О предложениях французских специалистов по международной стандартизации программного датчика случайных чисел на основе систем квадратичных уравнений

В.О. Дрелихов Г.Б. Маршалко А.В. Покровский

31 марта 2011 / РусКрипто'11

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Основные положения

- Определяет типы датчиков:
  - Физические датчики
  - Программные датчики
- Определяет свойства датчиков случайных чисел и требования предъявляемые к ним
- Определяет способы комбинирования датчиков
- Определяет конкретные типы программных датчиков

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Основные положения

- Определяет типы датчиков:
  - Физические датчики
  - Программные датчики
- Определяет свойства датчиков случайных чисел и требования предъявляемые к ним
- Определяет способы комбинирования датчиков
- Определяет конкретные типы программных датчиков

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Основные положения

- Определяет типы датчиков:
  - Физические датчики
  - Программные датчики
- Определяет свойства датчиков случайных чисел и требования предъявляемые к ним
- Определяет способы комбинирования датчиков
- Определяет конкретные типы программных датчиков

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Основные положения

- Определяет типы датчиков:
  - Физические датчики
  - Программные датчики
- Определяет свойства датчиков случайных чисел и требования предъявляемые к ним
- Определяет способы комбинирования датчиков
- Определяет конкретные типы программных датчиков

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Основные положения

- Определяет типы датчиков:
  - Физические датчики
  - Программные датчики
- Определяет свойства датчиков случайных чисел и требования предъявляемые к ним
- Определяет способы комбинирования датчиков
- Определяет конкретные типы программных датчиков

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Основные положения

- Определяет типы датчиков:
  - Физические датчики
  - Программные датчики
- Определяет свойства датчиков случайных чисел и требования предъявляемые к ним
- Определяет способы комбинирования датчиков
- Определяет конкретные типы программных датчиков

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Стандартизированные решения

- Датчики, основанные на функциях хеширования (SHA1/SHA2):
  - HASH_DRBG
  - HMAC_DRBG
- Датчики, основанные на блочных шифрах:
  - CTR_DRBG
  - OFB_DRBG
- Датчики, основанные на теоретико-числовых задачах:
  - Dual_EC_DRBG (Эллиптические кривые)
  - MS_DRBG (RSA)

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Стандартизированные решения

- Датчики, основанные на функциях хеширования (SHA1/SHA2):
  - HASH_DRBG
  - HMAC_DRBG
- Датчики, основанные на блочных шифрах:
  - CTR_DRBG
  - OFB_DRBG
- Датчики, основанные на теоретико-числовых задачах:
  - Dual_EC_DRBG (Эллиптические кривые)
  - MS_DRBG (RSA)

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Стандартизированные решения

- Датчики, основанные на функциях хеширования (SHA1/SHA2):
  - HASH_DRBG
  - HMAC_DRBG
- Датчики, основанные на блочных шифрах:
  - CTR_DRBG
  - OFB_DRBG
- Датчики, основанные на теоретико-числовых задачах:
  - Dual_EC_DRBG (Эллиптические кривые)
  - MS_DRBG (RSA)

В стандарте сформулированы рекомендации по оценке стойкости датчиков, которые включают в себя

- Модель нарушителя:
- Вопросы стойкости функций хеширования
- Методику сравнительной оценки алгоритмов и длин ключей
- Вопросы стойкости генераторов использующих блочные шифры
- Статистические критерии
- Вопросы оценки энтропии

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Вопросы оценки стойкости

В стандарте сформулированы рекомендации по оценке стойкости датчиков, которые включают в себя

- Модель нарушителя:
- Вопросы стойкости функций хеширования
- Методику сравнительной оценки алгоритмов и длин ключей
- Вопросы стойкости генераторов использующих блочные шифры
- Статистические критерии
- Вопросы оценки энтропии

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Вопросы оценки стойкости

В стандарте сформулированы рекомендации по оценке стойкости датчиков, которые включают в себя

- Модель нарушителя:
- Вопросы стойкости функций хеширования
- Методику сравнительной оценки алгоритмов и длин ключей
- Вопросы стойкости генераторов использующих блочные шифры
- Статистические критерии
- Вопросы оценки энтропии

В стандарте сформулированы рекомендации по оценке стойкости датчиков, которые включают в себя

- Модель нарушителя:
- Вопросы стойкости функций хеширования
- Методику сравнительной оценки алгоритмов и длин ключей
- Вопросы стойкости генераторов использующих блочные шифры
- Статистические критерии
- Вопросы оценки энтропии

В стандарте сформулированы рекомендации по оценке стойкости датчиков, которые включают в себя

- Модель нарушителя:
- Вопросы стойкости функций хеширования
- Методику сравнительной оценки алгоритмов и длин ключей
- Вопросы стойкости генераторов использующих блочные шифры
- Статистические критерии
- Вопросы оценки энтропии

ISO/IEC 18031. Information technology — Security techniques — Random Bit Generation

Вопросы оценки стойкости

В стандарте сформулированы рекомендации по оценке стойкости датчиков, которые включают в себя

- Модель нарушителя:
- Вопросы стойкости функций хеширования
- Методику сравнительной оценки алгоритмов и длин ключей
- Вопросы стойкости генераторов использующих блочные шифры
- Статистические критерии
- Вопросы оценки энтропии

Датчик MQ_DRBG
Описание

Датчик MQ_DRBG задается системой квадратичных уравнений

$$Q_k(\overline{x}) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j + \sum_{1 \le i \le n} b_i x_i + \gamma,\ 1 \le k \le n + r$$

над полем $GF(2^m)$.
При этом должны быть выполнены два условия

- Ранг каждого уравнения не меньше min_rank
- Ранг линейной комбинации не более max_weight уравнений не меньше min_rank

Также, для каждого набора параметров устанавливается максимальный интервал перезапуска l, после которого необходимо переинициализировать датчик.

Датчик MQ_DRBG
Аргументы „за“

- „QUAD: A practical stram cipher with provable sequrity“, C. Berbain, H.Gilbert, J. Patarin, EUROCRYPT'06
- Быстрота реализации: используются только операции AND и XOR (медленне AES, но быстрее теоретико-числовых генераторов)
- Основан на задаче решения квадратичных уравнений (NP-полна)
- Оценки сложности решения систем нелинейных уравнений (линеаризация, алгоритмы Фужера и т.д.): огромный объем памяти и сложность порядка $2^{n-O(\sqrt{n})}$ двоичных операций при $n = r$

Датчик MQ_DRBG
Доказательство стойкости

Доказательство стойкости датчика (неотличимости от случайной равновероятной последовательности, невозможности предсказывания предыдущего и последующего состояния) приводится авторами в терминах теории доказуемой стойкости. Таким образом, полученные оценки носят асимптотический характер и получаются усреднением по всему множеству систем и начальных состояний при случайном и равновероятном выборе системы и начального состояния.

Датчик MQ_DRBG
Параметры датчика

80 2-TDEA	n=r=112 $GF(2)$,l=2^{23}	n=r=128 $GF(2^4)$,l=2^{12}	n=r=192 $GF(2^6)$,l=2^{23}	n=r=256 $GF(2^8)$,l=
112 3-TDEA	n=120, r=112 $GF(2)$,l=2^{26}	n=r=128 $GF(2)$,l=2^{32}	n=r=192 $GF(2^4)$,l=2^{12}	n=r=256 $GF(2^4)$,l=
128 AES-128	–	n=r=128 $GF(2)$,l=2^{28}	n=r=192 $GF(2^3)$,l=2^{16}	n=r=256 $GF(2^4)$,l=
192 AES-192	–	–	n=200, r=192 $GF(2)$,l=2^{32}	n=r=256 $GF(2^2)$,l=
256 AES-256	–	–	–	n=272,r= $GF(2)$,l=

Анализ датчика MQ_DRBG

Практическая применимость результатов

Два вопроса:

- Выполняются ли для предложенного преобразования теоретико-вероятностные предположения, позволяющие использовать применяемый подход?
- Существуют ли классы систем, для которых полученные оценки не выполняются?

Анализ датчика MQ_DRBG

Экспериментальная оценка близости к случайному отображению

Одним из условий применения использованного авторами подхода к доказательству, является близость отображения к случайному. Теоретически доказать такой факт крайне сложно. Возможный подход - моделирование и оценка параметров графа переходов внутрених состояний датчика: средней длины максимального подхода $h_{\max}$, среднего числа компонент отображения n_{exp}, среднего числа циклических точек n_{cicl}, средней длина цикла l_{cicl}.

Анализ датчика MQ_DRBG

Параметры графа модели

n	$h_{\max}$	$n_{\exp}$	n_{cicl}	l_{cicl}
20	1785.19	7.41	1225.45	180.45
16	441.972	6.258	324.919	57.1186

Таблица: Экспериментальные значения

n	$h_{\max}$	$n_{\exp}$	n_{cicl}	l_{cicl}
20	1779.16	6.931	1283.39	185.942
16	444.79	5.545	320.85	57.863

Таблица: Теоретические значения

Вместе с тем существуют отображения с сильными отклонениями параметров от средних значений.

Анализ датчика MQ_DRBG

Построение системы не удовлетворяющей заявленной стойкости

Рассмотрим случай датчика над полем $GF(2)$ с параметрами $n = 112, r = 112, min\_rank = 106, max\_weight = 4$, который должен удовлетворять заявленой стойкости 2^{80} двоичных операций.

Построим систему вида

$$\bigoplus_{i=1}^{53} l_{2i-1}^{(j)}(x_{54}, \ldots, x_{112}) l_{2i}^{(j)}(x_1, \ldots, x_{53}),$$

где $j = \overline{1, T}$, $l_m^{(j)}$— линейная функция и набор

$$l_1^{(j)}(x_{54}, \ldots, x_{112}), l_2^{(j)}(x_1, \ldots, x_{53}), \ldots,$$

$$\ldots, l_{105}^{(j)}(x_{54}, \ldots, x_{112}), l_{106}^{(j)}(x_1, \ldots, x_{53})$$

линейно независим.

Анализ датчика MQ_DRBG

Построение системы не удовлетворяющей заявленной стойкости

Решение предложенной системы заключается в переборе значений переменных $x_1, \ldots, x_{53}$ после чего каждое квадратичное уравнение становится линейным, если не все переменные зафиксированы нулями. В результате для каждого варианта зафикисированных переменных будет получаться линейная система от 59 неизвестных, которую можно решить и тем самым восстановить инициализирующий вектор. Трудоемкость такого подхода, при $T = 53$ составляет $2^{53}(59)^3 \approx 2^{71}$ двоичных операций, что на девять порядков меньше обозначенной в проекте стандарта трудоемкости.

Анализ датчика MQ_DRBG

Построение системы не удовлетворяющей заявленной стойкости

Задача построения описанной системы сводится к задаче построения линейного кода с характеристиками $(53, 53 - m, d), d > 4, 2^m - 1 > n + r$. Коды с указанными параметрами существуют.

Таким образом, для указанных авторами проекта параметров можно построить квадратичные системы, трудоемкость решения которых существенно меньше указанного авторами значения.

Выводы

Проведенный анализ показал, что

- в среднем характеристики случайным образом вырабатываемых квадратичных систем близки к характеристикам случайного отображения;
- возможно построение систем, удовлетворяющих ограничениям, накладываемым проектом стандарта, но имеющих стойкость меньшую заявленной авторами оценки.