

Далее рассмотрим матроиды в аффинном m -мерном пространстве M над $\text{GF}(q)$. Как известно [9], $|M| = q^m$ и $|Z| = q^{m-1}$. В аффинном пространстве может быть два случая пересечения гиперпространств Z_i и Z_j : 1) либо пересекаются, т. е. $Z_i \cap Z_j \neq \emptyset$, тогда вторая аксиома матроида выполняется, как в проективном пространстве; 2) либо параллельны, т. е. $Z_i \cap Z_j = \emptyset$, тогда это тривиальный случай и вторая аксиома матроида также выполняется, так как объединение двух соответствующих гиперпространств циклов образует всё пространство M . Первая аксиома матроида выполняется в обоих случаях, как и в проективном пространстве.

При реализации идеальной однородной совершенной СРС гиперпространства соответствуют линейным функциям. На основе обобщённых кодов Рида — Маллера получена

Теорема 1. Аффинное и проективное пространства над $\text{GF}(q)$ являются однородными матроидами с гиперпространствами в качестве антициклов.

При этом возникает естественный и сложный вопрос полного описания класса однородных СРС над $\text{GF}(q)$. Для решения этого вопроса рассмотрена возможность добавления участников СРС однородного матроида. Путём комбинаторных рассуждений доказано

Утверждение 1. Линейные однородные разделяющие СРС над $\text{GF}(q)$ сводятся к подсхемам схемы некоторого проективного пространства над $\text{GF}(q)$ с гиперпространствами в качестве антициклов.

ЛИТЕРАТУРА

1. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003.
2. *Shamir A.* How to share a secret // Comm. ACM. NY, USA: ACM, 1979. V.22. No.11. P.612–613.
3. *Черемушкин А. В.* Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика. Приложение. 2009. № 2. С. 115–150.
4. Введение в криптографию / под общ. ред. В. В. Яценко. СПб.: Питер, 2001.
5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 11(1). Research Paper 72. 16 p.
6. *Медведев Н. В., Титов С. С.* Бинарные почти пороговые матроиды // Научно-технический вестник Поволжья. 2012. № 4. С. 136–142.
7. *Медведев Н. В., Титов С. С.* Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады ТУСУРа. 2011. № 1(23). Ч. 1. С. 91–96.
8. *Блейкли Г. Р., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. 1997. Т. 33. № 3. С. 102–110.
9. *Холл М.* Комбинаторика. М.: Мир, 1970. 424 с.

УДК 519.723

О НЕМИНИМАЛЬНЫХ СОВЕРШЕННЫХ ШИФРАХ

Н. В. Медведева, С. С. Титов

Рассмотрены свойства неминимальных совершенных шифров. Показано, что неминимальный совершенный шифр вкладывается в максимальный совершенный шифр. Доказан аналог теоремы К. Шеннона для неэндоморфных совершенных шифров.

Ключевые слова: совершенные шифры, неэндоморфные шифры, максимальные шифры, неминимальные шифры.

Цель современных криптографических методов защиты информации — создание шифров, не позволяющих раскрыть никаких сведений о соответствующих им открытых текстах. Систематически вопрос о теоретической стойкости шифров впервые исследовал К. Шеннон в своей фундаментальной работе [1], в которой рассмотрена вероятностная модель шифра.

Пусть X , Y — конечные множества открытых и закрытых текстов, с которыми оперирует некоторый шифр замены, K — множество ключей, $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, $\lambda > 1$, $\mu > 1$. Согласно [2, 3], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и расшифрования с заданными распределениями вероятностей на множествах l -грамм открытых текстов, закрытых текстов и ключей.

Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*. Такие шифры являются абсолютно стойкими к криптоатакам по шифртексту. Совершенным может быть лишь шифр с неограниченным ключом [3]. Шифры, для которых $|X| = |Y|$, называются *эндоморфными* [1]. К. Шеннон полностью описал эндоморфные совершенные шифры с минимальным возможным числом ключей ($|K| = |Y|$).

Согласно [3], шифр Σ_B называется *сильно совершенным*, если он остается совершенным для любого распределения $P(X)$ вероятностей на множестве открытых текстов.

Шифры, для которых $|Y| < |K|$, называются *неминимальными*. Шифры, для которых $|K| = \mu \cdot (\mu - 1) \cdot \dots \cdot (\mu - \lambda + 1)$, то есть шифры, содержащие все инъекции $X \rightarrow Y$, называются *максимальными*. Доказано

Утверждение 1. Неминимальный совершенный шифр вкладывается в максимальный совершенный шифр.

В утверждении 1 имеется в виду не только теоретико-множественное включение, но и теоретико-вероятностное включение в рамках рассматриваемой модели шифра.

Кроме эндоморфных, существуют также *неэндоморфные* ($|X| < |Y|$) шифры с неравновероятными ключами, являющиеся сильно совершенными. Такие шифры обладают дополнительными свойствами, важнейшие из которых — имитостойкость и помехоустойчивость. Изучение неэндоморфных совершенных шифров в общем виде предполагает знание распределения вероятностей $P(X^l)$ на множестве l -грамм алфавита открытых текстов. В работе [4] рассматриваются комбинаторные аспекты проблематики совершенных шифров. В качестве стандартного аппарата исследования распределения вероятностей на l -граммах используются стохастические матрицы и однородные цепи Маркова. При этом проблематика описания совершенных шифров связана с классическими задачами описания статистически неопределённых систем [5]. Справедлива

Теорема 1. Неэндоморфный совершенный шифр является сильно совершенным.

Эквивалентность понятий совершенности и сильной совершенности для неэндоморфных шифров даёт большие возможности для их изучения.

В работе показано, что распределение вероятностей на множествах l -грамм закрытых текстов и ключей, при котором максимальный шифр будет совершенным, можно найти с помощью системы линейных уравнений. Данная система совместна, при этом её неизвестные принадлежат отрезку $[0; 1]$. Поэтому искомое распределение вероятностей в пространстве вероятностей представляет собой некоторое выпуклое тело P^ℓ

(многогранник) в многомерном евклидовом пространстве. Многогранник P^ℓ описан как выпуклая оболочка вершин. Справедливо

Утверждение 2. Если $\ell_1 < \ell_2$, то для соответствующих многогранников P^{ℓ_1} и P^{ℓ_2} выполняется условие $P^{\ell_1} \subset P^{\ell_2}$, то есть многогранники P^ℓ для ℓ -грамм при разных ℓ вложены в друг друга.

Итак, показано, что изучение неэндоморфных шифров сводится к изучению максимальных неэндоморфных шифров. При этом распределения вероятностей на l -граммах могут рассматриваться и как независимые, что характерно для блочных шифров, и как порождённые режимом гаммирования. Справедлива

Теорема 2. Совершенными максимальными шифрами являются шифры с вероятностями ключей $P(K^\ell)$ из многогранника P^ℓ , и только они.

Данная теорема является аналогом теоремы К. Шеннона, доказанным для общего класса неэндоморфных неминимальных шифров.

ЛИТЕРАТУРА

1. Шеннон К. Терия связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. Алферов А. П., Zubov A. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2001.
3. Zubov A. Ю. Совершенные шифры. М.: Гелиос АРВ, 2003.
4. Титов С. С., Гутарин Д. С., Коновалова С. С. и др. Комбинаторные проблемы существования совершенных шифров // Труды ИММ УрО РАН. 2008. Т. 13. № 4. С. 61–73.
5. Медведева Н. В., Тимофеева Г. А. Сравнение линейных и нелинейных методов доверительного оценивания для статистически неопределённых систем // Автоматика и телемеханика. 2007. № 4. С. 51–60.

УДК 519.7

О СВЯЗЯХ МЕЖДУ ОСНОВНЫМИ ПОНЯТИЯМИ РАЗНОСТНОГО АНАЛИЗА ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ

А. И. Пестунов

Обозначаются некоторые из проблем и несоответствий в существующей терминологии разностного анализа итеративных блочных шифров. Предлагается один из возможных наборов определений, позволяющий сформировать единообразную систему понятий, которая согласована с существующими терминами. Формализованы соответствия между основными понятиями, в частности показано, что в рамках предлагаемого набора определений дифференциал, характеристика и усечённый дифференциал являются усечёнными характеристиками. Формализовано и обобщено понятие объединения дифференциалов и характеристик.

Ключевые слова: терминология, дифференциальный криптоанализ, разностный анализ, блочный шифр, дифференциал, характеристика.

Разностный (дифференциальный) анализ [1] — это распространённый подход к анализу стойкости итеративных блочных шифров, однако несмотря на его популярность и наличие ряда разновидностей [2–5] к настоящему времени не выработана строгая единообразная терминология, его описывающая: основные понятия вводятся либо не строго, либо с использованием авторских определений. Такая ситуация не мешает разраба-