Об одной низкоресурсной хэш-функции.

Бондакова Ольга Сергеевна

РТУ МИРЭА
институт Кибернетики
кафедра «Информационная безопасность»

19 марта 2020 г.

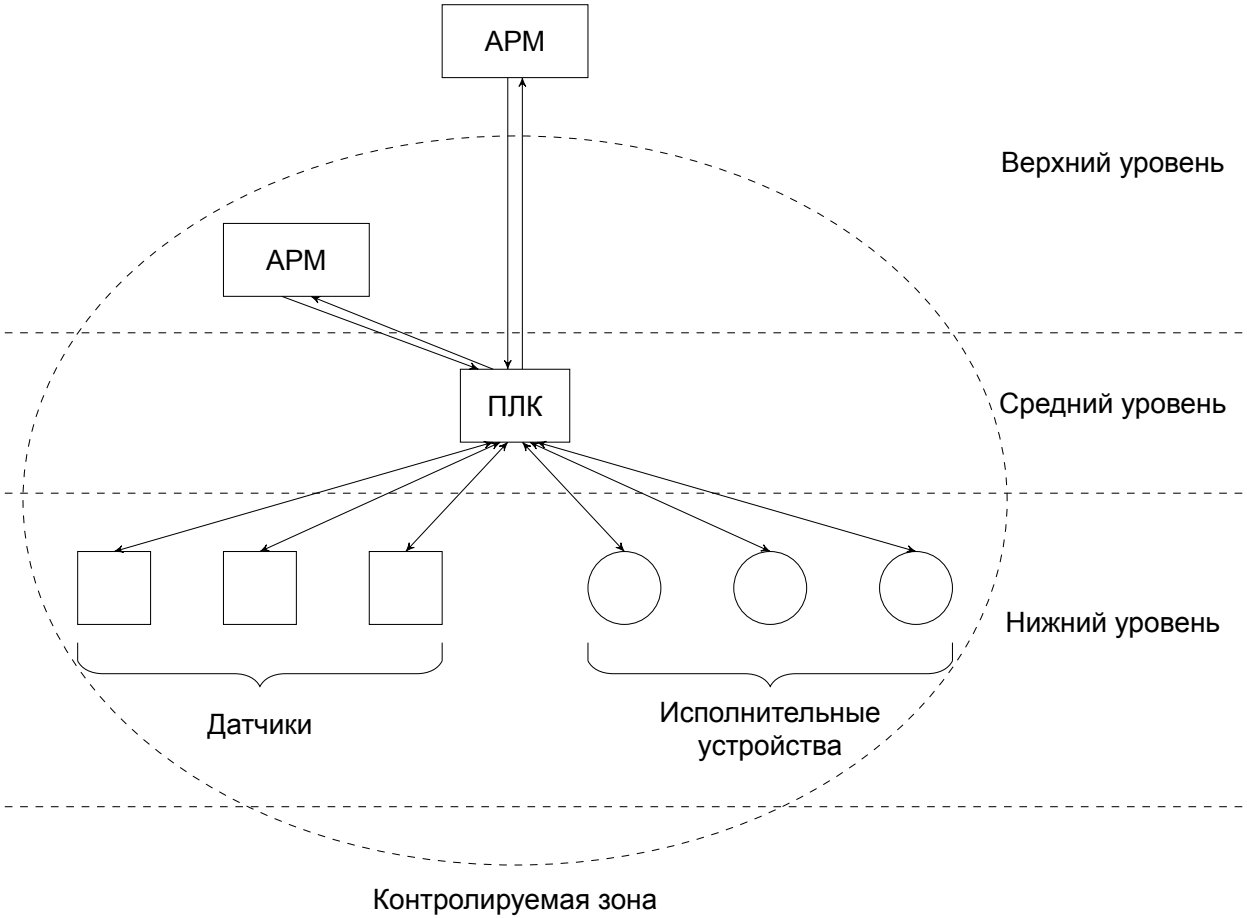
Перспективные исследования

Программа «Цифровая экономика Российской Федерации»
(утв. расп. Правительства Российской Федерации
от 28 июля 2017 года №1632-р)

«Основными сквозными цифровыми технологиями,
которые входят в рамки настоящей программы, являются:

- большие данные;
- нейротехнологии и искусственный интеллект;
- системы распределенного реестра;
- квантовые технологии;
- новые производственные технологии;
- **промышленный интернет;**
- компоненты робототехники и сенсорика;
- технологии беспроводной связи;
- технологии виртуальной и дополненной реальностей.»

Общая схема АСУ ТП



Основные особенности устройств полевого уровня

1. Малые вычислительные ресурсы.
2. Небольшое время жизни передаваемой информации.

Модель угроз

1. Искажение небольшого числа выбранных битовых позиций в передаваемых данных.
2. Искажение определённых битовых позиций для определённых сообщений.
3. Искажение данных управляющего устройства.

Криптографические методы защиты информации

1. Возможность защиты информации на всех этапах её обработки.

Криптографические методы защиты информации

1. Возможность защиты информации на всех этапах её обработки.
2. Возможность получения оценок уровня защищенности информации.

Подходы к снижению затрат ресурсов

1. Эффективные реализации существующих алгоритмов.

Подходы к снижению затрат ресурсов

1. Эффективные реализации существующих алгоритмов.
2. Модернизация существующих решений под конкретные требования.

Подходы к снижению затрат ресурсов

1. Эффективные реализации существующих алгоритмов.
2. Модернизация существующих решений под конкретные требования.

Предлагаемое решение:

Синтез криптографических примитивов с низкой ресурсоемкостью и приемлимым уровнем защиты информации.

Низкоресурсная хэш-функция для АСУ ТП

Наиболее перспективными криптографическими примитивами для решения сформулированных задач являются низкоресурсные хэш-функции.

Особенности анализа

1. Построение второго прообраза
2. Построение коллизии для сообщений с разницей определённого вида.

Структура синтезируемой хэш-функции

Распространённые конструкции хэш-функций:

Структура синтезируемой хэш-функции

Распространённые конструкции хэш-функций:

1. МД-конструкция (известная также как конструкция Меркла-Дамгорда).

Структура синтезируемой хэш-функции

Распространённые конструкции хэш-функций:

1. МД-конструкция (известная также как конструкция Меркла-Дамгорда).
2. Sponge-конструкция (известная также как «криптографическая губка»).

Структура синтезируемой хэш-функции

Существуют различные модификации МД-конструкции, улучшающие её свойства (HAIFA и другие).

Выбрана модификация МД-конструкции, на которой основана Российская функция хэширования ГОСТ Р 34.11-2012 («Стрибог»).

Подход к синтезу

Уменьшить размерности преобразований хорошо изученной хэш-функции «Стрибог», полностью сохранив структуру и принципы её построения.

Функция сжатия

Одношаговая функция сжатия «Стрибога» представляет собой однонаправленную функцию сжатия Миагучи-Принеля:

$$g_N(h_i, m_i) = E(LPS(h_{i-1} \oplus N),\ m_i) \oplus m_i \oplus h_{i-1}$$

Где $E(LPS(h_{i-1} \oplus N),\ m_i)$ —алгоритм блочного шифрования (XSPL-шифр) с размером блока равным размеру хэш-кода.

Блочный шифр

XSPL-шифр с размер блока $n = mk^2$ бит состоит из r раундов.

Раундовые преобразования:

1. Сложение по модулю 2 блока открытого текста с ключом $X : V_n \to V_n$.

Блочный шифр

XSPL-шифр с размер блока $n = mk^2$ бит состоит из r раундов.

Раундовые преобразования:

1. Сложение по модулю 2 блока открытого текста с ключом $X : V_n \to V_n$.
2. Нелинейное биективное преобразование $S : V_n \to V_n$, $S(a_{k^2-1}||...||a_0) = \pi(a_{k^2-1}), ..., \pi(a_0),$ где $\pi : V_m \to V_m$.

Блочный шифр

XSPL-шифр с размер блока $n = mk^2$ бит состоит из r раундов.

Раундовые преобразования:

1. Сложение по модулю 2 блока открытого текста с ключом $X : V_n \to V_n$.
2. Нелинейное биективное преобразование $S : V_n \to V_n$, $S(a_{k^2-1}||...||a_0) = \pi(a_{k^2-1}), ..., \pi(a_0)$, где $\pi : V_m \to V_m$.
3. Перестановка m-битных элементов входного вектора $P : V_n \to V_n$, $P(a_{k^2-1}||...||a_0) = a_{\tau(k^2-1)}||...||a_{\tau(0)}$, где $\tau : \mathbb{Z}_{k^2} \to \mathbb{Z}_{k^2}$.

Блочный шифр

XSPL-шифр с размер блока $n = mk^2$ бит состоит из r раундов.

Раундовые преобразования:

1. Сложение по модулю 2 блока открытого текста с ключом $X : V_n \to V_n$.
2. Нелинейное биективное преобразование $S : V_n \to V_n$, $S(a_{k^2-1}||...||a_0) = \pi(a_{k^2-1}), ..., \pi(a_0),$ где $\pi : V_m \to V_m$.
3. Перестановка m-битных элементов входного вектора $P : V_n \to V_n,\ P(a_{k^2-1}||...||a_0) = a_{\tau(k^2-1)}||...||a_{\tau(0)},$ где $\tau : \mathbb{Z}_{k^2} \to \mathbb{Z}_{k^2}$.
4. Линейное преобразование $L : V_n \to V_n,\ L(a_{k-1}||...||a_0) = l(a_{k-1})||...||l(a_0)$, где l умножение слева векторов размерности mk на битовую матрицу над полем GF(2). $l : V_{mk} \to V_{mk}$.

Блочный шифр

Блочный шифр в функции хэширования «Стрибог» имеет структуру квадрата:

Размер блока (*n*)	**Размерность подстановки (*m*)**	**Размерность матрицы (*k*)**
128	8	4
64	4	4

Блочный шифр

Блочный шифр в функции хэширования «Стрибог» имеет структуру квадрата:

Преобразование	**«Стрибог»**	**Уменьшенная хэш-функция**
X	$V_{512} \to V_{512}$	$V_{64} \to V_{64}$
S (π)	$V_{512} \to V_{512}$ $(V_8 \to V_8)$	$V_{64} \to V_{64}$ $(V_4 \to V_4)$
P (τ)	$V_{512} \to V_{512}$ $(\mathbb{Z}_{64} \to \mathbb{Z}_{64})$	$V_{64} \to V_{64}$ $(\mathbb{Z}_{16} \to \mathbb{Z}_{16})$
L (l)	$V_{512} \to V_{512}$ $(V_{64} \to V_{64})$	$V_{64} \to V_{64}$ $(V_{16} \to V_{16})$

Требования к параметрам. Полубайтовая перестановка

Перестановка является транспонированием квадратной матрицы и не требует отдельного рассмотрения подходов к построению.

$$a = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$$

$$P(a) = \tau(a_0)||...||\tau(a_{15}) = \begin{pmatrix} a_0 & a_4 & a_8 & a_{12} \\ a_1 & a_5 & a_9 & a_{13} \\ a_2 & a_6 & a_{10} & a_{14} \\ a_3 & a_7 & a_{11} & a_{15} \end{pmatrix}$$

Требования к параметрам. Подстановка

Характеристики нелинейного биективного преобразования полубайт:

1. Степень нелинейности $\lambda_\pi = \min\limits_{\beta \in V_m \setminus \{0\}} deg(\beta,\ \pi(x)) = 3.$
2. Разностная характеристика
   $\rho_\pi = \max\limits_{\alpha,\ \beta \neq 0} P\{\pi(x) \oplus \pi(x \oplus \alpha) = \beta\} = \frac{1}{4}.$
3. Линейная характеристика
   $\delta_\pi = \max\limits_{\alpha,\ \beta \neq 0} |2P\{(x,\ \alpha) = (\pi(x),\ \beta)\} - 1| = \frac{1}{2}.$

Требования к параметрам. Подстановка

[1] Шишкин В. А, Маршалко Г. Б., Миронкин В. О., Лавриков И. В. «Нелинейные биективные преобразования: задачи, которые решены, которые решают, которые предстоит решить». Доклад на семинаре "Актуальные проблемы дискретной математики"

$$\pi = (15,\ 9,\ 1,\ 7,\ 13,\ 12,\ 2,\ 8,\ 6,\ 5,\ 14,\ 3,\ 0,\ 11,\ 4,\ 10)$$

Требования к параметрам. Линейное преобразование

Матрица, используемая в преобразовании *l*, должна быть МДР-матрицей для улучшения рассеивающих свойств блочного шифра.

Требования к параметрам. Линейное преобразование

[2] Гонсалес С., Коусело Е., Марков В., Нечаев А. Параметры рекурсивных МДР-кодов. Дискретная математика. Т. 12, в. 4. 2000 г.

$$A = \begin{pmatrix} 2 & 12 & 13 & 13 \\ 9 & 1 & 2 & 3 \\ 6 & 14 & 5 & 6 \\ 12 & 8 & 6 & 13 \end{pmatrix}$$

$$A_b = \begin{matrix} 3a22 & 483b & 59e5 & ac52 \\ 8511 & 248c & bd7b & 56b1 \\ 4b99 & 1246 & cfac & b3c9 \\ 2cdd & 9123 & 6e56 & c86d \end{matrix}$$

Первичная оценка количества раундов (Ф. М. Малышев, Д. И. Трифонов)

Для XSPL-шифра:
$E(k, m) = X[k_r]LPSX[k_{r-1}]...LPSX[k_2]LPSX[k_1]LPSX[k](m)$
Можно определить показатель рассеивания:
$\theta(r) = (k+1)^2[\frac{r-1}{4}] + \theta(r - 4[\frac{r-1}{4}]), r \geq 5.$

Результаты криптоанализа

Атака	Наибольшее количество атакованных раундов	Рекомендации по количеству раундов
Построение коллизии для сообщений отличающихся в определённых полубайтах	4	6
Построение случайной коллизии	7.75	9

Результаты криптоанализа

Атака	Наибольшее количество атакованных раундов	Рекомендации по количеству раундов
Построение прообраза	5	7
Построение линейного различителя	7	9

Полученная оценка количества раундов

На основании результатов проведённого криптоанализа был сделан вывод, что наименьшее количество раундов, обеспечивающее стойкость к проведённым атакам, составит **9 раундов**.

Процесс получения итерационная констант

Значение счётчика	Итерационная константа
0000000000000001	c0164633575a9699
0000000000000002	925b4ef49a5e7174
0000000000000003	86a89cdcf673be26
0000000000000004	1885558f0eaca3f1
0000000000000005	dcfc5b89e35e8439
0000000000000006	54b9edc789464d23
0000000000000007	f80d49afde044bf9
0000000000000008	8cbbdf71ccaa43f1
0000000000000009	cb43af722cb520b9

Реализация

Спасибо за внимание!!!