Владимир Миронкин

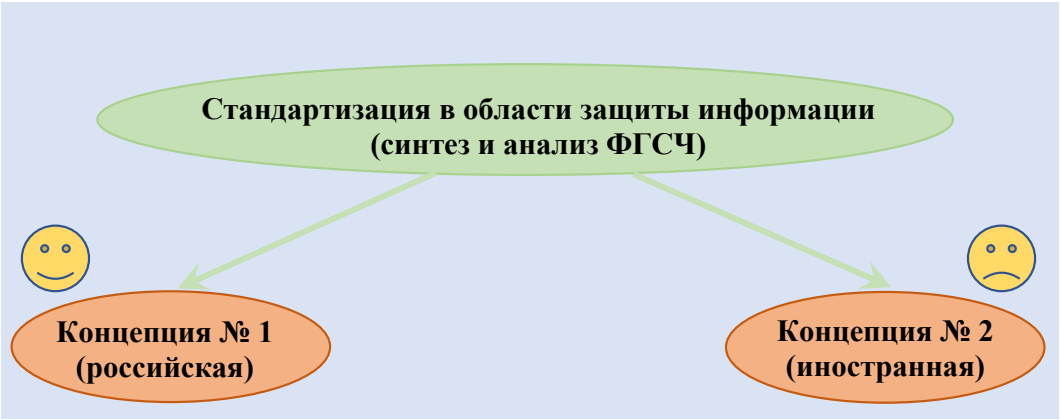
Оценка снизу энтропии Шеннона для одной теоретико-вероятностной модели источника криптографических ключей

1–5 июня 2026 года

г. Минск, Республика Беларусь

Введение

Параллельными курсами развиваются две концепции проверки криптографического качества двоичных последовательностей, формируемых с использованием ФГСЧ.



Первая концепция (разрабатываемая ТК 26) основана на:

- построении и проверке теоретико-вероятностной модели (далее – ТВМ) ФГСЧ;
- классификации схемы формирования двоичных последовательностей ФГСЧ;
- оценке криптографического качества ключей, формируемых из двоичных последовательностей ФГСЧ в соответствии с заданной схемой, с использованием функционала «практическая секретность ключа».

Замечание

Имеется жесткая взаимосвязь ТВМ и характеристик ФГСЧ, зависящих от схемы[a] *формирования знаков ФГСЧ и влияющих на практическую секретность ключей*[b].

[a] Bogdanov D.S., Logachev A.S., Mironkin V.O., "Theoretical Models of Physical Random Number Generators", *Automatic Control and Computer Sciences*, **8**:58 (2024), 1303–1310.

[b] Арбеков И.М., "Критерий секретности ключа", *Матем. вопр. криптографии*, **7**:1 (2016), 39–56.

Первая концепция (разрабатываемая ТК 26) основана на:

- построении и проверке теоретико-вероятностной модели (далее – ТВМ) ФГСЧ;
- классификации схемы формирования двоичных последовательностей ФГСЧ;
- оценке криптографического качества ключей, формируемых из двоичных последовательностей ФГСЧ в соответствии с заданной схемой, с использованием функционала «практическая секретность ключа».

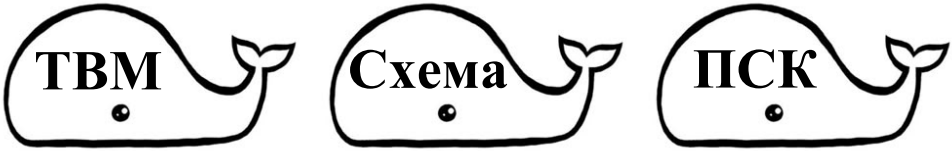
Замечание

Имеется жесткая взаимосвязь ТВМ и характеристик ФГСЧ, зависящих от схемы[a] *формирования знаков ФГСЧ и влияющих на практическую секретность ключей*[b].

[a] Bogdanov D.S., Logachev A.S., Mironkin V.O., "Theoretical Models of Physical Random Number Generators", *Automatic Control and Computer Sciences*, **8**:58 (2024), 1303–1310.

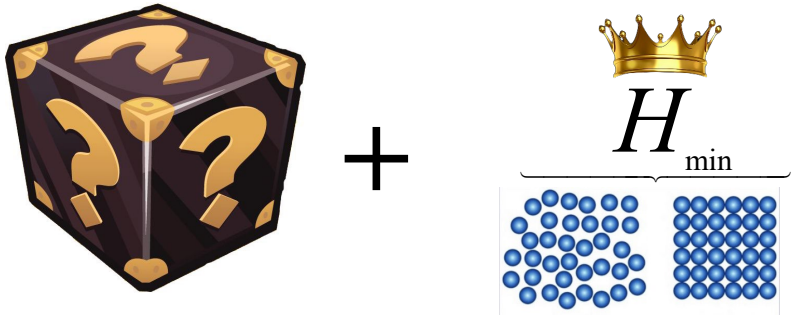
[b] Арбеков И.М., "Критерий секретности ключа", *Матем. вопр. криптографии*, **7**:1 (2016), 39–56.

Синтез и анализ ФГСЧ



Вторая концепция (NIST Special Publication 800-90B) допускает:

- рассмотрение ФГСЧ в качестве «черного ящика»;
- оценку криптографического качества ключей, формируемых из двоичных последовательностей ФГСЧ, с использованием min-энтропии.



Для второй концепции не все гладко. Есть вопросы:

1. Какую информацию о качестве ФГСЧ несет в себе оценка min-энтропии ВС, рассчитанная для конкретного выхода ФГСЧ (в том числе в модели «черного ящика»)? Не лучше ли рассматривать энтропию Шеннона дискретного источника?

---

2. Корректно ли говорить об энтропии Шеннона дискретного источника в случае нестационарности исходного случайного физического процесса?

---

3. Не занижаем ли мы искусственно реальную оценку min-энтропии, выбирая наименьшую из целой совокупности оценок, описанных в NIST SP 800-90B? Рискуем ли мы криптографически качественный ФГСЧ классифицировать неугодным?

Замечание

Наличие указанных вопросов способно существенным образом усложнить процесс синтеза и сертификации ФГСЧ.

Для второй концепции не все гладко. Есть вопросы:

1. Какую информацию о качестве ФГСЧ несет в себе оценка min-энтропии ВС, рассчитанная для конкретного выхода ФГСЧ (в том числе в модели «черного ящика»)? Не лучше ли рассматривать энтропию Шеннона дискретного источника?

---

2. Корректно ли говорить об энтропии Шеннона дискретного источника в случае нестационарности исходного случайного физического процесса?

---

3. Не занижаем ли мы искусственно реальную оценку min-энтропии, выбирая наименьшую из целой совокупности оценок, описанных в NIST SP 800-90B? Рискуем ли мы криптографически качественный ФГСЧ классифицировать неугодным?

Замечание

Наличие указанных вопросов способно существенным образом усложнить процесс синтеза и сертификации ФГСЧ.

Фундаментальная проблема!

Вопрос использования энтропии Шеннона для оценки криптографического качества двоичных последовательностей до сих пор остается открытым!

⇓⇓⇓⇓⇓⇓⇓⇓⇓⇓

Основополагающая статья Андрея Михайловича Зубкова[a].

[a] Зубков А.М., "Энтропия как характеристика качества случайных последовательностей", *Матем. вопр. криптогр.*, **12**:3 (2021), 31–48.

Особая роль ТВМ...

Будем использовать ТВМ источника криптографических ключей, приближенную к реальным условиям функционирования ФГСЧ[b] и позволившую оценить ПСК в предельном случае, наиболее благоприятном для противника и/или нарушителя.

Ее описание немного ниже!!!

[b] Серия докладов на РусКрипто'2026 (секция «Математические аспекты...ГСЧ»).

На практике используются и другие модели!

К примеру, ТВМ независимых s цепочек, подробно исследованная в работах

- ***Зубкова*** *Андрея Михайловича*,
- ***Харина*** *Юрия Семеновича*,
- ***Палухи*** *Владимира Юрьевича*,
- ***Мальцева*** *Михаила Владимировича* и др.,

в рамках которой подготовлены статьи по:

- статистической проверке сложных гипотез об s-мерном распределении вероятностей двоичных последовательностей (2024);
- проведению асимптотического анализа статистических оценок энтропии Шеннона двоичных s-грамм (2025),

позволяет описывать широкий класс генераторов и их свойства.

На практике используются и другие модели!

К примеру, ТВМ независимых s цепочек, подробно исследованная в работах

- ***Зубкова*** *Андрея Михайловича*,
- ***Харина*** *Юрия Семеновича*,
- ***Палухи*** *Владимира Юрьевича*,
- ***Мальцева*** *Михаила Владимировича* и др.,

в рамках которой подготовлены статьи по:

- **статистической проверке сложных гипотез об s-мерном распределении вероятностей двоичных последовательностей (2024)**;
- проведению асимптотического анализа статистических оценок энтропии Шеннона двоичных s-грамм (2025),

позволяет описывать широкий класс генераторов и их свойства.

На практике используются и другие модели!

К примеру, ТВМ независимых s цепочек, подробно исследованная в работах

- ***Зубкова*** *Андрея Михайловича*,
- ***Харина*** *Юрия Семеновича*,
- ***Палухи*** *Владимира Юрьевича*,
- ***Мальцева*** *Михаила Владимировича* и др.,

в рамках которой подготовлены статьи по:

- **статистической проверке сложных гипотез об s-мерном распределении вероятностей двоичных последовательностей (2024)**;
- **проведению асимптотического анализа статистических оценок энтропии Шеннона двоичных s-грамм (2025)**,

позволяет описывать широкий класс генераторов и их свойства.

На практике используются и другие модели!

К примеру, ТВМ независимых s цепочек, подробно исследованная в работах

- ***Зубкова*** *Андрея Михайловича*,
- ***Харина*** *Юрия Семеновича*,
- ***Палухи*** *Владимира Юрьевича*,
- ***Мальцева*** *Михаила Владимировича* и др.,

в рамках которой подготовлены статьи по:

- **статистической проверке сложных гипотез об s-мерном распределении вероятностей двоичных последовательностей (2024)**;
- **проведению асимптотического анализа статистических оценок энтропии Шеннона двоичных s-грамм (2025)**,

позволяет описывать широкий класс генераторов и их свойства.

Под руководством Харина Ю.С. разработаны следующие методики:

1. “Методика оценки энтропии источников случайности” (2022);
2. “Методика статистического тестирования выходных последовательностей генераторов случайных чисел” (2022).

Указанные документы являются основополагающими!

Используются испытательными лабораториями при проведении сертификационных испытаний средств криптографической защиты информации на соответствие требованиям *СТБ 34.101.27-2022 “Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности”*.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

В рамках выбранной ТВМ

1. **построим** достижимое распределение на множестве криптоключей, формируемых ФГСЧ, на котором энтропия Шеннона соответствующей ВС принимает минимальное значение;
2. **покажем**, что указанное распределение не зависит от времени формирования битов ключа и, как следствие, характеризует интегральные теоретико-информационные свойства случайного процесса, лежащего в основе ФГСЧ;
3. **сравним** полученную характеристику с min-энтропией криптоключей.

Попутно решим следующие задачи:

1. **дополним** первую концепцию еще одним криптографическим функционалом – достижимой оценкой снизу энтропии Шеннона криптоключей.
2. **исключим** избыточный расчет оценок min-энтропии, предписанный NIST Special Publication 800-90B.

Модель источника криптографических ключей

Рассмотрим невырожденный двоичный дискретный источник – вероятностное пространство $(\{0,1\}^\infty, \mathcal{F}, \mathbf{P})$, где

- $\mathcal{F}$ – наименьшая по включению σ-алгебра на $\{0,1\}^\infty$, содержащая все цилиндрические множества общего вида;
- вероятность $\mathbf{P}$ такова, что для ее конечномерных распределений $P_{t_1,t_2,\ldots,t_k}$, $1 \le t_1 < t_2 < \ldots < t_k$, $k = 1, 2 \ldots$, выполняется соотношение[a]

$$\left(\frac{1}{2} - \varepsilon\right)^k \le P_{t_1,t_2,\ldots,t_k}(x_1, x_2, \ldots, x_k) \le \left(\frac{1}{2} + \varepsilon\right)^k \tag{1}$$

для произвольных $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$, где $0 \le \varepsilon < \frac{1}{2}$.

[a] Логачев А.С., Миронкин В.О., "О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа", *ПДМ*, **8**:65 (2024), 66–83.

Замечание

Источник типа (1) *– это приближенная к реальности математическая модель ФГСЧ, формирующего «сырые» двоичные последовательности, которые в дальнейшем подвергаются детерминированному преобразованию*[a].

[a] Арбеков И.М., Молотков С.Н., “Квантовые генераторы случайных чисел, экстракция доказуемо случайных битовых последовательностей из траекторий цепи Маркова”, *Успехи физических наук*, **194**:9 (2024), 974–993.

Тогда для произвольного фиксированного $n \in \mathbb{N}$ каждая последовательность $(x_1, \ldots, x_n) \in \{0,1\}^n$ вырабатывается в соответствии с полиномиальной схемой, зависящей от вектора $\bar{t} = (t_1, t_2, \ldots, t_n)$:

$$\mathcal{A}_\varepsilon(\bar{t}) \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ p_1(\bar{t}) & p_2(\bar{t}) & \ldots & p_{2^n}(\bar{t}) \end{pmatrix}. \tag{2}$$

Замечание

Источник типа (1) *– это приближенная к реальности математическая модель ФГСЧ, формирующего «сырые» двоичные последовательности, которые в дальнейшем подвергаются детерминированному преобразованию*[a].

[a] Арбеков И.М., Молотков С.Н., "Квантовые генераторы случайных чисел, экстракция доказуемо случайных битовых последовательностей из траекторий цепи Маркова", *Успехи физических наук*, **194**:9 (2024), 974–993.

Тогда для произвольного фиксированного $n \in \mathbb{N}$ каждая последовательность $(x_1, \ldots, x_n) \in \{0,1\}^n$ вырабатывается в соответствии с полиномиальной схемой, зависящей от вектора $\bar{t} = (t_1, t_2, \ldots, t_n)$:

$$\mathcal{A}_\varepsilon\left(\bar{t}\right) \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ p_1\left(\bar{t}\right) & p_2\left(\bar{t}\right) & \ldots & p_{2^n}\left(\bar{t}\right) \end{pmatrix}. \tag{2}$$

Здесь $\omega_j \in \{0,1\}^n$, $j = 1, 2, \ldots, 2^n$, а компоненты вектора распределения $\overline{p}\left(\overline{t}\right) = \left(p_1\left(\overline{t}\right), p_2\left(\overline{t}\right), \ldots, p_{2^n}\left(\overline{t}\right)\right)$ удовлетворяют системе соотношений

$$\begin{cases} p_1\left(\overline{t}\right) + p_2\left(\overline{t}\right) + \ldots + p_{2^n}\left(\overline{t}\right) = 1, \\ 1 > p_1\left(\overline{t}\right) \geq p_2\left(\overline{t}\right) \geq \ldots \geq p_{2^n}\left(\overline{t}\right) > 0, \\ \left(\frac{1}{2} - \varepsilon\right)^n \leq p_j\left(\overline{t}\right) \leq \left(\frac{1}{2} + \varepsilon\right)^n, \ j = 1, 2, \ldots, 2^n. \end{cases} \tag{3}$$

Наша цель

Для источника вида (1) в условиях ограничений (3) построить достижимую оценку снизу для энтропии Шеннона ВС $\mathcal{A}_\varepsilon\left(\overline{t}\right)$.

Для этого сформулируем ряд вспомогательных утверждений о монотонности энтропии Шеннона ВС.

Монотонность энтропии Шеннона дискретной вероятностной схемы

Рассмотрим пространство элементарных исходов $\Omega = \{\omega_1, \ldots, \omega_{2^n}\}$, $n \in \mathbb{N}$, и заданную на нем дискретную ВС

$$\mathcal{A} \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ p_1 & p_2 & \ldots & p_{2^n} \end{pmatrix},$$

где $0 < p_i < 1$, $i = 1, \ldots, 2^n$, $\sum\limits_{i=1}^{2^n} p_i = 1$, $p_1 = \max(p_1, \ldots, p_{2^n})$, $p_{2^n} = \min(p_1, \ldots, p_{2^n})$.

Определение

Энтропией Шеннона ВС $\mathcal{A}$ называется величина

$$H(\mathcal{A}) \equiv H(p_1, \ldots, p_{2^n}) = -\sum_{i=1}^{2^n} p_i \log_2 p_i.$$

Важное свойство

Степень однородности распределения ВС напрямую связана с величиной энтропии ВС: чем равномернее распределение, тем выше значение энтропии Шеннона. Рассмотрим различные модификации ВС $\mathcal{A}$:

1. *Максимизация наибольшего значения элементов распределения ВС $\mathcal{A}$.*

Утверждение

Пусть $n \in \mathbb{N}$ и дискретная ВС $\mathcal{B}$ получена из $\mathcal{A}$ путем увеличения значения p_1:

$$\mathcal{B} \sim \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_{2^n} \\ p_1 + \Delta & p_2 - \Delta_2 & \dots & p_{2^n} - \Delta_{2^n} \end{pmatrix},$$

где $0 \le \Delta < 1 - p_1, \Delta = \sum\limits_{i=2}^{2^n} \Delta_i, 0 \le \Delta_i < p_i,\ i = 2, \dots, 2^n$.

Тогда $H(\mathcal{B}) \le H(\mathcal{A})$.

Важное свойство

Степень однородности распределения ВС напрямую связана с величиной энтропии ВС: чем равномернее распределение, тем выше значение энтропии Шеннона. Рассмотрим различные модификации ВС $\mathcal{A}$:

1. ***Максимизация наибольшего значения элементов распределения ВС $\mathcal{A}$.***

Утверждение

Пусть $n \in \mathbb{N}$ и дискретная ВС $\mathcal{B}$ получена из $\mathcal{A}$ путем увеличения значения p_1:

$$\mathcal{B} \sim \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_{2^n} \\ p_1 + \Delta & p_2 - \Delta_2 & \dots & p_{2^n} - \Delta_{2^n} \end{pmatrix},$$

где $0 \le \Delta < 1 - p_1, \Delta = \sum\limits_{i=2}^{2^n} \Delta_i, 0 \le \Delta_i < p_i,\ i = 2, \dots, 2^n.$

Тогда $H(\mathcal{B}) \le H(\mathcal{A})$.

Таким образом, для распределений вида (3) имеет место неравенство

$$H\left(p_1\left(\bar{t}\right), p_2\left(\bar{t}\right), \ldots, p_{2^n}\left(\bar{t}\right)\right) \geq H\left(\left(\frac{1}{2}+\varepsilon\right)^n, \widetilde{p}_2\left(\bar{t}\right), \ldots, \widetilde{p}_{2^n}\left(\bar{t}\right)\right),$$

где $\left(\frac{1}{2}-\varepsilon\right)^n \leq \widetilde{p}_i\left(\bar{t}\right) \leq p_i\left(\bar{t}\right)$, $i = 2, \ldots, 2^n$, и $\sum\limits_{i=2}^{2^n} \widetilde{p}_i\left(\bar{t}\right) = 1 - \left(\frac{1}{2}+\varepsilon\right)^n$.

2. *Минимизация наименьшего значения элементов распределения ВС $\mathcal{A}$.*

Утверждение

Пусть $n \in \mathbb{N}$ и дискретная ВС $\mathcal{B}$ получена из $\mathcal{A}$ путем уменьшения значения p_{2^n}:

$$\mathcal{B} \sim \begin{pmatrix} \omega_1 & \ldots & \omega_{2^n-1} & \omega_{2^n} \\ p_1+\Delta_1 & \ldots & p_{2^n-1}+\Delta_{2^n-1} & p_{2^n}-\Delta \end{pmatrix},$$

где $0 \leq \Delta < p_{2^n}, \Delta = \sum\limits_{i=1}^{2^n-1} \Delta_i, 0 \leq \Delta_i < 1-p_i$, $i = 1, \ldots, 2^n-1$.

Тогда $H(\mathcal{B}) \leq H(\mathcal{A})$.

Таким образом, для распределений вида (3) имеет место неравенство

$$H\left(p_1\left(\bar{t}\right), p_2\left(\bar{t}\right), \ldots, p_{2^n}\left(\bar{t}\right)\right) \geq H\left(\left(\frac{1}{2}+\varepsilon\right)^n, \widetilde{p}_2\left(\bar{t}\right), \ldots, \widetilde{p}_{2^n}\left(\bar{t}\right)\right),$$

где $\left(\frac{1}{2}-\varepsilon\right)^n \leq \widetilde{p}_i\left(\bar{t}\right) \leq p_i\left(\bar{t}\right)$, $i=2,\ldots,2^n$, и $\sum\limits_{i=2}^{2^n} \widetilde{p}_i\left(\bar{t}\right) = 1-\left(\frac{1}{2}+\varepsilon\right)^n$.

❷ ***Минимизация наименьшего значения элементов распределения ВС $\mathcal{A}$.***

Утверждение

Пусть $n \in \mathbb{N}$ и дискретная ВС $\mathcal{B}$ получена из $\mathcal{A}$ путем уменьшения значения p_{2^n}:

$$\mathcal{B} \sim \begin{pmatrix} \omega_1 & \ldots & \omega_{2^n-1} & \omega_{2^n} \\ p_1+\Delta_1 & \ldots & p_{2^n-1}+\Delta_{2^n-1} & p_{2^n}-\Delta \end{pmatrix},$$

где $0 \leq \Delta < p_{2^n}, \Delta = \sum\limits_{i=1}^{2^n-1} \Delta_i, 0 \leq \Delta_i < 1-p_i$, $i=1,\ldots,2^n-1$.

Тогда $H(\mathcal{B}) \leq H(\mathcal{A})$.

Из последнего утверждения для распределений вида (3) следует неравенство

$$H\left(p_1\left(\bar{t}\right),\ldots,p_{2^n-1}\left(\bar{t}\right),p_{2^n}\left(\bar{t}\right)\right)\geq H\left(\widetilde{p}_1\left(\bar{t}\right),\ldots,\widetilde{p}_{2^n-1}\left(\bar{t}\right),\left(\frac{1}{2}-\varepsilon\right)^n\right),$$

где $p_i\left(\bar{t}\right)\leq\widetilde{p}_i\left(\bar{t}\right)\leq\left(\frac{1}{2}+\varepsilon\right)^n$, $i=1,\ldots,2^n-1$, и $\sum\limits_{i=1}^{2^n-1}\widetilde{p}_i\left(\bar{t}\right)=1-\left(\frac{1}{2}-\varepsilon\right)^n$.

Далее рассмотрим удовлетворяющую (3) дискретную ВС

$$\mathcal{A}\sim\begin{pmatrix}\omega_1 & \ldots & \omega_a & \omega_{a+1} & \ldots & \omega_{b-1} & \omega_b & \ldots & \omega_{2^n}\\ \left(\frac{1}{2}+\varepsilon\right)^n & \ldots & \left(\frac{1}{2}+\varepsilon\right)^n & p_{a+1} & \ldots & p_{b-1} & \left(\frac{1}{2}-\varepsilon\right)^n & \ldots & \left(\frac{1}{2}-\varepsilon\right)^n\end{pmatrix},$$

где $a,b\in\mathbb{N}$, $1\leq a<b\leq 2^n$, и $p_{a+1}\geq\ldots\geq p_{b-1}$ такие, что

$$\left(\frac{1}{2}-\varepsilon\right)^n\leq p_i\leq\left(\frac{1}{2}+\varepsilon\right)^n,\ i=a+1,\ldots,b-1,$$

$$\sum_{i=a+1}^{b-1}p_i=1-a\left(\frac{1}{2}+\varepsilon\right)^n-b\left(\frac{1}{2}-\varepsilon\right)^n.$$

❸ ***Минимизация и максимизация неэкстремальных значений элементов распределения BC $\mathcal{A}$.***

Утверждение

Пусть $n \in \mathbb{N}$ и дискретная BC $\mathcal{B}$ получена из $\mathcal{A}$ путем

- *увеличения p_{a+1} на Δ, $0 \le \Delta \le \left(\frac{1}{2}+\varepsilon\right)^n - p_{a+1}$, за счет уменьшения $p_{a+2}, \dots, p_{b-1}$:*

$$\Delta = \sum_{i=a+2}^{b-1} \Delta_i,\ 0 \le \Delta_i \le p_i - \left(\frac{1}{2}-\varepsilon\right)^n,\ i = a+2, \dots, b-1.$$

- *уменьшения p_{b-1} на Δ, $0 \le \Delta \le p_{b-1} - \left(\frac{1}{2}-\varepsilon\right)^n$, за счет увеличения $p_{a+1}, \dots, p_{b-2}$:*

$$\Delta = \sum_{i=a+1}^{b-2} \Delta_i,\ 0 \le \Delta_i \le \left(\frac{1}{2}+\varepsilon\right)^n - p_i,\ i = a+2, \dots, b-1.$$

Тогда $H(\mathcal{B}) \le H(\mathcal{A})$.

Из приведенных утверждений следует, что конечномерное распределение типа (3), минимизирующее значение энтропии Шеннона ВС (12), имеет следующий вид:

$$\hat{p}_1\left(\bar{t}\right) = \ldots = \hat{p}_s\left(\bar{t}\right) = \left(\frac{1}{2}+\varepsilon\right)^n,$$

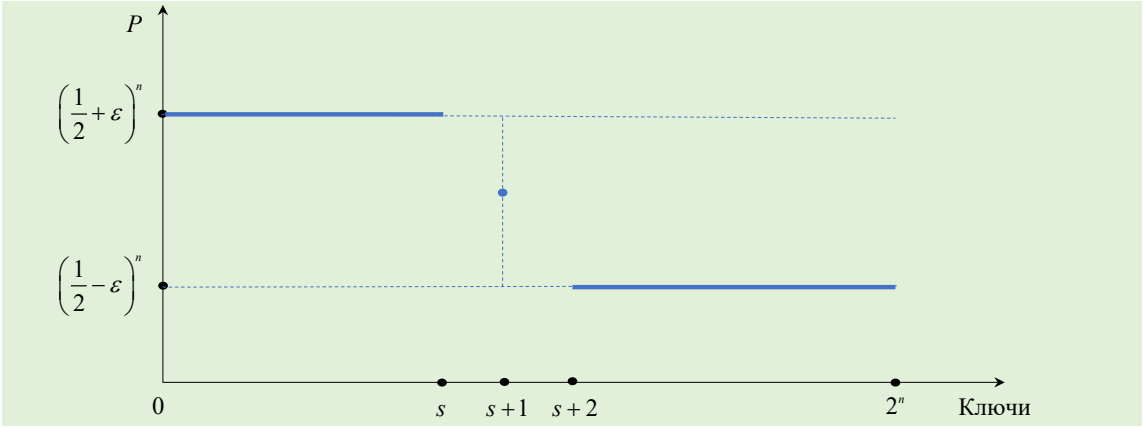
$$\hat{p}_{s+2}\left(\bar{t}\right) = \ldots = \hat{p}_{2^n}\left(\bar{t}\right) = \left(\frac{1}{2}-\varepsilon\right)^n, \tag{4}$$

$$\hat{p}_{s+1}\left(\bar{t}\right) = 1 - \sum_{j=1}^{s}\hat{p}_i\left(\bar{t}\right) - \sum_{j=s+2}^{2^n}\hat{p}_i = 1 - s\left(\frac{1}{2}+\varepsilon\right)^n - \left(2^n - s - 1\right)\left(\frac{1}{2}-\varepsilon\right)^n > 0,$$

где

$$s = s_n\left(\varepsilon\right) \equiv \begin{cases} \left[2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}\right], & 0 < \varepsilon < \frac{1}{2}, \\ 2^n, & \varepsilon = 0. \end{cases}$$

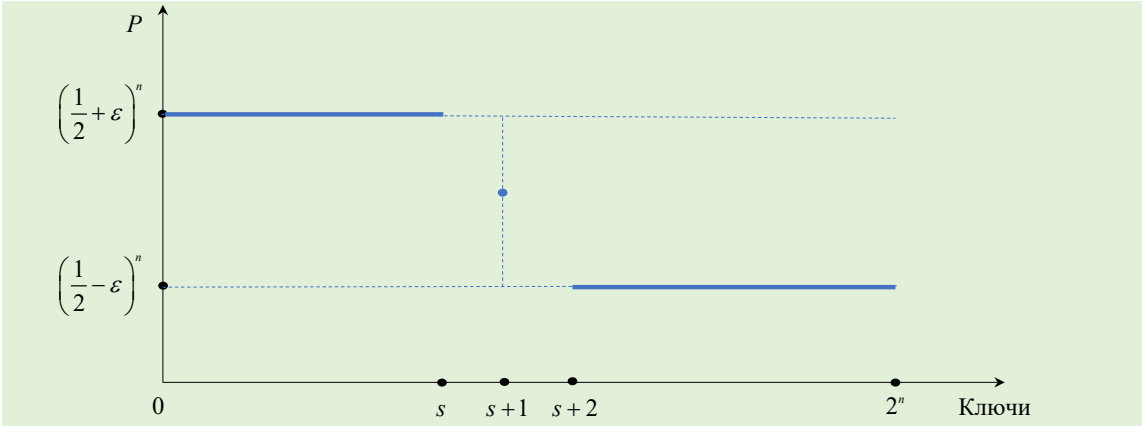
Схематично распределение (4) можно представить так:



Практически значимый факт

Не зависящее от времени распределение (4) в точности совпадает конечномерным распределением типа (3), минимизирующим ПСК.

Схематично распределение (4) можно представить так:



Практически значимый факт

Не зависящее от времени распределение (4) в точности совпадает конечномерным распределением типа (3), минимизирующим ПСК.

Он позволяет

Установить взаимосвязь между энтропией Шеннона и ПСК в рамках оценивания криптографического качества ключей!

Рассмотрим непрерывную на интервале $\left(0; \frac{1}{2}\right)$ функцию

$$r_n(\varepsilon) = \begin{cases} 2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}, & 0 < \varepsilon < \frac{1}{2}, \\ 2^n, & \varepsilon = 0. \end{cases} \tag{5}$$

Утверждение

Пусть $n \in \mathbb{N}$. Тогда функция $r_n(\varepsilon)$, принимающая значения из множества $\left(1; 2^{n-1}\right) \cup \{2^n\}$, монотонно убывает по $\varepsilon \in \left[0; \frac{1}{2}\right)$.

Следствие

Распределение (4) стремится к вырожденному с ростом $\varepsilon \in [0; \frac{1}{2})$. Таким образом, энтропия Шеннона распределения (4) монотонно убывает, достигая нуля в пределе.

Он позволяет

Установить взаимосвязь между энтропией Шеннона и ПСК в рамках оценивания криптографического качества ключей!

Рассмотрим непрерывную на интервале $\left(0; \frac{1}{2}\right)$ функцию

$$r_n(\varepsilon) = \begin{cases} 2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}, & 0 < \varepsilon < \frac{1}{2}, \\ 2^n, & \varepsilon = 0. \end{cases} \tag{5}$$

Утверждение

Пусть $n \in \mathbb{N}$. Тогда функция $r_n(\varepsilon)$, принимающая значения из множества $\left(1; 2^{n-1}\right) \cup \{2^n\}$, монотонно убывает по $\varepsilon \in \left[0; \frac{1}{2}\right)$.

Следствие

Распределение (4) стремится к вырожденному с ростом $\varepsilon \in [0; \frac{1}{2})$. Таким образом, энтропия Шеннона распределения (4) монотонно убывает, достигая нуля в пределе.

Он позволяет

Установить взаимосвязь между энтропией Шеннона и ПСК в рамках оценивания криптографического качества ключей!

Рассмотрим непрерывную на интервале $\left(0; \frac{1}{2}\right)$ функцию

$$r_n(\varepsilon) = \begin{cases} 2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n-(1-2\varepsilon)^n}, & 0 < \varepsilon < \frac{1}{2}, \\ 2^n, & \varepsilon = 0. \end{cases} \tag{5}$$

Утверждение

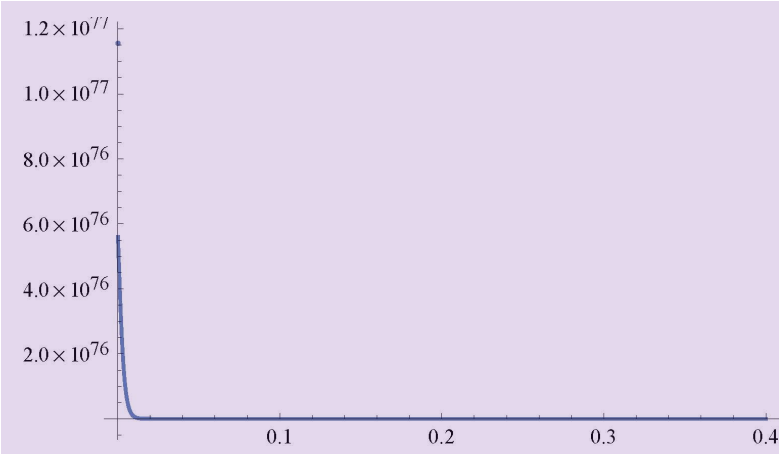
Пусть $n \in \mathbb{N}$. *Тогда функция* $r_n(\varepsilon)$, *принимающая значения из множества* $\left(1; 2^{n-1}\right) \cup \{2^n\}$, *монотонно убывает по* $\varepsilon \in \left[0; \frac{1}{2}\right)$.

Следствие

Распределение (4) *стремится к вырожденному с ростом* $\varepsilon \in [0; \frac{1}{2})$. *Таким образом, энтропия Шеннона распределения* (4) *монотонно убывает, достигая нуля в пределе.*

В качестве примера проиллюстрируем характер зависимости функций $r_n(\varepsilon)$ и $s_n(\varepsilon)$ от $\varepsilon \in \left[0; \frac{1}{2}\right)$ при $n = 4$.

На рис. ниже представлен график $s_n(\varepsilon)$ при типичном значении размера ключа $n = 256$.



<> Теперь мы можем перейти к изложению основного результата статьи! <>

Достижимая оценка снизу энтропии Шеннона

Обозначение

$\mathcal{B}_\varepsilon$ – дискретная ВС с распределением (4), соответствующим предельному случаю, наиболее благоприятному для противника и/или нарушителя.

Для произвольных $n \in \mathbb{N}$ и ε, $0 \leq \varepsilon < \frac{1}{2}$, определим величину

$$\mathcal{H}_n(\varepsilon) \equiv \min_{\bar{t}} \left(\min_{p_1(\bar{t}),\ldots,p_{2^n}(\bar{t})} \left(H\left(p_1\left(\bar{t}\right), \ldots, p_{2^n}\left(\bar{t}\right)\right)\right)\right),$$

- $\bar{t} = (t_1, t_2, \ldots, t_n)$ такие, что $1 \leq t_1 < t_2 < \ldots < t_n$;
- $\left(p_1\left(\bar{t}\right), p_2\left(\bar{t}\right), \ldots, p_{2^n}\left(\bar{t}\right)\right)$ – векторы, удовлетворяющие (3).

По построению

$$\mathcal{H}_n(\varepsilon) = H(\mathcal{B}_\varepsilon).$$

Теорема

Для произвольных $n \in \mathbb{N}$ *и* ε, $0 \leq \varepsilon < \frac{1}{2}$, *справедливы равенства:*

- *если* $r_n(\varepsilon) = k \in \{2, \ldots, 2^{n-1}\} \cup \{2^n\}$, *то*

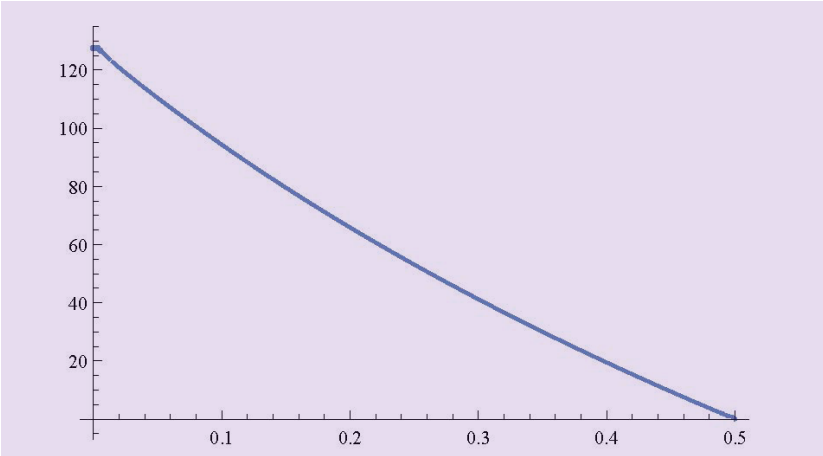
$$\mathcal{H}_n(\varepsilon) = -kn \left(\frac{1}{2} + \varepsilon\right)^n \log_2 \left(\frac{1}{2} + \varepsilon\right) - (2^n - k)\, n \left(\frac{1}{2} - \varepsilon\right)^n \log_2 \left(\frac{1}{2} - \varepsilon\right), \qquad (6)$$

- *если* $r_n(\varepsilon) \notin \{2, \ldots, 2^{n-1}\} \cup \{2^n\}$, *то*

$$\mathcal{H}_n(\varepsilon) = -s \left(\frac{1}{2} + \varepsilon\right)^n \log_2 \left(\frac{1}{2} + \varepsilon\right)^n - \hat{p}_{s+1} \cdot \log_2 \hat{p}_{s+1} - \\ - (2^n - s - 1) \left(\frac{1}{2} - \varepsilon\right)^n \log_2 \left(\frac{1}{2} - \varepsilon\right)^n, \qquad (7)$$

где $r_n(\varepsilon) = 2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}$, $s = [r_n(\varepsilon)]$.

Для функционала $\mathcal{H}_n(\varepsilon)$ имеет место монотонное убывание с ростом $\varepsilon \in \left[0; \frac{1}{2}\right)$. На рис. ниже приведена зависимость $\mathcal{H}_n(\varepsilon)$ от ε при $n = 128$.



Сравнение оценки снизу энтропии Шеннона с *min*-энтропией криптографических ключей

Определение

Пусть на $\Omega = \{\omega_1, \ldots, \omega_{2^n}\}$, $n \in \mathbb{N}$, *задана дискретная ВС*

$$\mathcal{A} \sim \begin{pmatrix} \omega_1 & \omega_2 & \ldots & \omega_{2^n} \\ p_1 & p_2 & \ldots & p_{2^n} \end{pmatrix},$$

где $0 < p_i < 1$, $i = 1, \ldots, 2^n$, $\sum\limits_{i=1}^{2^n} p_i = 1$. *Тогда минимальной энтропией (или min-энтропией) ВС* $\mathcal{A}$ *называется величина*

$$H_{min}(\mathcal{A}) = -\log_2 \max(p_1, \ldots, p_{2^n}).$$

Из равенства $\mathcal{H}_n(\varepsilon) = H(\mathcal{B}_\varepsilon)$ вытекает соотношение

$$H_{min}(\mathcal{B}_\varepsilon) \leq \mathcal{H}_n(\varepsilon).$$

Оценим фактическую близость величин $\mathcal{H}_n(\varepsilon)$ и $H_{min}(\mathcal{B}_\varepsilon)$ при всех допустимых ε:

$$\Delta_\varepsilon = \mathcal{H}_n(\varepsilon) - H_{min}(\mathcal{B}_\varepsilon).$$

Следствие

Для произвольных $n \in \mathbb{N}$ и ε, $0 \le \varepsilon < \frac{1}{2}$, справедливы неравенства:

- *если $r_n(\varepsilon) = k \in \{2, \dots, 2^{n-1}\} \cup \{2^n\}$, то*

$$\frac{4\varepsilon n\,(2^n - k)}{\ln 2}\left(\frac{1}{2} - \varepsilon\right)^n \le \Delta_\varepsilon \le \frac{4\varepsilon n\,(2^n - k)}{(1 - 4\varepsilon^2)\ln 2}\left(\frac{1}{2} - \varepsilon\right)^n,$$

- *если $r_n(\varepsilon) \notin \{2, \dots, 2^{n-1}\} \cup \{2^n\}$, то*

$$\frac{4\varepsilon n\,(2^n - s - 1)}{\ln 2}\left(\frac{1}{2} - \varepsilon\right)^n \le \Delta_\varepsilon \le \frac{4\varepsilon n}{(1 - 4\varepsilon^2)\ln 2}\left(1 - s\left(\frac{1}{2} + \varepsilon\right)^n\right),$$

где $r_n(\varepsilon) = 2^n \frac{1-(1-2\varepsilon)^n}{(1+2\varepsilon)^n - (1-2\varepsilon)^n}$, $s = [r_n(\varepsilon)]$.

Замечание

Результат следствия позволяет сделать вывод о возможности использования min-энтропии (вместо величины $\mathcal{H}_n(\varepsilon)$) в рамках анализа криптографического качества ключей, формируемых источником (1).

В качестве примера приведем значения $\mathcal{H}_n(\varepsilon)$ и $H_{min}(\mathcal{B}_\varepsilon)$ для некоторых типичных параметров ε и n.

Оценка энтропии	ε							
	10^{-4}	$5 \cdot 10^{-4}$	10^{-3}	$5 \cdot 10^{-3}$	10^{-2}	$5 \cdot 10^{-2}$	10^{-1}	$4 \cdot 10^{-1}$
$n = 56$ (DES)								
$\mathcal{H}_n(\varepsilon)$	55.999	55.998	55.991	55.780	55.182	48.344	41.270	8.513
$H_{min}(\mathcal{B}_\varepsilon)$	55.984	55.919	55.839	55.196	54.400	48.300	41.270	8.512
$n = 112$ (3DES)								
$\mathcal{H}_n(\varepsilon)$	112.0	111.991	111.964	111.181	109.407	96.600	82.540	17.024
$H_{min}(\mathcal{B}_\varepsilon)$	111.968	111.838	111.677	110.392	108.800	96.600	82.540	17.024

Замечание

Результат следствия позволяет сделать вывод о возможности использования min-энтропии (вместо величины $\mathcal{H}_n(\varepsilon)$) в рамках анализа криптографического качества ключей, формируемых источником (1).

В качестве примера приведем значения $\mathcal{H}_n(\varepsilon)$ и $H_{min}(\mathcal{B}_\varepsilon)$ для некоторых типичных параметров ε и n.

Оценка энтропии	ε							
	10^{-4}	$5\cdot10^{-4}$	10^{-3}	$5\cdot10^{-3}$	10^{-2}	$5\cdot10^{-2}$	10^{-1}	$4\cdot10^{-1}$
$n = 56$ (DES)								
$\mathcal{H}_n(\varepsilon)$	55.999	55.998	55.991	55.780	55.182	48.344	41.270	8.513
$H_{min}(\mathcal{B}_\varepsilon)$	55.984	55.919	55.839	55.196	54.400	48.300	41.270	8.512
$n = 112$ (3DES)								
$\mathcal{H}_n(\varepsilon)$	112.0	111.991	111.964	111.181	109.407	96.600	82.540	17.024
$H_{min}(\mathcal{B}_\varepsilon)$	111.968	111.838	111.677	110.392	108.800	96.600	82.540	17.024

Оценка энтропии	ε							
	10^{-4}	$5 \cdot 10^{-4}$	10^{-3}	$5 \cdot 10^{-3}$	10^{-2}	$5 \cdot 10^{-2}$	10^{-1}	$4 \cdot 10^{-1}$
$n = 128$ (AES, DEAL, KASUMI, Present, SEED, Speck)								
$\mathcal{H}_n(\varepsilon)$	128.0	127.988	127.953	126.959	124.859	110.400	94.332	19.456
$H_{min}(\mathcal{B}_\varepsilon)$	127.963	127.815	127.631	126.163	124.343	110.400	94.332	19.456
$n = 168$ (3DES)								
$\mathcal{H}_n(\varepsilon)$	167.999	167.980	167.919	166.342	163.515	144.899	123.810	25.537
$H_{min}(\mathcal{B}_\varepsilon)$	167.952	167.758	167.516	165.588	163.200	144.899	123.810	25.537
$n = 192$ (AES, DEAL, Speck)								
$\mathcal{H}_n(\varepsilon)$	191.999	191.973	191.895	189.944	186.739	165.599	141.497	29.185
$H_{min}(\mathcal{B}_\varepsilon)$	191.945	191.723	191.447	189.244	186.515	165.599	141.497	29.185
$n = 256$ («Кузнечик», «Магма», AES, DEAL, Speck, Threefish)								
$\mathcal{H}_n(\varepsilon)$	255.998	255.953	255.815	252.848	248.770	220.799	188.663	38.913
$H_{min}(\mathcal{B}_\varepsilon)$	255.926	255.631	255.262	252.325	248.686	220.799	188.663	38.913

Спасибо за внимание!