О практической секретности ключей, формируемых по схеме выбросов процесса восстановления

Богданов Д.С.

МГУ им. М.В. Ломоносова

CTCrypt 2026, г. Минск, Республика Беларусь

Физические генераторы случайных чисел

ФГСЧ используют случайность, возникающую в физических процессах.

Примеры источников:

- лавинный шум;
- тепловой шум;
- квантовые эффекты;
- другие случайные физические процессы.

Проблема

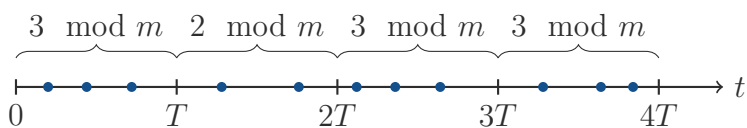
Выходные биты ФГСЧ на практике могут быть зависимыми и не вполне равновероятными.

Схема выбросов

На каждом интервале длины T подсчитывается число случайных событий.

Выходной символ:

$$\gamma_k = \left(X_{kT} - X_{(k-1)T}\right) \mod m, \qquad k \in \mathbb{N}.$$



Процесс восстановления

Пусть $\xi_1, \xi_2, \ldots$ — независимые одинаково распределённые неотрицательные случайные величины с распределением F.

Моменты восстановлений:

$$S_n = \xi_1 + \ldots + \xi_n.$$

Число восстановлений к моменту t:

$$X_t = \sup\{n : S_n \leq t\}.$$

Используются также:

- $U_t = t - S_{X_t}$ — возраст процесса в момент t (недоскок);
- $V_t = S_{X_t+1} - t$ — остаточное время до следующего восстановления (перескок).

Пример: подсчёт фотонов

Пусть источник испускает фотоны в случайные моменты времени.

Если ξ_n — время между испусканием $(n-1)$-го и n-го фотона, то

$$X_t = \sup\{n : S_n \le t\}$$

есть число испущенных фотонов к моменту t.

При регистрации числа фотонов на интервалах длины T:

$$\gamma_k = \left(X_{kT} - X_{(k-1)T}\right) \mod 2.$$

Это частный случай схемы выбросов при $m = 2$.

Пример основан на: Furst M., Weier H., Nauerth S. et al. High speed optical quantum random number generation // OPTICS EXPRESS, 2010, Vol. 18, No. 12, pp. 13029–13037.

Что нужно оценивать

Для криптографических приложений важно понимать, насколько распределение ключа близко к идеальной модели.

Идеальная модель:

$$\text{независимые равновероятные символы} \quad \{0, 1, \ldots, m-1\}.$$

В работе рассматривается параметр отклонения ε, связанный с **практической секретностью ключа**.

Практическая секретность ключа

Определение (по И. М. Арбекову)

Практическая секретность ключа — это среднее число опробований, которое необходимо совершить злоумышленнику для нахождения истинного ключа.

Связь с параметром ε

В работах Логачёва и Миронкина (2024) показано, что практическая секретность ключа **однозначно определяется** параметром ε.

Источники: Арбеков И. М. Критерии секретности ключа // Матем. вопр. криптогр., 2016; Логачёв А. С., Миронкин В. О. О влиянии вероятностных характеристик... // ПДМ, 2024.

Отклонение от равномерной модели

Пусть $\gamma_1, \gamma_2, \ldots$ принимают значения в $\{0, 1, \ldots, m-1\}$.

Будем говорить, что отклонение не превосходит ε, если для любых $k \geq 1$, попарно различных индексов $n_1, \ldots, n_k$ и любых $x_i \in \{0, \ldots, m-1\}$ выполнено

$$\left(\frac{1}{m} - \varepsilon\right)^k \leq \mathbf{P}(\gamma_{n_1} = x_1, \ldots, \gamma_{n_k} = x_k) \leq \left(\frac{1}{m} + \varepsilon\right)^k.$$

Смысл

Чем меньше ε, тем ближе источник к модели независимых равномерных символов.

Достаточное условие: идея

Вместо совместных вероятностей удобно контролировать условные вероятности.

Достаточно получить оценку вида

$$\left| \mathbf{P}(\gamma_{t_1} = x_1 \mid \gamma_{t_2} = x_2, \ldots, \gamma_{t_k} = x_k) - \frac{1}{m} \right| \leq \varepsilon.$$

Тогда условие на совместные вероятности получается последовательным разложением:

$$\mathbf{P}(A_1 \cap \ldots \cap A_k) = \prod_{j=1}^{k} \mathbf{P}(A_j \mid A_1, \ldots, A_{j-1}).$$

Условные вероятности как случайные величины

Рассматриваем условную вероятность относительно σ-алгебры:

$$\mathbf{P}(\gamma_{t_1} = x_1 \mid \gamma_{t_2}, \ldots, \gamma_{t_k}).$$

Формально:

$$\mathbf{P}(\gamma_{t_1} = x_1 \mid \gamma_{t_2}, \ldots, \gamma_{t_k}) = \mathbf{E}\left(\mathbb{I}_{\{\gamma_{t_1} = x_1\}} \mid \sigma(\gamma_{t_2}, \ldots, \gamma_{t_k})\right).$$

Для оценки таких величин используется

$$\operatorname{ess\,sup} \left| \mathbf{P}(\gamma_{t_1} = x_1 \mid \gamma_{t_2}, \ldots, \gamma_{t_k}) - \frac{1}{m} \right|.$$

Монотонность по информации

Используется стандартный факт.

Пусть

$$\mathscr{B}_2 \subseteq \mathscr{B}_1 \subseteq \mathscr{F}.$$

Тогда

$$\operatorname{ess\,sup} \mathbf{E}(\xi \mid \mathscr{B}_2) \leq \operatorname{ess\,sup} \mathbf{E}(\xi \mid \mathscr{B}_1).$$

Интерпретация

Если дать противнику дополнительную информацию, то практическая секретность не может стать лучше.

Как используется монотонность

Для фиксированных n и r:

$$\operatorname{ess\,sup} \left| \mathbf{P}(\gamma_n = r \mid \gamma_{t_1}, \ldots, \gamma_{t_k}) - \frac{1}{m} \right|$$
$$\leq \operatorname{ess\,sup} \left| \mathbf{P}(\gamma_n = r \mid \gamma_{n+1}, \gamma_{n-1}, \gamma_{n+2}, \ldots) - \frac{1}{m} \right|.$$

То есть достаточно оценить условную вероятность при условии, что известны все остальные символы последовательности.

Далее это условие заменяется более удобной информацией о процессе восстановления.

Ключевое сведение

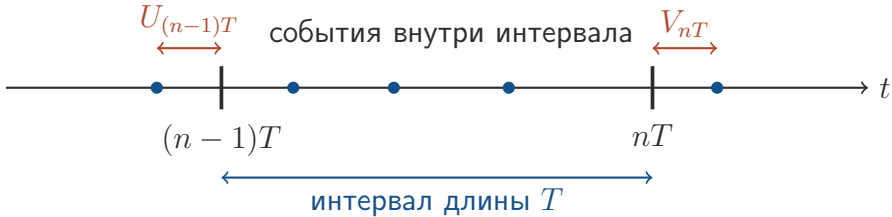
Для схемы выбросов получается оценка:

$$\sup_n \max_r \operatorname{ess\,sup} \left| \mathbf{P}(\gamma_n = r \mid \gamma_{n+1}, \gamma_{n-1}, \ldots) - \frac{1}{m} \right|$$
$$\leq \sup_n \max_r \operatorname{ess\,sup} \left| \mathbf{P}(\gamma_n = r \mid U_{(n-1)T}, V_{nT}) - \frac{1}{m} \right|.$$

Смысл

Для оценки достаточно знать недоскок в начале интервала и перескок в конце интервала.

Геометрия процесса



Значение γ_n определяется числом событий внутри выделенного интервала.

Вспомогательный процесс

При фиксированных значениях

$$U_{(n-1)T} = x, \qquad V_{nT} = y$$

вводится вспомогательный процесс восстановления $N_t^{(x,y)}$.

Обозначим

$$p_r^{(x,y)}(T) = \mathbf{P}\{N_T^{(x,y)} \equiv r \mod m\}.$$

Тогда исходная задача сводится к оценке

$$\max_{0 \le r \le m-1} \sup_{x,y} \left| p_r^{(x,y)}(T) - \frac{1}{m} \right|.$$

Что произошло со сложной зависимостью

Изначально нужно было контролировать условные вероятности вида

$$\mathbf{P}(\gamma_n = r \mid \gamma_{n+1}, \gamma_{n-1}, \ldots).$$

После сведения нужно изучить только

$$\mathbf{P}\{N_T^{(x,y)} \equiv r \mod m\}.$$

Итог

Криптографическая задача превращается в задачу теории восстановления: исследовать число событий на интервале длины T при фиксированных граничных временах.

Предельный результат

Рассматриваем

$$p_r^{(x,y)}(T) = \mathbf{P}\{N_T^{(x,y)} \equiv r \mod m\}.$$

Теорема

Если время между восстановлениями имеет конечное среднее

$$\mathbf{E}\xi = \mu < \infty,$$

то для фиксированных x, y и любого r

$$\lim_{T\to\infty} p_r^{(x,y)}(T) = \frac{1}{m}.$$

Идея доказательства: уравнение восстановления

Вероятности $p_r^{(x,y)}(T)$ удовлетворяют уравнениям восстановления.

В общем виде:

$$p_r(T) = a_r(T) + (p_r * F^{m*})(T).$$

Здесь:

- $a_r(T)$ — известный свободный член;
- F^{m*} — распределение суммы m межсобытийных интервалов;
- $*$ — свёртка.

Появление F^{m*} связано с тем, что добавление m восстановлений не меняет остаток по модулю m.

Идея доказательства: предел

К уравнению восстановления применяется теорема восстановления.

Так как

$$\mathbf{E}(\xi_1 + \ldots + \xi_m) = m\mu,$$

предельное значение имеет вид

$$\lim_{T\to\infty} p_r(T) = \frac{1}{m\mu}\int_0^\infty a_r(t)\,dt.$$

В рассматриваемой задаче

$$\int_0^\infty a_r(t)\,dt = \mu.$$

Поэтому

$$\lim_{T\to\infty} p_r(T) = \frac{\mu}{m\mu} = \frac{1}{m}.$$

Следствие предельного результата

Для фиксированных граничных значений x, y:

$$p_r^{(x,y)}(T) \to \frac{1}{m}, \qquad T \to \infty.$$

Это означает, что при больших T распределение остатка числа восстановлений становится асимптотически равномерным.

Важно

Для оценки параметра ε требуется допредельная или равномерная по x, y оценка:

$$\sup_{x,y} \max_r \left| p_r^{(x,y)}(T) - \frac{1}{m} \right|.$$

Почему нужен допредельный анализ

Предельный результат говорит:

$$p_r^{(x,y)}(T) \to \frac{1}{m} \qquad \text{при } T \to \infty.$$

Но в приложениях T фиксировано.

Нужно оценить

$$\max_r \sup_{x,y} \left| p_r^{(x,y)}(T) - \frac{1}{m} \right|$$

для конкретного T.

Метод

Решить уравнение восстановления с помощью преобразования Лапласа.

Преобразование Лапласа

Для интегрируемой функции g:

$$\mathcal{L}\{g\}(s) = \int_0^\infty e^{-st} g(t)\, dt.$$

Два свойства, которые используются:

$$\mathcal{L}\{g_1 * g_2\}(s) = \mathcal{L}\{g_1\}(s)\mathcal{L}\{g_2\}(s),$$

$$\mathcal{L}\left\{\int_0^T g(u)\, du\right\}(s) = \frac{1}{s}\mathcal{L}\{g\}(s).$$

Именно поэтому уравнения восстановления удобно решать в образах Лапласа.

Общий вид допредельного уравнения

Для фиксированного остатка r:

$$p_r(T) = a_r(T) + (p_r * G)(T),$$

где обычно

$$G = F^{m*}.$$

После преобразования Лапласа:

$$\mathcal{L}\{p_r\}(s) = \mathcal{L}\{a_r\}(s) + \mathcal{L}\{p_r\}(s)\mathcal{L}\{G\}(s).$$

Поэтому

$$\mathcal{L}\{p_r\}(s) = \frac{\mathcal{L}\{a_r\}(s)}{1 - \mathcal{L}\{G\}(s)}.$$

Это уже алгебраическая формула.

Случай $m = 2$: обозначения

Для битов рассматриваем $m = 2$.

Интересует вероятность чётного числа восстановлений:

$$p_0^{(x,y)}(T) = \mathbf{P}\{N_T^{(x,y)} \equiv 0 \mod 2\}.$$

Обозначим:

$$\phi(s) = \mathcal{L}\{f\}(s),$$
$$\phi_1^{(x)}(s) = \mathcal{L}\{f_1^{(x)}\}(s), \qquad \phi_2^{(y)}(s) = \mathcal{L}\{f_2^{(y)}\}(s).$$

Здесь f — плотность межсобытийного интервала, а $f_1^{(x)}, f_2^{(y)}$ отвечают граничным условиям.

Случай $m = 2$: уравнение

Для $p_0^{(x,y)}(T)$ уравнение имеет вид

$$p_0^{(x,y)}(T) = a_0^{(x,y)}(T) + \left(p_0^{(x,y)} * F^{2*}\right)(T).$$

Известный свободный член:

$$\begin{aligned} a_0^{(x,y)}(T) =& 1 - F_1^{(x)}(T) + F^{2*} * F_1^{(x)}(T) - F^{2*}(T) \\ &+ F_1^{(x)} * F_2^{(y)}(T) - F_1^{(x)} * F_2^{(y)} * F(T). \end{aligned}$$

Важно

Правая часть полностью выражается через известные распределения и их свёртки.

Случай $m = 2$: образ Лапласа

После преобразования Лапласа:

$$\mathcal{L}\{p_0^{(x,y)}\}(s) = \mathcal{L}\{a_0^{(x,y)}\}(s) + \mathcal{L}\{p_0^{(x,y)}\}(s)\phi(s)^2.$$

Следовательно,

$$\mathcal{L}\{p_0^{(x,y)}\}(s) = \frac{\mathcal{L}\{a_0^{(x,y)}\}(s)}{1 - \phi(s)^2}.$$

Это основная формула для получения допредельного распределения при $m = 2$.

Случай $m = 2$: явная формула

Подставляя выражение для $a_0^{(x,y)}$, получаем:

$$\mathcal{L}\{p_0^{(x,y)}\}(s) = \frac{1}{s} \cdot \frac{1 - \phi_1^{(x)} + \phi^2 \phi_1^{(x)} - \phi^2 + \phi_1^{(x)} \phi_2^{(y)} (1 - \phi)}{1 - \phi^2}.$$

Здесь аргумент s у функций ϕ, $\phi_1^{(x)}$, $\phi_2^{(y)}$ опущен для краткости.

Дальнейший шаг

Найти обратное преобразование Лапласа и оценить

$$\left| p_0^{(x,y)}(T) - \frac{1}{2} \right|.$$

Алгоритм для конкретного распределения

Для заданного распределения межсобытийных интервалов:

1. Найти
$$\phi(s) = \mathcal{L}\{f\}(s).$$
2. Найти граничные преобразования
$$\phi_1^{(x)}(s), \qquad \phi_2^{(y)}(s).$$
3. Подставить их в формулу для $\mathcal{L}\{p_0^{(x,y)}\}(s)$.
4. Выполнить обратное преобразование:
$$p_0^{(x,y)}(T) = \mathcal{L}^{-1}\{\mathcal{L}p_0^{(x,y)}\}(T).$$

Что получается на практике

Полученная формула конструктивна.

- Если $\phi(s)$ рациональна, обратное преобразование часто находится явно.
- Если формулы слишком громоздкие, можно использовать численное обращение преобразования Лапласа.
- После этого берётся верхняя оценка по x, y.

$$\varepsilon(T) \leq \sup_{x,y} \left| p_0^{(x,y)}(T) - \frac{1}{2} \right|.$$

Проверка метода: экспоненциальный случай

Пусть

$$f(t) = \lambda e^{-\lambda t}.$$

Тогда

$$\phi(s) = \frac{\lambda}{s + \lambda}.$$

В экспоненциальном случае условные остаточные распределения совпадают с исходным:

$$\phi_1^{(x)}(s) = \phi_2^{(y)}(s) = \phi(s).$$

Подстановка в общую формулу даёт простой образ Лапласа:

$$\mathcal{L}\{p_0\}(s) = \frac{1}{2s} + \frac{1}{2(s + 2\lambda)}.$$

Экспоненциальный случай: результат

Обратное преобразование даёт

$$p_0(T) = \frac{1}{2} + \frac{1}{2}e^{-2\lambda T}.$$

Поэтому

$$\left| p_0(T) - \frac{1}{2} \right| = \frac{1}{2}e^{-2\lambda T}.$$

Следовательно, для битов:

$$\sup_n \operatorname{ess\,sup} \left| \mathbf{P}(\gamma_n = 0 \mid \gamma_{n+1}, \gamma_{n-1}, \ldots) - \frac{1}{2} \right| \leq \frac{1}{2}e^{-2\lambda T}.$$

Это простая проверка общего метода на распределении, для которого всё вычисляется явно.

Основные результаты

1. Рассмотрена схема

$$\gamma_k = (X_{kT} - X_{(k-1)T}) \mod m.$$

2. Оценка практической секретности сведена к условным вероятностям.
3. Получено сведение к задаче теории восстановления:

$$\max_r \sup_{x,y} \left| p_r^{(x,y)}(T) - \frac{1}{m} \right|.$$

4. Показано, что при $T \to \infty$

$$p_r^{(x,y)}(T) \to \frac{1}{m}.$$

5. Для конечного T предложен метод через преобразование Лапласа.

Спасибо за внимание!