from instantaneous values of a stationary Gaussian process».

# Основная идея доклада

- Ранее были предложены **точечные оценки** на величину практической секретности в **фиксированной вероятностной модели**.
- Фактически, мы находимся в ситуации неопределенности: параметры вероятностной модели оцениваются по данным; оценкам сопутствует некоторая неустранимая неопределенность.
- Предлагается учитывать эту неопределенность в оценке практической секретности с помощью стандартного аппарата доверительного оценивания.
- Рассмотрены две статистические модели:  $\{X_n\}$  образуют последовательность независимых случайных величин с неизвестным одинаковым  $p$  (схема Бернулли);  $\{X_n\}$  образуют марковскую цепь фиксированного порядка  $r$ .

# Направления исследования

- Получение теоретических результатов в некоторых базовых предположениях.
- Проверка полученных результатов на синтетических данных (модельные условия):  $M = 10^3$  выборок, длина каждой выборки  $N = 10^6$ .
- По полученным синтетическим выборкам строились доверительные интервалы (ДИ) для логарифма практической секретности.
- Полученный фактический уровень покрытия ДИ истинного значения сравнивался с теоретически ожидаемым уровнем  $(1 - \alpha)$ , где  $\alpha$  — фиксированный уровень значимости для ДИ.

# Обозначения

$\hat{\theta}_n$ : оценка для параметра  $\theta$ , построенная по выборке объема  $n$ ;

$X_n \xrightarrow{\mathbf{P}} \xi$ ,  $X_n \xrightarrow{\mathcal{D}} \xi$ : сходимость случайных величин  $X_n$  к  $\xi$  по вероятности/по распределению;

$\text{Ber}(p)$ : распределение Бернулли с параметром  $p$ ;

$\mathcal{N}(\mu, \sigma^2)$ ,  $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ : нормальное распределение со средним  $\mu$  (вектором средних  $\boldsymbol{\mu}$ ) и дисперсией  $\sigma^2$  (матрицей ковариации  $\boldsymbol{\Sigma}$ );

$\text{grad}g(\boldsymbol{\mu})$ : значение градиента функции  $g: \mathbb{R}^r \rightarrow \mathbb{R}$  в точке  $\boldsymbol{\mu}$ ;

$\text{bitstr}_\ell(x)$ : двоичное представление  $x$  в виде  $\ell$ -битового числа;



# Содержание раздела

- 1 Введение
- 2 Схема Бернулли**
- 3 Дельта-метод
- 4 Монотонное преобразование
- 5 Параметрический бутстрэп
- 6 Марковская цепь фиксированного порядка

# Объект изучения

- Схема Бернулли — последовательность  $(X_1, X_2, X_3, \dots)$ ,  $X_i \sim \text{Ber}(p)$ , независимых одинаково распределенных случайных величин.
- Смещение: величина  $\varepsilon = p - 1/2$ .
- Практическая секретность  $T_{klen}(\varepsilon)$ : зависит от параметра  $\varepsilon$  и длины ключа  $klen$  (минимизируем по  $\pi_0$ ).
- Для численной стабильности будем оценивать логарифм:  $T(\varepsilon) = \log(T_{256}(\varepsilon))$ .
- Основная задача: оценить  $\varepsilon$ , учесть неопределенность оценки, перенести неопределенность в оценку на  $T(\varepsilon)$ .

# Рассмотренные методы

- **Дельта-метод:** стандартная оценка с помощью среднего арифметического  $\Rightarrow$  асимптотическая нормальность оценки  $\Rightarrow$  сохранение свойства при функциональных преобразованиях (дельта-метод)  $\Rightarrow$  асимптотически нормальная оценка на практическую секретность.
- **Монотонные преобразования:** доверительные интервалы для  $\varepsilon$  (Клоппера-Пирсона, Уилсона, Логит)  $\Rightarrow$  монотонное преобразование  $(x \rightarrow T(x))$   $\Rightarrow$  доверительный интервал для  $T(\varepsilon)$ .
- **Бутстрэп:** оценивание дисперсии оценки с помощью процедуры (параметрического) бутстрэпа.

# Содержание раздела

- 1 Введение
- 2 Схема Бернулли
- 3 Дельта-метод**
- 4 Монотонное преобразование
- 5 Параметрический бутстрэп
- 6 Марковская цепь фиксированного порядка

# Асимптотически нормальная оценка

- Рассмотрим оценку  $\widehat{\varepsilon}_n = \left( \frac{\sum_{i=1}^n X_i}{n} - \frac{1}{2} \right)$ .
- В силу Центральной предельной теоремы:

$$\sqrt{n} \cdot (\widehat{\varepsilon}_n - \varepsilon) \xrightarrow{\mathcal{D}} \mathcal{N} \left( 0, \frac{1}{4} - \varepsilon^2 \right).$$

- Дельта-метод для функции  $x \rightarrow T(x)$ :

$$\sqrt{n} \cdot (T(\widehat{\varepsilon}_n) - T(\varepsilon)) \xrightarrow{\mathcal{D}} \mathcal{N} \left( 0, \left( \frac{1}{4} - \varepsilon^2 \right) \cdot (T'(\varepsilon))^2 \right).$$

- $\left( \frac{1}{4} - \varepsilon^2 \right)$  оцениваем сверху значением  $1/4$ .
- Для  $(T'(\varepsilon))^2$  по теореме о непрерывном отображении справедливо:

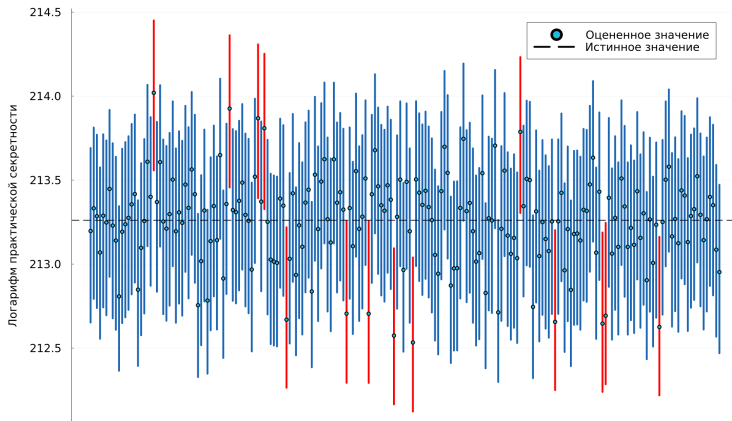
$$(T'(\widehat{\varepsilon}_n))^2 \xrightarrow{\mathbf{P}} (T'(\varepsilon))^2.$$

# Асимптотически нормальная оценка: ДИ

- Получен асимптотический ДИ для величины  $T(\varepsilon)$ :

$$\left( T(\hat{\varepsilon}_n) + \frac{|T'(\hat{\varepsilon}_n)| \cdot q_{\alpha/2}}{2\sqrt{n}}, T(\hat{\varepsilon}_n) + \frac{|T'(\hat{\varepsilon}_n)| \cdot q_{1-\alpha/2}}{2\sqrt{n}} \right).$$

- Величина  $T'(\hat{\varepsilon}_n)$  может быть оценена методами автоматического или численного дифференцирования.



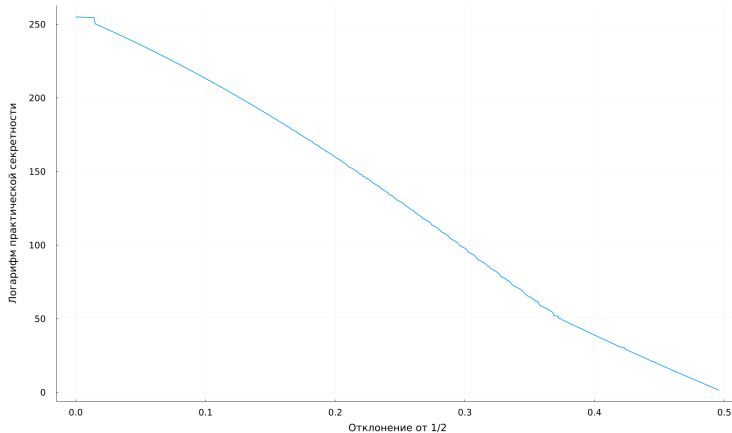
**Рис. 1:** Асимптотические двусторонние 95%-ные ДИ, дельта-метод; синим (красным) отмечены интервалы, (не) покрывающие истинное значение логарифма практической секретности; доля интервалов, покрывших истинное значение логарифма, равна  $0.948 \approx 1 - \alpha$

# Содержание раздела

- 1 Введение
- 2 Схема Бернулли
- 3 Дельта-метод
- 4 Монотонное преобразование**
- 5 Параметрический бутстрэп
- 6 Марковская цепь фиксированного порядка



# Зависимость сложности перебора от неравновероятности

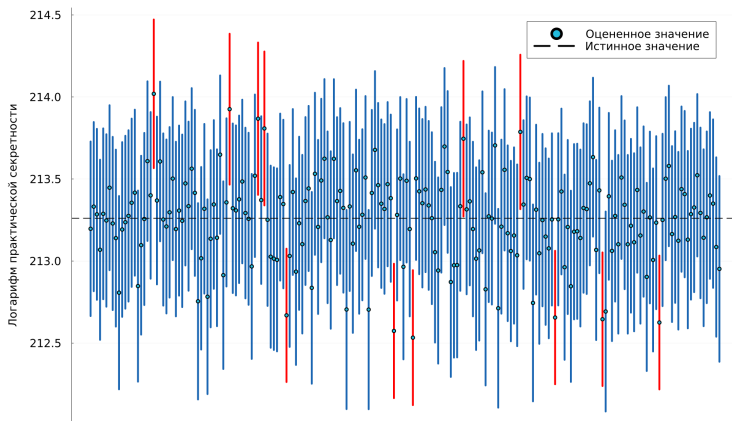


**Рис. 2:** Логарифм практической секретности в зависимости от отклонения  $\varepsilon$ ,  $T(x)$  является монотонно убывающей

# Монотонное преобразование: идея

- Пусть для параметра  $p$  схемы Бернулли построен ДИ  $(\hat{p}_L, \hat{p}_R)$  уровня  $(1 - \alpha)$ .
- Положим  $\hat{\varepsilon}_L = \hat{p}_L - 1/2$ ,  $\hat{\varepsilon}_R = \hat{p}_R - 1/2$ .
- Если  $\varepsilon_L < 0$ , то положим  $\varepsilon_R = \max(|\varepsilon_L|, |\varepsilon_R|)$ ,  $\varepsilon_L = 0$ .
- В таком случае для величины  $T(\varepsilon)$  можно построить ДИ  $(T(\hat{\varepsilon}_R), T(\hat{\varepsilon}_L))$ :

$$\begin{aligned}\mathbb{P}[\hat{\varepsilon}_L \leq \varepsilon \leq \hat{\varepsilon}_R] &\geq 1 - \alpha, \\ \mathbb{P}[T(\hat{\varepsilon}_R) \leq T(\varepsilon) \leq T(\hat{\varepsilon}_L)] &\geq 1 - \alpha.\end{aligned}$$



**Рис. 3:** Двусторонние 95%-ные ДИ, монотонное преобразование на основе интервала Клоппера-Пирсона; синим (красным) отмечены интервалы, (не) покрывающие истинное значение логарифма практической секретности; доля интервалов, покрывших истинное значение логарифма, равна  $0.945 \approx 1 - \alpha$

# Содержание раздела

- 1 Введение
- 2 Схема Бернулли
- 3 Дельта-метод
- 4 Монотонное преобразование
- 5 Параметрический бутстрэп**
- 6 Марковская цепь фиксированного порядка

# Параметрический бутстрэп

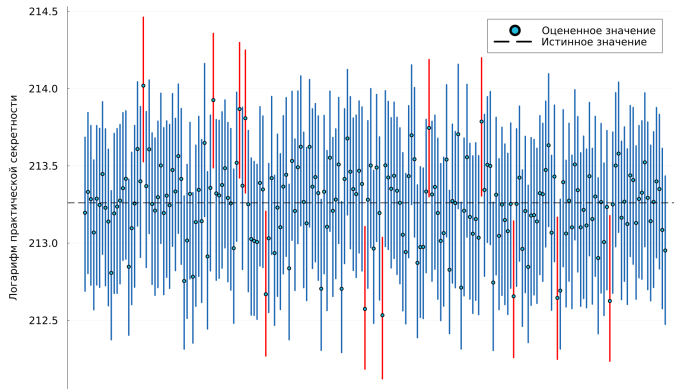
- Пусть для исходной выборки фиксирована некоторая вероятностная модель  $M = \{\xi(\alpha)\}$  — семейство распределений  $\xi$  с параметрами  $\alpha = (\alpha_1, \dots, \alpha_r)$ .
- По исходной выборке оценим параметры конкретного распределения  $\hat{\alpha}_n$  из модели  $M$ .
- Сгенерируем  $B$  псевдовыборок размера  $N$   $\mathbf{X}_j^*$ ,  $1 \leq j \leq B$ , из распределения  $\xi^* = M(\hat{\alpha}_n)$ .
- По каждой псевдовыборке  $\mathbf{X}_j^*$ ,  $1 \leq j \leq B$ , оценим искомую величину:

$$\hat{\theta}_{N,j} = f(\mathbf{X}_j^*), \quad 1 \leq j \leq B.$$

- В качестве двустороннего  $(1 - \alpha)$ -ДИ для  $\theta$  возьмем интервал

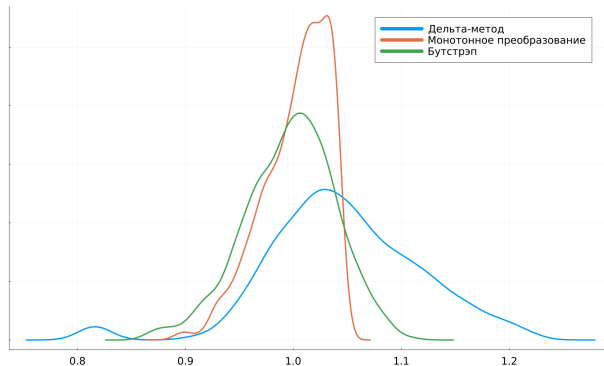
$$\left( \text{quantile} \left( (\hat{\theta}_{N,j})_{j=1}^B, \alpha/2 \right), \text{quantile} \left( (\hat{\theta}_{N,j})_{j=1}^B, 1 - \alpha/2 \right) \right).$$

# Параметрический бутстрэп: результаты



**Рис. 4:** Двусторонние 95%-ные ДИ, параметрический бутстрэп; синим (красным) отмечены интервалы, (не) покрывающие истинное значение логарифма практической секретности; доля интервалов, покрывших истинное значение логарифма, равна  $0.944 \approx 1 - \alpha$

# Небольшое сравнение методов



**Рис. 5:** Распределение длин полученных ДИ для разных методов, ядерная оценка плотности

# Небольшое сравнение методов

Метод	Ср. зн.	СКО	min	$q_{0.25}$	Мед.	$q_{0.75}$	max
Дельта	1.0464	0.0707	0.8119	1.0037	1.0434	1.0914	1.2201
Моноот.	1.0024	0.0306	0.8913	0.9823	1.0089	1.0268	1.0435
Boot.	0.9967	0.0422	0.8642	0.9692	0.9999	1.026	1.11



# Содержание раздела

- 1 Введение
- 2 Схема Бернулли
- 3 Дельта-метод
- 4 Монотонное преобразование
- 5 Параметрический бутстрэп
- 6 Марковская цепь фиксированного порядка**

# Объект изучения

- Марковская цепь порядка  $r \in \mathbb{N}$  — последовательность случайных величин  $\{X_n\}$ ,  $X_i \in \{0, 1\}$ , для любого  $n \in \mathbb{N}$  выполнено

$$\begin{aligned} \mathbb{P}[X_{n+r} = b_{n+r} \mid X_1 = b_1, \dots, X_{n+r-1} = b_{n+r-1}] = \\ = \mathbb{P}[X_{n+r} = b_{n+r} \mid X_n = b_n, \dots, X_{n+r-1} = b_{n+r-1}]. \end{aligned}$$

- В работе [6] формула для  $T(\varepsilon)$  получена в случае, когда распределение двоичных знаков  $\{X_n\}$  таково, что для любого  $n \in \mathbb{N}$  выполнены неравенства

$$\left(\frac{1}{2} - \varepsilon\right)^n \leq \mathbb{P}[X_1 = b_1, \dots, X_n = b_n] \leq \left(\frac{1}{2} + \varepsilon\right)^n.$$

- Как оценить  $\varepsilon$  для цепей Маркова?

---

[6] А. С. Логачев и В. О. МIRONKIN, «О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа».

# Оценка $\varepsilon$ для цепей Маркова

- Пусть известна прямоугольная таблица  $T$  (размера  $2^r \times 2$ ) переходных вероятностей цепи Маркова порядка  $r$ :

$$\mathbb{P}[X_{n+r} = b_{r+1} \mid X_n = b_1, \dots, X_{n+r-1} = b_r].$$

- Вложим  $T$  в квадратную матрицу  $P$  порядка  $2^r \times 2^r$  переходных вероятностей цепи Маркова, где на пересечении строки с двоичным номером  $(b_1, \dots, b_r)$  и столбца с двоичным номером  $(b_2, \dots, b_{r+1})$  стоит выписанная выше вероятность.
- Пусть  $\pi$  — вектор, задающий стационарное распределение цепи Маркова, определенной с помощью матрицы переходных вероятностей  $P$ . Обозначим через  $\pi_{min}$ ,  $\pi_{max}$ : минимальный и максимальный элементы вектора  $\pi$ ;  
 $p_{min}$ ,  $p_{max}$ : минимальный и максимальный элементы таблицы  $T$ .

# Оценка величины $\varepsilon$

- Для вероятностей  $\mathbb{P}[X_1 = b_1, \dots, X_n = b_n]$  для каждого  $n \in \mathbb{N}$ ,  $n \geq r + 1$ , справедлива оценка

$$\pi_{min} \cdot p_{min}^{n-r} \leq \mathbb{P}[X_1 = b_1, \dots, X_n = b_n] \leq \pi_{max} \cdot p_{max}^{n-r}.$$

- Потребуем  $\left(\frac{1}{2} - \varepsilon\right)^n \leq \pi_{min} \cdot p_{min}^{n-r}$ ,  $\pi_{max} \cdot p_{max}^{n-r} \leq \left(\frac{1}{2} + \varepsilon\right)^n$ .

- В качестве  $\varepsilon$  берем значение

$$\varepsilon = \max \left( \max_{n \in \mathbb{N}} \left( \frac{1}{2} - \pi_{min}^{1/n} \cdot p_{min}^{1-\frac{r}{n}} \right), \max_{n \in \mathbb{N}} \left( \pi_{max}^{1/n} \cdot p_{max}^{1-\frac{r}{n}} - \frac{1}{2} \right) \right).$$

# Оценка величины $\varepsilon$

- Мы не знаем точных вероятностей перехода; они оцениваются из данных.
- В качестве оценок переходных вероятностей берем частотные оценки (ОМП):

$$\hat{p}_i = \frac{\sum_{t=1}^{N-r-1} \mathbb{I}[X_t = i_1, X_{t+1} = i_2, \dots, X_{t+r} = i_r, X_{t+r+1} = 1]}{\sum_{t=1}^{N-r-1} \mathbb{I}[X_t = i_1, X_{t+1} = i_2, \dots, X_{t+r} = i_r]},$$

$$\text{bitstr}_r(i) = (i_1, \dots, i_r).$$

- Многомерная Центральная предельная теорема дает нормальность распределения вектора

$$\hat{\mathbf{p}}_n = (\hat{p}_1, \dots, \hat{p}_{2^r}).$$

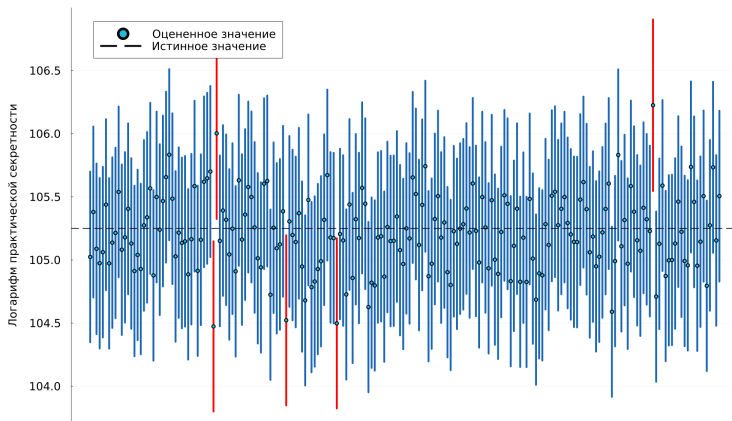
- Многомерный дельта-метод дает нормальность распределения  $T(\hat{\varepsilon})$ , поскольку  $\hat{\varepsilon}$  — функция от  $(p_1, \dots, p_{2^r})$ , а  $T$  — функция от  $\hat{\varepsilon}$ .

# Асимптотически нормальная оценка

- Для практической секретности в условиях справедливости базовой статистической модели (марковская цепь порядка  $r$ ) получен ДИ

$$\left( T(\hat{\mathbf{p}}_n) + \frac{q_{\alpha/2} \sqrt{\text{grad}T(\hat{\mathbf{p}}_n)^T \cdot \Sigma \cdot \text{grad}T(\hat{\mathbf{p}}_n)}}{\sqrt{n}}, \right. \\ \left. T(\hat{\mathbf{p}}_n) + \frac{q_{1-\alpha/2} \sqrt{\text{grad}T(\hat{\mathbf{p}}_n)^T \cdot \Sigma \cdot \text{grad}T(\hat{\mathbf{p}}_n)}}{\sqrt{n}} \right).$$

- Матрица  $\Sigma$  является диагональной:  $\Sigma = \text{diag} \left( \frac{1}{4\beta_1}, \dots, \frac{1}{4\beta_{2^r}} \right)$ .
- Частоты попадания марковской цепи в состояния  $\text{bitstr}_r(i-1)$  равны  $n_i = \beta_i \cdot n$ , где  $\beta_i$  — некоторые константы.



**Рис. 6:** Асимптотические двусторонние 95%-ные ДИ, многомерный дельта-метод; синим (красным) отмечены интервалы, (не) покрывающие истинное значение оценки логарифма практической секретности; доля интервалов, покрывших истинное значение оценки логарифма, равна  $0.977 \approx 1 - \alpha$

# Результаты работы

## Схема Бернулли

- Построены ДИ для логарифма практической секретности с помощью трех различных подходов (дельта-метод, монотонное преобразование, бутстрэп).
- Теоретические результаты проверены на синтетических данных.

## Цепи Маркова

- Цепи Маркова сведены к ранее изученной общей схеме с зависимыми двоичными знаками; предложена оценка на параметр  $\varepsilon$ .
- Построен ДИ для оценки логарифма практической секретности с помощью многомерного дельта-метода.
- Теоретический результат проверен на синтетических данных.



# Дальнейшие возможные направления исследований

- На практике сама статистическая модель не всегда специфицирована до конца — как учесть неопределенность, например, в параметре порядка марковской цепи: байесовские методы?
- Насколько велика может быть ошибка при некорректной спецификации?
- Оценка  $\varepsilon$  является излишне пессимистичной и грубой: можно ли лучше?

# Спасибо за внимание!



tsaregorodtsev@aktiv-company.ru  
sma@aktiv-company.ru



www.rutoken.ru  
www.aktiv-company.ru








+7 495 925-77-90







## РусКрипто

# Список литературы I

-  Arbekov, I. M. «Lower bounds for the practical secrecy of a key». В: *Математические вопросы криптографии* 8.2 (2017), с. 29—38.
-  Arbekov, I. M. и S. N. Molotkov. «Shannon unicity distance,  $\varepsilon$ -secrecy criterion and Holevo information in quantum cryptography». В: *Laser Physics Letters* 18.1 (2020), с. 015205.
-  Bogdanov, D. S. «On the practical secrecy of keys formed from instantaneous values of a stationary Gaussian process». В: *Proceedings of the XIV Workshop on Current Trends in Cryptology (CTCrypt 2025)*. 2025.
-  Арбеков, И. М. «Критерии секретности ключа». В: *Математические вопросы криптографии* 7.1 (2016), с. 39—56.
-  Арбеков, И. М. и С. Н. Молотков. «Различимость квантовых состояний и трудоемкость по Шеннону в квантовой криптографии». В: *Журнал экспериментальной и теоретической физики* 152.1 (2017), с. 62.

## Список литературы II

-  Дрелихов, В. О. «О практической безопасности ключа». В: *Математические вопросы криптографии* 15.4 (2024), с. 43—59.
-  Логачев, А. С. и В. О. МIRONKIN. «О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа». В: *Прикладная дискретная математика* 65 (2024), с. 66—83.
-  МIRONKIN, В. О. и М. М. Михайлов. «Об энтропии последовательной процедуры опробования дискретной вероятностной схемы». В: *Обозрение прикладной и промышленной математики* 27.1 (2020), с. 76—79.
-  Молотков, С. Н. «Одноразовый блокнот, сложность перебора ключей и практическая секретность квантовой криптографии». В: *Журнал экспериментальной и теоретической физики* 150.5 (11) (2016), с. 903—916.