Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

О НОВОМ АЛГОРИТМЕ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ

Владимир Фомичёв, Алиса Коренева, Тимур Набиев

КОД БЕЗОПАСНОСТИ

Актуальность

Контроль целостности (КЦ): присоединение создателем информации (отправителем) к информационному *l*-битовому блоку *m*-битового кода контроля целостности, $m<l$.

Код контроля целостности (ККЦ): двоичная комбинация, связанная с блоком.

Используемые алгоритмы КЦ имеют недостатки:

- Надёжные криптографические хэш-функции требовательны к ресурсам.
- Циклические избыточные коды (CRC) обеспечивают помехоустойчивое кодирование, но поиск коллизии весьма вероятен.

Актуальная задача – построение альтернативных алгоритмов контроля целостности (АКЦ).

Цель исследования

Разработка скоростных АКЦ для больших массивов (ПО).

Важно достичь приемлемого компромисса между криптографическими свойствами АКЦ и ресурсами, необходимыми для его реализации.

Криптографические и эксплуатационные требования к АКЦ

- Биективность преобразования, на основе которого строится АКЦ
  (позволяет получать более точные оценки вероятности совпадения двух ККЦ для различных блоков)
- Полное перемешивание входных данных, то есть существенная зависимость каждого бита ККЦ от каждого бита блока данных
  (позволяет точно контролировать целостность, затрудняет навязывание ложных блоков)
- Невысокая вычислительная и емкостная (по памяти) сложность реализации
  (позволяет эффективно контролировать целостность больших массивов данных, в том числе в условиях ограниченных ресурсов)

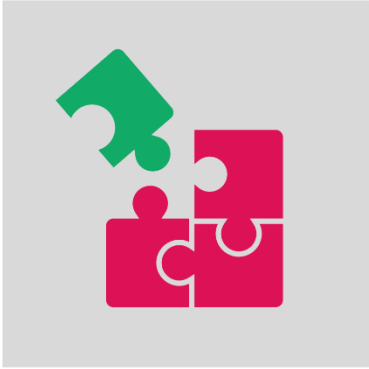
Задача генерации ККЦ

Построить алгоритм генерации *m*-битового ККЦ для информационного *l*-битового блока.

Для контроля целостности файла размера более *l* бит файл разбивается на отрезки по *l* бит и для каждого отрезка генерируется уникальный ККЦ.

Это ограничение не является принципиальным.

В докладе *l*=8192 бита (1КБайт), *m*=128 бит.



Обозначения

V_n — множество двоичных n-мерных векторов;

$\bar{X}$ — двоичное представление числа X из кольца вычетов $Z_{2^{64}}$;

$\boxplus$ — сложение чисел по модулю 2^{64}; $\oplus$ – XOR-суммирование;

$s(a_0,\dots,a_7)$ — функция ***вполне перемешивающего***[1] s-бокса размера 8×8 бит;

$s_0(a_0,\dots,a_7),\dots,s_7(a_0,\dots,a_7)$ — булевы координатные функции s-бокса;

φ – регистровое преобразование множества состояний аддитивного генератора длины 16 над V_{64} с одной обратной связью $f(X_0,\dots,X_{15})$ (в ячейке записан вычет $X \in Z_{2^{64}}$ или, что равносильно, вектор $\bar{X} \in V_{64}$):

$$\varphi(X_0,\dots,X_{15}) = (X_1,\dots,X_{15}, f(X_0,\dots,X_{15})).$$

[1] V.M. Fomichev. Matrix-graph approach for studying nonlinearity of transformations on vector space, CTCrypt 2019, https://ctcrypt.ru/files/files/2019/materials/08_Fomichev.pdf

АКЦ (1)

Алгоритм генерации 128-битового ККЦ блока 1 КБайт реализует функцию $\psi(g^t)$: $V_{8192} \to V_{128}$, где g: $V_{8192} \to V_{8192}$ — преобразование множества состояний схемы из 8 идентичных аддитивных генераторов $AG_0,\dots,AG_7$, функция обратной связи АГ

$$f(X_0,\dots,X_{15})=X_0 \boxplus X_5 \boxplus X_{10} \boxplus X_{15}.$$

При $t \geq 0$ преобразование $S^{(t)}$ задано формулой:

$$S^{(t)} = (s_0^{(t)}(\omega^{(t)}),\dots,s_7^{(t)}(\omega^{(t)})), \text{ где}$$

- $\omega^{(t)}=(\sigma(\bar{X}_{0,15}^{(t)}),\dots,\sigma(\bar{X}_{7,15}^{(t)}))$,
- $\sigma(x_0,\dots,x_{63})=x_0 \oplus \dots \oplus x_{63}$ – линейная булева функция четности веса вектора $(x_0,\dots,x_{63})$,
- $s_0^{(t)}(\omega^{(t)})=s(\omega^{(t)})$, $s_j^{(t)}(\omega^{(t)})=s(s_{j-1}^{(t)}(\omega^{(t)}) \oplus \omega^{(t)})$, $j=1,\dots,7$,
- s – нелинейный биективный s-бокс из ГОСТ 34.11-2018 (Стрибог) и ГОСТ 34.12-2018 (Кузнечик).

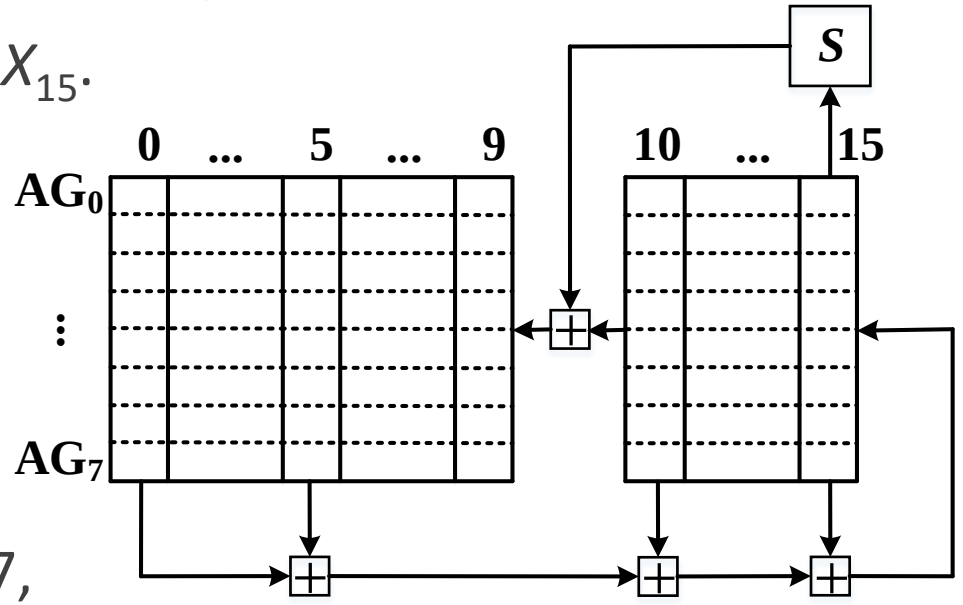


Рисунок – Регистр над $((Z_{2^{64}})^8, \boxplus)$

АКЦ (2)

АКЦ моделируется автономным автоматом Мили без выходов $A=(V_{8,16,64},g)$, где
g – функция переходов и
$V_{8,16,64}=\{x_{i,j,k}\}$ – множество состояний автомата, представимое как трехмерное множество двоичных чисел, множество координат которых биективно соответствует подмножеству P элементов трехмерного пространства с целыми координатами, ограниченному параллелепипедом:
$0 \le i < 8$, $0 \le j < 16$, $0 \le k < 64$.

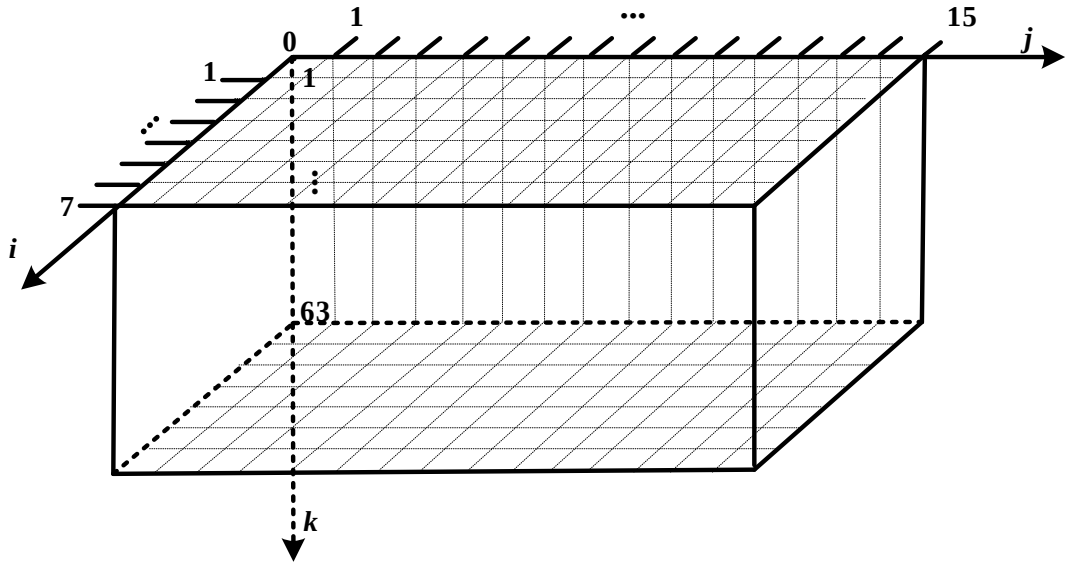


Рисунок – Параллелепипед, содержащий множество вершин (с целыми координатами) перемешивающего графа преобразования g

АКЦ (3)

Множество состояний автомата в такте $t \geq 0$ обозначим $V_{8,16,64}^{(t)} = \{x_{i,j,k}^{(t)}\}$, или матрицей $M_A^{(t)} = (X_{i,j}^{(t)})$ над $Z_{2^{64}}$, где $\bar{X}_{i,j}^{(t)} = (x_{i,j,0}^{(t)}, \ldots, x_{i,j,63}^{(t)})$ – состояние в t-м такте j-й ячейки АГ$_i$. Функция переходов автомата задана равенствами:

$$(X_{i,0}^{(t+1)}, \ldots, X_{i,n-1}^{(t+1)}) = (Y_{i,1}^{(t)}, \ldots, Y_{i,n-1}^{(t)}, f(Y_{i,0}^{(t)}, \ldots, Y_{i,n-1}^{(t)})),$$

где $Y_{i,j}^{(t)} = X_{i,j}^{(t)}$ при $j \neq 10$ и $Y_{i,10}^{(t)} = X_{i,10}^{(t)} \boxplus S^{(t)}$; $0 \leq i < 8$.

Код, генерируемый АКЦ блока данных, определим как 128-битовую строку:

$$\psi(g^t)(V_{8,16,64}) = (X_{0,15}^{(t)} \boxplus X_{1,15}^{(t)} \boxplus X_{2,15}^{(t)} \boxplus X_{3,15}^{(t)}, X_{4,15}^{(t)} \boxplus X_{5,15}^{(t)} \boxplus X_{6,15}^{(t)} \boxplus X_{7,15}^{(t)}). \quad (1)$$

Свойства АКЦ: биективность

Преобразование g биективное. Число прообразов любого значения функции $\psi(g^t)$ равно 2^{l-2r}.

Следовательно, при случайном равновероятном выборе начального состояния u из множества $V_{8,16,64}$ вероятность получить заданный код Q равна 2^{-128}.

Среднее число опробований для поиска блоков u, u' таких, что $u \neq u'$ и $Q(u)=Q(u')$, оценивается с помощью «парадокса дней рождения» величиной порядка 2^{64}.

Свойства АКЦ (2): перемешивание

Перемешивающие свойства АКЦ оценены с помощью развития МГП для оценки перемешивающих свойств модифицированных АГ [2].

Для перемешивания в крайних ячейках регистров (требуется в соответствии с (1)) оценен локальный экспонент перемешивающего орграфа Г(g) :

$$*U\text{-exp}\Gamma(g) \le 6,$$

где $U=\bigcup_{0\le i<8;0\le k<64}\{(i,15,k)\}$. Оценка следует из [3, с.457] (для всех допустимых пар вершин ((*i*,15,*j*),(*i*′,15,*j*′)) оценена длина пути из одной вершины в другую, проходящего через некоторую вершину с петлей).

[2] V.M. Fomichev, A.M. Koreneva. Mixing properties of modified additive generators, J. Appl. Industr. Math., 11:2 (2017), 215–226 pp., DOI: 10.1134/s1990478917020077

[3] Fomichev, Ya.E. Avezova, A.M. Koreneva, S.N. Kyazhin. Primitivity and Local Primitivity of Digraphs and Nonnegative Matrices, J. Appl. Industr. Math., 12:3, 2018, 453-469 pp. DOI: 10.1134/s1990478918030067

Свойства АКЦ: выбор числа тактов t

Для надежного контроля целостности необходимо вычисление ККЦ с помощью вполне перемешивающей функции.

Установлено, что при $t \geq 6$ обе функции, формирующие ККЦ,

$$X_{0,15}^{(t)} \boxplus X_{1,15}^{(t)} \boxplus X_{2,15}^{(t)} \boxplus X_{3,15}^{(t)} \text{ и}$$

$$X_{4,15}^{(t)} \boxplus X_{5,15}^{(t)} \boxplus X_{6,15}^{(t)} \boxplus X_{7,15}^{(t)}$$

вполне перемешивающие.

Экспериментально определено, что при $6 \leq t \leq 100$ свойство полного перемешивания этих функций сохраняется.

Свойства АКЦ: реализация

Сложность вычисления функции $\psi(g^t)$ оценивается величиной порядка $t(5u+8v)$, где u – вычислительная сложность суммирования двух чисел по mod 2^{64}, v – сложность вычисления s-бокса.

В таблице даны результаты измерения скорости генерации и времени вычисления 128-битового ККЦ для блока данных 1 Кбайт при различных t.

Таблица. Скорость генерации и время вычисления ККЦ

Число тактов, t	6	12	18	36	72	96
Скорость генерации, Мбит/сек	3500	1900	1200	650	330	250
Время вычисления, мс	0,018	0,032	0,049	0,096	0,2	0,25

Эксперименты проведены на ПЭВМ с процессором Intel Core i5-8600 и тактовой частотой 3.1 GHz.

Спасибо за внимание!

Вопросы ?