Александр А. Козлов
ООО «Научно-технический центр «Вулкан»,
ул. Ибрагимова, 31, Москва, 105318, Россия
e-mail: a.kozlov@ntc-vulkan.ru, https://orcid.org/0000-0002-4310-2360

РАЗРАБОТКА ФУНКЦИИ СВЯЗЫВАНИЯ КЛЮЧЕЙ В ARX-АЛГОРИТМАХ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2021.4.05

Аннотация. В данной работе представлен анализ ARX-алгоритмов стохастического преобразования данных на основе связанных ключей. Анализ проводится по выбранному открытому тексту и связанным некоторой функцией раундовым ключам. Особым случаем применения связанных ключей является проведение анализа алгоритма, состоящего только из операций сложения по модулю 2^n, сложения по модулю 2 и циклического сдвига. Такие алгоритмы называются ARX-алгоритмами стохастического преобразования. Актуальным методом анализа на основе связанных ключей является сдвиговый анализ, который позволяет сформулировать требования только по числу операций сложения по модулю 2^n. Рассмотренные особенности этого метода показали необходимость разработки требований к ARX-алгоритмам по числу операций циклического сдвига. Исходя из особенностей математических операций, использующихся в ARX-алгоритмах, для связывания ключей предложена функция нециклического сдвига. Показано, что среди ARX-операций только функция циклического сдвига оказывает влияние на вероятность сохранения такой связи. Получена оценка сложности проведения анализа на основе связанных ключей для ARX-алгоритма в зависимости от числа операций циклического сдвига в нем. Доказано, что стойкость ARX-алгоритмов по отношению к проведению анализа на основе связанных ключей определяется минимальным из двух чисел: числа операций сложения по модулю 2^n и числа операций циклического сдвига в алгоритме.

Ключевые слова: связанные ключи, ARX-алгоритмы, стохастическое преобразование, малоресурсные алгоритмы.

Для цитирования: КОЗЛОВ, Александр А. РАЗРАБОТКА ФУНКЦИИ СВЯЗЫВАНИЯ КЛЮЧЕЙ В ARX-АЛГОРИТМАХ СТОХАСТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 63–73, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1377. DOI: http://dx.doi.org/10.26583/bit.2021.4.05.

Alexander A. Kozlov
OOO NTC «Vulkan»,
Ibragimova str., 31, 105318, Moscow, Russia
e-mail: a.kozlov@ntc-vulkan.ru, https://orcid.org/0000-0002-4310-2360

Development of a related key function in ARX stochastic data transformation algorithms

DOI: http://dx.doi.org/10.26583/bit.2021.4.05

Abstract. In this paper an analysis of ARX stochastic algorithms based on related keys is considered. Analysis based on this approach is carried out using the selected open text and the keys linked by some function. A special case of using related keys is the analysis of an algorithm consisting only of the operations of modular addition modulo 2^n, modulo 2, and cyclic shift. Such algorithms are so-called ARX stochastic algorithms. The common method of analysing the algorithms based on related keys is the rotation analysis method. This method allows formulating requirements only for the number of addition operations modulo 2^n. The considered properties of the rotation analysis method demonstrated the need to develop requirements for ARX algorithms in terms of the number of cyclic shift operations. Based on the properties of the mathematical operations used in the ARX stochastic algorithms, a non-cyclic related key function was proposed. Among ARX operations, only the cyclic shift function affects the probability of such relation. The complexity of the analysis based on non-cyclic related key function has been estimated. It is proved that the complexity of relation key analysis of ARX algorithms is determined by the

minimum of two numbers: the number of addition operations modulo 2^n and cyclic shift operations in the algorithm.

Keywords: related keys, ARX, stochastic algorithms, lightweight algorithms.
For citation: KOZLOV, Alexander A. Development of a related key function in ARX stochastic data transformation algorithms. IT Security (Russia), [S.l.], v. 28, n. 4, p. 63–73, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1377. DOI: http://dx.doi.org/10.26583/bit.2021.4.05.

Введение

Стохастическими методами защиты информации принято называть методы, обеспечивающие непредсказуемое поведение средств и объектов защиты информации [1]. Такие методы прямо или косвенно основаны на использовании генераторов псевдослучайных чисел. Они являются универсальными и могут использоваться совместно с любыми другими методами защиты информации, повышая при этом их качество. Примерами реализации стохастических методов защиты информации являются: алгоритмы блочного и поточного преобразования данных в криптографии, алгоритмы обфускации исходных кодов в области разработки программного обеспечения. Основным требованием к стохастическим алгоритмам преобразования данных в контексте защиты информации является их устойчивость по отношению к известным методам анализа их непредсказуемости.

Стохастические алгоритмы широко применяются для решения задач защиты информации, обрабатываемой в малоресурсных программно-аппаратных средах. Именно эта область применения накладывает на них дополнительные технические ограничения. В [2] отмечается, что одной из проблем при построении таких алгоритмов является одновременное соблюдение требований по их надежности и размеру аппаратной схемы, реализующей эти алгоритмы. При этом размеры схемы имеют прямую корреляцию с ее энергопотреблением – надежные алгоритмы используют в основе своих раундовых операций сложные математические преобразования, требующие существенного числа электронных компонентов для их реализации. Это приводит к большим затратам электрической мощности при их вычислении. Но требование надежности и требование низкого энергопотребления не могут быть удовлетворены одновременно.

Одним из решений может быть использование уже зарекомендовавших себя надежных стохастических алгоритмов преобразования данных, но с некоторыми изменениями в части реализации раундового преобразования или алгоритма выработки раундового ключа. К таким изменениям можно отнести, например, уменьшение числа раундов самого преобразования. Однако, это ставит вопрос о надежности полученного в итоге алгоритма под сомнение.

Другим решением может быть построение новых алгоритмов стохастического преобразования данных, учитывающих требования по скорости работы и надежности еще на этапе разработки. Если при этом для построения алгоритма используются математические операции, не требующие для своей реализации большого числа электронных компонентов, то такие алгоритмы называются малоресурсными [3]. К таким математическим операциям относятся операция сложения по модулю 2^n, операция циклического сдвига и операция сложения по модулю 2 (XOR). Алгоритмы стохастического преобразования данных, построенные исключительно на этих математических операциях, называются ARX-алгоритмами (Addition-Rotate-XOR). Такие алгоритмы являются объектом исследования данной статьи.

ARX-алгоритмы находят применение в различных прикладных технических областях. Частным случаем важнейшего приложения таких алгоритмов является построение надежным систем подвижной связи. Например, одной из проблем передачи

данных в системах земля-воздух является надежность устанавливаемого канала связи. В [4] приведены разработанные решения по обеспечению конфиденциальности и целостности передаваемых по подобным каналам данных. Такой подход получил название стохастического кодирования. Предложенные решения охватывают различные модели каналов передачи данных и базируются на использовании генератора псевдослучайных чисел в качестве источника энтропии для кодирования и обеспечения безопасности передаваемых данных одновременно. В [1] показано, как для этих целей могут быть использованы стохастические алгоритмы преобразования данных.

Кроме организации надежных каналов связи типа земля-воздух такие алгоритмы имеют серьезный потенциал для решения различных прикладных задач стохастического преобразования данных в малоресурсных аппаратных или аппаратно-программных комплексах. В [5] обозначена проблема надежной реализации облачных вычислений в области телемедицины. В [6, 7] приведен обзор приложений малоресурсных алгоритмов, в том числе ARX-алгоритмов, для решения задач Интернета вещей, который четко демонстрирует вектор развития этой области.

Частные решения по применению малоресурсных стохастических алгоритмов в уже апробированных технологиях передачи данных рассмотрены в [8, 9]. В [8] рассмотрен вопрос обеспечения защиты RFID канала передачи данных от угроз информационной безопасности, связанных с особенностями среды передачи. Позитивные результаты были получены за счет имплементации малоресурсного стохастического алгоритма преобразования данных, не вносящего существенных ограничений на полезную нагрузку протокола передачи данных. В [9] также демонстрируется решение проблемы обеспечения безопасности канала связи в среде «умных» устройств путем внедрения стохастического алгоритма в их протоколы обмена информацией.

Особо важными являются приложения ARX-алгоритмов для передачи данных в носимой технике. Носимая техника может быть частью экосистемы биомедицинских технологий [10], требования к безопасности передаваемых данных в которой продиктованы особенностями ее применения. В области одноранговых сетей также существует широкий круг приложений для таких алгоритмов [11]. Уязвимости систем связи в рассмотренных ситуациях несут в себе угрозы различной степени опасности. Решение задач обеспечения безопасности информации в таких системах, учитывая особенности их применения, требует использование малоресурсных алгоритмов стохастического преобразования данных.

Рассмотренные области применения ARX-алгоритмов позволяют сформулировать проблему их построения, связанную с исследованием их надежности. Надежность подобных алгоритмов является их приоритетным свойством. При этом ее оценка может быть обеспечена анализом сложности исследования непредсказуемости конкретного стохастического преобразования.

Широко распространенное применение в области оценки надежности имеют методы анализа, основанные на исследовании статистических свойств математических операций и их композиций, используемых в алгоритмах стохастического преобразования данных. Наибольшего внимания заслуживают универсальные методы анализа, которые могут быть применены к любому алгоритму стохастического преобразования данных вне зависимости от математических операций, составляющих его раундовую функцию преобразования. Среди таких методов можно выделить три, имеющие существенные как теоретические, так и практические результаты: методы, основанные на линейных свойствах математических операций, методы, основанные на разностных свойствах

математических операций, а также методы, основанные на модели связывания ключей конкретных стохастических алгоритмов математической функцией.

Проблема проведения линейного анализа ARX-алгоритмов стохастического преобразования данных рассматривается в [12], исследуются ограничения, вносимые каждой из ARX-операций на статистические свойства всего алгоритма. Среди ARX-операций единственной нелинейной является операция сложения по модулю 2^n. Полученные в [12] результаты определяют границы применимости подходов к анализу ARX-алгоритмов на основе линейных свойств его математических операций.

Схожие проблемы изучаются в части применения разностного подхода. В [13] рассматривается возможность построения разностных характеристик для произвольного ARX-алгоритма с помощью машинного обучения. Предложенные решения демонстрируют широкие возможности разностного подхода. На их основе могут быть получены оценки надежности ARX-алгоритмов стохастического преобразования, достаточные для обоснования требований по их построению.

Третьим эффективным подходом к анализу алгоритмов стохастического преобразования является анализ на основе связанных ключей, впервые предложенный в [14]. Идея предложенного подхода основана на практических особенностях проведения анализа стохастических алгоритмов преобразования данных. Вместо того чтобы проводить анализ по модели, для которой аналитик рассматривает только одну реализацию алгоритма, можно предположить наличие второй. Вторая реализация снижает уровень энтропии ключевой информации анализируемого алгоритма опосредованно функциональной связи между ними. Иначе говоря, анализ проводится по выбранному открытому тексту и выбранному ключу. На основе такой модели были предложены различные успешные методы проведения анализа алгоритмов стохастического преобразования. Одним из них является метод сдвигового анализа, впервые предложенный в [15].

Основной идеей метода сдвигового анализа является использование статистических свойств открытых текстов, связанных функцией циклического сдвига. Использование функции циклического сдвига для связывания ключей позволило продемонстрировать потенциал предложенного метода. В качестве практического приложения полученных результатов была представлена оценка надежности алгоритма Threefish. Однако, полученные в [15] результаты оставляют ряд вопросов, связанных с требованиями к числу ARX-операций в надежных стохастических алгоритмах преобразования данных.

Проблемой ARX-алгоритмов стохастического преобразования является использование такого числа ARX-операций, при котором сохраняется существенная вероятностная связь входных и выходных слов алгоритма. Метод сдвигового анализа позволяет сформулировать требования к числу операций сложения по модулю 2^n в алгоритме, при котором такая вероятностная связь будет неотличима от равновероятной, и проведение подобного анализа будет невозможно. Однако требования по числу операций циклического сдвига в ARX-алгоритме стохастического преобразования по отношению к анализу на основе связанных ключей на текущий момент отсутствуют.

Целью данной работы является разработка новой функции связывания ключей ARX-алгоритмов стохастического преобразования, позволяющей сформулировать требования на число операций циклического сдвига для обеспечения их надежности.

1. Метод сдвигового анализа

Рассмотрим процесс исследования ARX-алгоритма стохастического преобразования

методом сдвигового анализа. Характерной для него является аналитическая позиция, предполагающая выбор пар открытых текстов и функции связывания ключей *F*. Основной идеей метода является рассмотрение в качестве входных слов ARX-алгоритма таких пар, которые связаны друг с другом функцией циклического сдвига. Аналитические свойства метода обеспечивает именно выбор функции связывания ключей.

Ключевой величиной для рассматриваемого метода проведения анализа является оценка вероятности распространения связанных выбранной операцией циклического сдвига пар открытого текста через раундовые операции стохастического преобразования. Свойства функции циклического сдвига в приложении к ARX-операциям используются для получения значимых статистических данных. В [15] рассматриваются все три ARX-операции с точки зрения их циклических свойств, дается оценка вероятности на распространение циклических пар через каждую из них. Обратимся к полученным результатам анализа. Для этого рассмотрим циклические свойства каждой из этих операций.

Пусть на вход некоторой ARX-операции поступают произвольные входные слова $X = \{x_1, x_2, ..., x_n\}$ и $Y = \{y_1, y_2, ..., y_n\}$. Для операции сложения по модулю 2 в [15] была получена следующая оценка вероятности распространения сдвиговых пар (X, Y) и (X, Y):

$$\text{Prob}(X \oplus Y = X \oplus Y) = 1. \quad (1)$$

При этом важно отметить, что оценка (1) не зависит от величины циклического сдвига в функции *F*. Именно это свойство используется в [15] для получения оценки вероятности распространения циклически связанных пар через полноценные ARX-алгоритмы.

В [15] была получена также оценка вероятности распространения таких же сдвиговых пар через операцию циклического сдвига, эта оценка справедлива для любого значения величины сдвига *r*, а именно:

$$\text{Prob}(X_{>>>r} = X_{>>>r}) = 1, \quad (2)$$

где $X = X_{>>>r}$, $Y = Y_{>>>r}$ – операции циклического сдвига на *r* разрядов вправо. При этом, полученная оценка (2) также не зависит от величины циклического сдвига в самой функции *F*.

Наконец рассмотрим результаты, полученные для третьей ARX-операции – операции сложения по модулю 2^n. Для этой математической операции в [15] была получена оценка вероятности, имеющая четкую статистическую зависимость от величины циклического сдвига в функции связывания ключей. Для циклически связанных пар было получено:

$$\text{Prob}(X + Y = X + Y) = \frac{1}{4}(1 + 2^{r-n} + 2^{-r} + 2^{-n}). \quad (3)$$

Рассмотренные в [15] операции являются единственными математическими операциями, используемыми в ARX-алгоритмах. Обеспеченная таким образом полнота исследования сдвиговых свойств ARX-операций позволила сформулировать требования на число операций сложения по модулю 2^n в надежных ARX-алгоритмах.

Проведение сдвигового анализа предполагает вычисление оценки вероятности наличия связи по функции *F* выходных сдвиговых пар анализируемого алгоритма. Любой ARX-алгоритм можно рассматривать как композицию некоторого числа операций сложения по модулю 2, операций сложения по модулю 2^n и операций циклического сдвига. На основании (1) и (2) в [15] было доказано, что операции сложения по модулю 2 и операции циклического сдвига не влияют на эту функциональную связь.

Операцией, оказывающей статистически значимое влияние на связь выходных сдвиговых пар через функцию F, является операция сложения по модулю 2^n. Исходя из результатов оценки вероятности для этой операции (3), в [15] было доказано, что вероятность сохранения функциональной связи между сдвиговыми парами слов снижается всякий раз при прохождении через операцию сложения по модулю 2^n не меньше чем на 3/8. При этом такое уменьшение вероятности достигается при граничном значении циклического сдвига, используемом для обеспечения сдвиговой связи пар входных слов анализируемого алгоритма, – циклическом сдвиге на 1.

Полученная в [15] оценка в контексте проблемы построения надежных ARX-алгоритмов стохастического преобразования данных четко определяет требование по числу операций сложения по модулю 2^n в них. В итоге, имея численное выражение зависимости оценки вероятности каждой из ARX-операций относительно метода сдвигового анализа, можно утверждать, что сложность проведения такого анализа зависит только от числа операций сложения по модулю 2^n, используемых в алгоритме стохастического преобразования, и не зависит от числа операций сложения по модулю 2 и операций циклического сдвига в нем.

Отметим, что рассмотренный метод сдвигового анализа не накладывает какие-либо ограничения на число операций циклического сдвига в ARX-алгоритмах. При этом, как будет показано далее, корреляция числа операций циклического сдвига с числом операций сложения по модулю 2^n в исследуемом алгоритме является значимой в части оценки его надежности. Если стохастический алгоритм преобразования данных имеет достаточное число операций сложения по модулю 2^n для обеспечения его стойкости по отношению к сдвиговому анализу, это не дает информации о его стойкости по отношению к анализу по модели связанных ключей в общем. Возможность применения анализа на основе связанных ключей к алгоритмам, стойким по отношению к сдвиговому анализу, является предметом исследования данной статьи.

2. Новая функция связывания ключей

Рассмотренный метод сдвигового анализа позволил по-новому взглянуть на проблему применимости подхода на основе связанных ключей к ARX-алгоритмам. Однако, имеющиеся в соответствии с этим методом результаты формируют ограничения только на число операций сложения по модулю 2^n. Источником этих ограничений в методе сдвигового анализа является выбранная функция связи ключей. Для обеспечения возможности формирования требований к числу операций циклического сдвига в надежных ARX-алгоритмах требуется выбрать такую функцию связывания ключей, которая накладывает именно на нее значимые статистические ограничения.

Рассмотрим в качестве такой функции связывания ключей $F(x) = 2x \mod 2^n$, $n \in Z$. Для данной функции последовательно проведем анализ свойств каждой из ARX-операций относительно возможности сохранения функциональной связи по F между произвольными входными парами слов после выполнения этих математических операций. В начале докажем оценку вероятности сохранения связи по F для операции сложения по модулю 2^n.

Утверждение 1. $\mathrm{Prob}(F(x)+F(y)=F(x+y))=1,\ \forall x,\ y \in Z_2^n,\ n \in Z$, где $"+"$ – операция сложения по модулю 2^n.

Доказательство. Пусть на вход операции сложения по модулю 2^n поступает пара $x, y \in Z_2^n$. Тогда $F(x)+F(y)=(2x+2y) \mod 2^n$. В то же время $F(x+y)=2(x+y) \mod 2^n=(2x+2y) \mod 2^n=F(x)+F(y)$.

Доказанное утверждение демонстрирует отсутствие влияния операции сложения по модулю 2^n на выбранную функциональную связь для любых пар входных слов.

Аналогичным свойством обладает операция сложения по модулю 2.

Утверждение 2. $\text{Prob}(F(x) \oplus F(y) = F(x \oplus y)) = 1,\ \forall x,\ y \in Z_2^n,\ n \in Z.$

Доказательство. Пусть на вход операции XOR поступает пара $x, y \in Z_2^n$, $x = (x_{n-1}, x_{n-2}, ...x_0),\ y = (y_{n-1}, y_{n-2}, ...y_0),\ x \oplus y = z,\ \ z = (y_{n-1} \oplus x_{n-1}, ...y_0 \oplus x_0)$. Тогда:

$$F(x) \oplus F(y) = (2x \oplus 2y) = x \oplus y = z, \tag{4}$$

где $x = (x_{n-2}, ...x_0, 0),\ y = (y_{n-2}, ...y_0, 0),\ z = (y_{n-2} \oplus x_{n-2}, ...y_0 \oplus x_0, 0).$

В то же время $F(x \oplus y) = 2(x \oplus y) \mod 2^n = 2z = z$.

Единственной ARX-операцией, имеющей статистическое влияние на пары входных слов, связанные через выбранную функцию *F*, является операция циклического сдвига. В этом случае предпосылка выбора функции связи ключей совпадает с полученным теоретическим результатом.

Утверждение 3. $\text{Prob}(F(x)_{>>>r} = F(x_{>>>r})) = \frac{1}{4},\ \forall x \in Z_2^n,\ n,\ r \in Z.$

Доказательство. Пусть на вход операции циклического сдвига поступает $x \in Z_2^n$, $x = (x_{n-1}, x_{n-2}, ...x_0)$. Тогда:

$$F(x)_{<<<r} = x, \tag{5}$$

где $x = (x_{n-2-r}, ...x_0, 0, x_{n-2}, ...x_{n-r+1}, x_{n-r}, x_{n-r-1})$.

В то же время

$$F(x_{<<<r}) = x, \tag{6}$$

где $x = (x_{n-2-r}, ...x_0, x_n, ...x_{n-r+1}, x_{n-r}, 0).$

Из (5) и (6) видно, что $x \equiv x$ только в том случае, когда $x_{n-r-1} = 0$ и $x_n = 0$. Отсюда следует доказываемое утверждение.

Замечание. Полученная оценка вероятности распространения функции $F(x) = 2x \mod 2^n$ через операцию циклического сдвига совпадает с оценкой максимального значения вероятности распространения функции, используемой в сдвиговом анализе для связывания ключей через операцию сложения по модулю 2^n. Оценка вероятности распространения функции $F(x) = 2x \mod 2^n$ через операции сложения по модулю 2^n и XOR также совпадает с оценкой вероятности распространения функции, используемой в сдвиговом анализе для связывания ключей через операции XOR и циклического сдвига, и равна 1. Полученная корреляция с результатами сдвигового анализа является важной и, как будет показано далее, может быть использована для конструктивного наложения требований к стойким по отношению к анализу на основе связанных ключей ARX-алгоритмам стохастического преобразования.

Утверждения 1–3 показывают, что выбранная функция связи ключей имеет статистические свойства, которые могут позволить провести анализ ARX-алгоритмов. Такой анализ может быть проведен за счет оценки вероятности распространения связанных функцией *F* входных пар через конкретный анализируемый алгоритм. Для этого докажем утверждение о сложности проведения анализа ARX-алгоритмов по методу

связанных ключей при использовании в качестве функции связывания ключей функции $F(x) = 2x \mod 2^n$.

Утверждение 4. Рассмотрим ARX-алгоритм стохастического преобразования *arx*. Пусть известно, что число операций циклического сдвига в нем равно *R*. Тогда такой алгоритм может быть проанализирован по методу связанных ключей с функцией связывания ключей $F(x) = 2x \mod 2^n$, если $R < \frac{n}{2}$.

Доказательство. Проведение анализа на основе связанных ключей подразумевает использование пар открытого текста $(F(c), c),\ c \in Z_2^n$. При этом для таких пар исследуется оценка вероятности выполнения соотношения

$$arx_F(F(c)) = arx(c), \tag{7}$$

где arx_F – это алгоритм arx, раундовые ключи которого связаны с ключами алгоритма arx функцией *F*.

Согласно утверждениям 1 и 2, вероятность выполнения соотношения (7) не меняется после применения к *c* и $F(c)$ соответственно операции сложения по модулю 2^n и операции XOR вне зависимости от числа этих операций и их последовательности.

Из утверждения 3 имеем, что для любой операции циклического сдвига в исследуемом алгоритме $\forall x \in Z_2^n \ \ \mathrm{Prob}(F(x)_{>>>r} = F(x_{>>>r})) = \frac{1}{4}$. Это означает, что каждый раз при прохождении связанных функцией *F* слов через операцию циклического сдвига вероятность того, что на выходе слова также будут связаны, понижается на $\frac{1}{2^2}$. Для произвольной функции связывания $P: Z_2^n \to Z_2^n$, для произвольного $x \in Z_2^n$ вероятность выполнения соотношения $arx_p(P(x)) = arx(x)$ равна $\frac{1}{2^n}$. Проведение анализа возможно только в случае, если соотношение (7) выполняется с вероятностью, отличной от случая произвольной функции связывания. Отсюда получаем условие на проведение анализа:

$$\frac{1}{2^{2R}} > \frac{1}{2^n}. \tag{8}$$

Полученная оценка на число операций циклического сдвига позволяет различать надежные и ненадежные ARX-алгоритмы в контексте рассматриваемого метода анализа. Используя ее, а также рассмотренные результаты для метода сдвигового анализа, можно усилить существующие требования по числу операций в ARX-алгоритмах стохастического преобразования. Для этого докажем следующее утверждение.

Утверждение 5. Стойкость ARX-алгоритмов по отношению к проведению анализа на основе связанных ключей определяется минимальным из двух чисел: числа операций сложения по модулю 2^n и числа операций циклического сдвига в алгоритме.

Доказательство. Всего имеется 3 возможных случая. Пусть в ARX-алгоритме стохастического преобразования число операций сложения по модулю 2^n больше, чем число операций циклического сдвига. Тогда можно воспользоваться сдвиговым анализом.

Пусть в ARX-алгоритме стохастического преобразования число операций циклического сдвига больше, чем число операций сложения по модулю 2^n. Тогда можно воспользоваться анализом на основе связанных ключей с функцией

связывания ключей $F(x) = 2x \mod 2^n$.

Если в ARX-алгоритме стохастического преобразования число операций сложения по модулю 2^n совпадает с числом операций циклического сдвига, то тогда анализ на основе связанных ключей с функцией связывания ключей $F(x) = 2x \mod 2^n$ и сдвиговый анализ дают в худшем случае одинаковую оценку на сложность проведения анализа подобного алгоритма.

Заключение

В данной работе была исследована проблема построения надежных ARX-алгоритмов стохастического преобразования данных, которые имеют широкое применение в различных областях жизнедеятельности: медицина, ЖКХ, умный дом, умный город. Каждая из рассмотренных прикладных областей имеет свою специфику, но при этом их всех объединяет требование по безопасности обрабатываемых данных.

С целью исследования надежности ARX-алгоритмов был рассмотрен подход к исследованию их непредсказуемости на основе связанных ключей по методу сдвигового анализа. Результаты исследования показали наличие объективных особенностей этого метода, опосредованных выбором функции связывания ключей – операцией циклического сдвига. Использование такой функции позволяет составить требования к надежным ARX-алгоритмам стохастического преобразования только в отношении числа операций сложения по модулю 2^n.

С учетом особенностей математических операций, использующихся в ARX-алгоритмах, была предложена новая функция для связывания ключей. В качестве этой функции была выбрана $F(x) = 2x \mod 2^n$. Для новой функции связывания ключей исследованы ее математические свойства.

Для операции сложения по модулю 2 и сложения по модулю 2^n были получены оценки вероятности распространения связанных выбранной функцией F пар входных слов. Данный результат позволяет сделать вывод об отсутствии влияния на выбранную функциональную связь между произвольными парами входных слов для этих математических операций. Для операции циклического сдвига проведенные исследования показали наличие существенного ее влияния на вероятность распространения связанных пар входных слов. Проведенный анализ позволил доказать оценку снижения вероятности сохранения выбранной функциональной связи между произвольными парами входных слов после прохождения этой операции. Было доказано, что вероятность сохранения функциональной связи F между парами входных слов снижается всякий раз при прохождении через операцию циклического сдвига на 1/4. Используя эту оценку, было доказано, что стойкость ARX-алгоритмов по отношению к проведению анализа на основе связанных ключей определяется минимальным из двух чисел: числа операций сложения по модулю 2^n и числа операций циклического сдвига в алгоритме.

СПИСОК ЛИТЕРАТУРЫ:

1. Иванов М.А. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи. Вопросы кибербезопасности. 2019. №3(31). С 45–50. DOI: http://dx.doi.org/10.21681/2311-3456-2019-3-45-50.
2. Жуков А.Е. Легковесная криптография. Часть 1. Вопросы кибербезопасности. 2015. №1(9). С. 23–46. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_09_04.pdf (дата обращения: 02.10.2021).
3. Жуков А.Е. Легковесная криптография. Часть 2. Вопросы кибербезопасности. 2015. №2(10). С. 2–10. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_10_01.pdf (дата обращения: 02.10.2021).
4. Осмоловский С.А. Стохастическая информатика: инновации в информационных системах. М.: Горячая линия-Телеком, 2011. – 320 с.

5. AbdulRaheem M. et al. (2021) An Enhanced Lightweight Speck System for Cloud-Based Smart Healthcare. In: Florez H., Pollo-Cattaneo M.F. (eds) Applied Informatics. ICAI 2021. Communications in Computer and Information Science, vol 1455. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-89654-6_26.
6. Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 (2021). DOI: https://doi.org/10.1007/s42452-021-04156-9.
7. Alahdal, Abdulrazzaq and Deshmukh, Nilesh K., A Systematic Technical Survey of Lightweight Cryptography on IoT Environment (MARCH 03, 2020). International Journal of Scientific & Technology Research. Vol. 9, Issue 3, March 2020. URL: https://ssrn.com/abstract=3739014 (дата обращения: 24.11.2021).
8. G. Ramu, Z. Mishra and B. Acharya. Hardware implementation of Piccolo Encryption Algorithm for constrained RFID application, 2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON), 2019. P. 85–89. DOI: http://dx.doi.org/10.1109/IEMECONX.2019.8877071.
9. Girija, M., Manickam, P. & Ramaswami, M. PriPresent: an embedded prime LightWeight block cipher for smart devices. Peer-to-Peer Netw. Appl. 14, 2462–2472 (2021). DOI: https://doi.org/10.1007/s12083-020-00992-5.
10. Jabeen, T., Ashraf, H. & Ullah, A. A survey on healthcare data security in wireless body area networks. J Ambient Intell Human Comput 12, 9841–9854 (2021). DOI: https://doi.org/10.1007/s12652-020-02728-y.
11. Gautam, A.K., Kumar, R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Appl. Sci. 3, 50 (2021). DOI: https://doi.org/10.1007/s42452-020-04089-9s.
12. Козлов Александр А.; Иванов, Михаил А. Исследование возможности применения линейного анализа к ARX алгоритмам стохастического преобразования данных в зависимости от функции смешения с раундовым ключом. Безопасность информационных технологий, [S.l.]. Т. 28, № 2. С. 62–69, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.2.06.
13. Wang G., Wang G. (2021) Improved Differential-ML Distinguisher: Machine Learning Based Generic Extension for Differential Analysis. In: Gao D., Li Q., Guan X., Liao X. (eds) Information and Communications Security. ICICS 2021. Lecture Notes in Computer Science, vol 12919. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-88052-1_2.
14. Biham E. New types of cryptanalytic attacks using related keys. J. Cryptology 7, 229–246 (1994). DOI: https://doi.org/10.1007/BF00203965.
15. Khovratovich D., Nikolić I. (2010) Rotational Cryptanalysis of ARX. In: Hong S., Iwata T. (eds) Fast Software Encryption. FSE 2010. Lecture Notes in Computer Science, vol 6147. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-13858-4_19.

REFERENCES:

[1] Ivanov M.A. A way to ensure universal protection of information transmitted via communication channels. Cybersecurity Issues. 2019. No 3(31). P. 45–50. DOI: http://dx.doi.org/10.21681/2311-3456-2019-3-45-50 (in Russian).
[2] Zhukov A.E. Lightweight Cryptography. Part 1. Cybersecurity Issues. 2015. No 1(9). P. 23–46. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_09_04.pdf (accessed: 02.10.2021) (in Russian).
[3] Zhukov A.E. Lightweight Cryptography. Part 2. Cybersecurity Issues. 2015. No 2(10). P. 2–10. URL: https://cyberrus.com/wp-content/uploads/2015/05/vkb_10_01.pdf (accessed: 02.10.2021) (in Russian).
[4] Osmolovskij S.A. Stohasticheskaya informatika: innovacii v informacionnyh sistemah. M.: Goryachaya liniya-Telekom, 2011. – 320 p. (in Russian).
[5] AbdulRaheem M. et al. (2021) An Enhanced Lightweight Speck System for Cloud-Based Smart Healthcare. In: Florez H., Pollo-Cattaneo M.F. (eds) Applied Informatics. ICAI 2021. Communications in Computer and Information Science, vol 1455. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-89654-6_26.
[6] Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 (2021). DOI: https://doi.org/10.1007/s42452-021-04156-9.
[7] Alahdal, Abdulrazzaq and Deshmukh, Nilesh K., A Systematic Technical Survey of Lightweight Cryptography on IoT Environment (MARCH 03, 2020). International Journal of Scientific & Technology Research. Vol. 9, Issue 3, March 2020. URL: https://ssrn.com/abstract=3739014 (accessed: 24.11.2021).
[8] G. Ramu, Z. Mishra and B. Acharya. Hardware implementation of Piccolo Encryption Algorithm for constrained RFID application, 2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON), 2019. P. 85–89. URL: 10.1109/IEMECONX.2019.8877071.
[9] Girija, M., Manickam, P. & Ramaswami, M. PriPresent: an embedded prime LightWeight block cipher for smart devices. Peer-to-Peer Netw. Appl. 14, 2462–2472 (2021). DOI: https://doi.org/10.1007/s12083-020-00992-5.

[10] Jabeen, T., Ashraf, H. & Ullah, A. A survey on healthcare data security in wireless body area networks. J Ambient Intell Human Comput 12, 9841–9854 (2021). DOI: https://doi.org/10.1007/s12652-020-02728-y.
[11] Gautam, A.K., Kumar, R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Appl. Sci. 3, 50 (2021). DOI: https://doi.org/10.1007/s42452-020-04089-9s.
[12] Kozlov Alexander A.; Ivanov Mikhail A. The possibility of applying linear analysis to the ARX stochastic algorithms depending on round key functions. IT Security (Russia), [S.l.]. Vol. 28, № 2. P. 62–69, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.2.06 (in Russian).
[13] Wang G., Wang G. (2021) Improved Differential-ML Distinguisher: Machine Learning Based Generic Extension for Differential Analysis. In: Gao D., Li Q., Guan X., Liao X. (eds) Information and Communications Security. ICICS 2021. Lecture Notes in Computer Science, vol 12919. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-88052-1_2.
[14] Biham, E. New types of cryptanalytic attacks using related keys. J. Cryptology 7, 229–246 (1994). DOI: https://doi.org/10.1007/BF00203965.
[15] Khovratovich D., Nikolić I. (2010) Rotational Cryptanalysis of ARX. In: Hong S., Iwata T. (eds) Fast Software Encryption. FSE 2010. Lecture Notes in Computer Science, vol 6147. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-13858-4_19.

Поступила в редакцию – 11 июля 2021 г. Окончательный вариант – 01 декабря 2021 г.
Received – July 11, 2021. The final version – December 01, 2021.