Обзор результатов анализа хэш-функций ГОСТ Р 34.11-2012

Лавриков И.В., Маршалко Г.Б., Рудской В.И., Смышляев С.В., Шишкин В.А.

РусКрипто 2015

18 марта 2015 года

Введение

История

- Первый анонс – РусКрипто 2010
- Национальный стандарт – ГОСТ Р 34.11-2012
- Открытый конкурс работ
- Стандартизация в ISO

Основные направления исследований

- Свойства функции сжатия
- Свойства конструкции хэш-функции в целом
- Вопросы реализации

Исследования свойств функции сжатия

- AlTawy R., Youssef A. M. – Preimage Attacks on reduced-round Stribog
- AlTawy R., Kircanski A., Youssef A. M. – Rebound attacks on Stribog
- Kazymyrov O., Kazymyrova V. – Algebraic aspects of the russian hash standard GOST R 34.11-2012.
- Ma B., Li B., Hao R., Li X. – Improved cryptanalysis of reduced-round GOST and Whirlpool hash function
- Zou J., Wu W., Wu S. – Cryptanalysis of the round-reduced GOST hash function
- AlTawy R., Youssef A. M. – Integral distinguishers for reduced-round Stribog
- AlTawy R., Youssef, A. M. – Watch your Constants: Malicious Streebog

AlTawy R., Youssef A. M. – Preimage Attacks on reduced-round Stribog

- Задача построения псевдо-прообраза
- Используется подход Sasaki Y. et. al. для Whirlpool и AES в режиме хэширования
- Метод встречи посередине

Псевдо-прообраз для функции сжатия

- 5 из 12 раундов – 2^{448} функций сжатия и 2^{64} памяти
- 6 из 12 раундов – 2^{496} функций сжатия и 2^{112} памяти

Функция хэширования с усеченной фукнцией сжатия

- Метод построения мультиколлизий
- 5 из 12 раундов – 2^{481} и 2^{256} памяти
- 6 из 12 раундов – 2^{505} и 2^{256} памяти
- По сравнению с Whirlpool – больше трудоемкость и больше памяти

AlTawy R., Kircanski A., Youssef A. M. – Rebound attacks on Stribog

- Применяется известный метод столкновения (rebound attack: Mendel, Rechberger, Schläffer, Thomsen, FSE 2009)
- Разностные соотношения для блочного шифра – inbound-outbound
- Коллизия для 5 раундов и произвольного начального значения
- Для 7.75 раундов – свободная коллизия для функции сжатия за 2^{184}
- Для 8.75 раундов – свободная почти-коллизия функции сжатия за 2^{128}

Kazymyrov O., Kazymyrova V. – Algebraic aspects of the russian hash standard GOST R 34.11-2012

- Исследуются алгебраические характеристики
- Предложено эквивалентное представление блочного шифра

Ma B., Li B., Hao R., Li X. – Improved cryptanalysis of reduced-round GOST and Whirlpool hash function

- Известные методы построения мультиколлизий и супер S-блоков
- Встреча посередине без больших объемов памяти
- Коллизия Стрибог-256, 6.5 раундов – 2^{125} ф.с., память 2^{64}
- Коллизия Стрибог-512, 7.5 раундов – 2^{181} ф.с., память 2^{64}
- Прообраз Стрибог-512, 6 раундов – 2^{496} ф.с., память 2^{64}
- Прообраз Стрибог-512, 6 раундов – 2^{504} ф.с., память 2^{11}
- Различитель Стрибог-512, 9.5 раундов – 2^{441} ф.с., память 2^{136}

Zou J., Wu W., Wu S. – Cryptanalysis of the round-reduced GOST hash function

- Известные методы построения мультиколлизий и супер S-блоков
- Коллизия Стрибог-256/512, 5 раундов – 2^{122} ф.с., память 2^{64}

AlTawy R., Youssef, A. M. – Watch your Constants: Malicious Streebog

- Метод столкновения
- Модификация раундовых констант (6 из 12)
- Получена коллизия для модифицированной функции за практическое время
- Константы – фиксированный элемент
- Коллизия-«закладка»

Как генерировались константы

- Генерация псевдо-случайным образом
- Стрибог-подобная хэш-функция
- $C_1 = C_2 = \ldots = C_{12} = 0^{512}$
- Матрица преобразования l имеет обратный порядок столбцов

1	e2e5ede1e5f0c3
2	f7e8e2eef0e8ece8e4e0ebc220e9e5e3f0e5d1
3	f5f3ecc4
4	f7e8e2eef0e4ede0f1eae5ebc020e9e5f0e4edc0
5	ede8e3fbc4
6	f7e8e2eeebe9e0f5e8cc20f1e8ede5c4
7	ede8f5fef2e0cc
8	f7e8e2eef0eef2eae8c220e9e8f0f2e8ecc4
9	e9eeeaf1e4f3d0
10	f7e8e2e5f0eee3c820f0e8ece8e4e0ebc2
11	ede8eaf8e8d8
12	f7e8e2e5e5f1eae5ebc020e9e8ebe8f1e0c2

Исследования свойств конструкции хэш-функции в целом

- Седов Г. – Стойкость ГОСТ Р 34.11-2012 к атаке на прообраз и атаке поиска коллизий
- Guo J., Jean J., Leuren G., Peyrin T., Wang L. – The Usage of Counter Revisited: Second-Preimage

Седов Г. – Стойкость ГОСТ Р 34.11-2012 к атаке на прообраз и атаке поиска коллизий

- Исследуются общие свойства конструкции функций ГОСТ Р 34.11-2012
- Строится семейство функций
- Демонстрируются специальные свойства этого семейства:
  - Стойкость семейства к методам построения прообраза
  - Стойкость семейства к методам построения коллизии
- Свидетельствует в пользу синтезных решений

Guo J., Jean J., Leuren G., Peyrin T., Wang L. – The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function

- Методы построения второго прообраза в стандартных предположениях
- Способ обработки счетчика
- Эквивалентное представление – «счетчик» $\Delta(i) = i \oplus (i+1)$
- Композиция методов:
  - Метод мультиколлизии Gauravaram-Kelsey
  - Древовидная мультиколлизия («diamond-structure»)
  - Метод Kelsey-Schneier
- Используются свойства последовательности $\Delta(i)$
- 2^{342} для сообщения длины 2^{179} (блоков)
- 2^{266} для сообщения длины 2^{259} (блоков)
- Для классической конструкции Меркля-Дамгарда трудоемкость 2^{n-x} для сообщения 2^x блоков
- Для Стрибог-256 трудоемкость выше универсального метода

Исследования вопросов реализации

- Borodin M., Rybkin A., Urivskiy A. – High-Speed Software Implementation of the Prospective 128-bit Block Cipher and Streebog Hash-Function.
- Бородин М., Рыбкин А. – Эффективная реализация базовых криптограифческих конструкций: песрпективного алгоритма блочного шифрвоания с длиной блока 128 бит, функции хэширования ГОСТ Р 34.11-2012 и ЭЦП ГОСТ Р 34.10-2012.
- Lebedev P.A. – Comparison of old and new cryptographic hash function national standards of Russian Federation on CPUs and NVIDIA 196 GPUs
- Казимиров А., Смышляев С. – О создании эффективных программных реализаций отечественных криптограифческих стандартов.

Borodin M., Rybkin A., Urivskiy A. – High-Speed Software Implementation of the Prospective 128-bit Block Cipher and Streebog Hash-Function

- Эффективные программные реализации алгоритмов
- Табличное задание LS-преобразования
- Использование SSE4
- 92 МБ/с – core i7-2600 @3.4 GHz

Lebedev P.A. – Comparison of old and new cryptographic hash function national standards of Russian Federation on CPUs and NVIDIA 196 GPUs

- Сравниваются стандарты ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012
- Исследования на x86-64 и NVIDIA CUDA
- Стрибог быстрее на процессорах общего назначения, но медленнее на GPU и lightweight-платформах

Казимиров А., Смышляев С. – О создании эффективных программных реализаций отечественных криптографических стандартов

- ГОСТ 28147, ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012
- Процессоры общего назначения
- Функция сжатия и полный цикл
- Сравнение с зарубежными функциями
- Стрибог превосходит ГОСТ Р 34.11-94, но уступает SHA-2
- Стрибог сопоставим с Keccak по функции сжатия, но в 2.5 раза уступает на полном цикле

Заключение

- Функция ГОСТ Р 34.11-2012
- За 5 лет с момента анонса появилось множество работ
- Большинство существующих подходов были рассмотрены
- Подтверждается правильный выбор синтезных решений
- Хорошие эксплуатационные характеристики

Спасибо за внимание!