Построение Стойкой Асимметричной Криптосистемы на Основе Конечных Автоматов

Сирануш Чопурян

Государственный Инженерный
Университет Армении
(Политехник)
Ереван, Армения
e-mail: siranush.ch@gmail.com

АННОТАЦИЯ

В статье детально анализированы существующие асимметричные криптосистемы на основе конечных автоматов. Представлены методы криптоанализа асимметричных криптосистем на основе конечных автоматов с использованием атак, специфичных для данного класса криптосистем. В результате спроектирована улучшенная асимметричная криптосистема, которая может противостоять представленным атакам. Стойкая асимметричная криптосистема строится на основе генерирования, удовлетворяющего требованиям линейного и нелинейного конечных автоматов, которые можно инвертировать.

Ключевые слова

Асимметричная криптосистема, криптоанализ, теория автоматов.

1. ВВЕДЕНИЕ

Асимметричные криптосистемы, которые обсуждаются в настоящей статье, основаны на теории автоматов. В асимметричной криптосистеме на основе конечных автоматов открытый ключ является композицией нелинейного и линейного конечных автоматов, которые легко можно инвертировать. Секретный ключ – это особая комбинация полученных инверсных автоматов.

Известно, что непосредственное инвертирование конечного автомата шифрования является трудноразрешимой задачей [1,2]. С другой стороны, при применении алгебраической теории автоматов компонентные автоматы открытого ключа, а так же их инверсные автоматы, могут быть легко вычислены [3].

В статье исследуются недостатки криптосистем при атаках на основе выбранного открытого текста в случае использования не нелинейного и линейного автоматов. С целью повышения стойкости асимметричных криптосистем на основе конечных автоматов предлагается метод генерации, удовлетворяющий требованиям линейного и нелинейного автоматов

Показывается уязвимость асимметричных криптосистем на основе конечных автоматов также по отношению к атакам методом полного перебора. Это возможно, когда противнику известно окончание открытого текста. В статье предлагается способ воспрепятствования атак методом полного перебора.

2. ЛЕГКОИНВЕРТИРУЕМЫЕ ЛИНЕЙНЫЕ АВТОМАТЫ

Конечный автомат представляется в виде пяти обьектов $M_l =< X, Y, S_l, \delta_l, \lambda_l >$, где X – конечное непустое множество входных сигналов, называемое входным алфавитом, Y - конечное непустое множество выходных сигналов, называемое выходным алфавитом, S_l - конечное непустое множество состояний, $\delta_l : S_l \times X \to S_l$ - функция переходов и $\lambda_l : S_l \times X \to Y$ - функция выходов. X и Y являются l-мерными линейными пространствами над полем GF(2)={0,1}. Если $y(i) \in Y$ – это выходной элемент в момент i, а $x(i) \in X$ – это вектор-столбец, тогда автомат M_l может быть представлен следующим образом:

$$y(i) = \sum_{j=0}^{\tau} A_j x(i-j) + \sum_{j=1}^{t} B_j y(i-j), \quad i = 0,1,2,\ldots \quad (1)$$

Конечный автомат M_l является конечным автоматом с памятью порядка <τ, t>, т.е. для определения исходного состояния необходимо знание покрайней мере последних τ входных и t выходных элементов. Совокупность $< x(-1), x(-2), \ldots, x(-\tau), y(-1), y(-2), \ldots, y(-t) >$ представляет из себя исходное состояние конечного автомата M_l.

В формуле (1) A_j и B_j (j=0,1,2,…,τ) являются $l \times l$ линейные коэффициентные матрицы, которые однозначно определяют конечный автомат M_l. Операции, использованные в формуле (1) – это обычное суммирование и умножение над полем GF(2).

Конечный автомат M_l, который определен по формуле (1), называется линейным автоматом. [4]

Далее мы рассмотрим автомат M_l как линейный конечный автомат, который зависит только от τ количества входных элементов и определяется по формуле (2).

$$y(i) = A_0 x(i) + A_1 x(i-1) + \cdots + A_\tau x(i-\tau), \qquad i = 0,1,2,\ldots \quad (2)$$

Утверждение: Конечный автомат M_l является легко инвертируемым конечным автоматом с задержкой τ тогда и только тогда, когда из набора матриц A_j (j=0,1,2,…,τ) можно извлечь набор матриц $A_0^{-1}, A_1^{-1}, \ldots, A_\tau^{-1}, \tilde{A}_0^{-1}, \tilde{A}_1^{-1}, \ldots, \tilde{A}_\tau^{-1}$, для которых верно следующее равенство:

$$x(i) = \sum_{j=0}^{\tau} A_j^{-1} y(i+j) + \sum_{j=1}^{t} \tilde{A}_j x(i-j), \quad i = 0,1,2,\ldots \quad (3)$$

Для произвольного состояния $s = < x(-1), x(-2), \ldots, x(-\tau) >$ конечного автомата M_l и для произвольной входной последовательности $x(0), x(1), \ldots, x(n+\tau) \in X$, если $y(0)y(1)\cdots y(n+\tau) = \lambda(x(0)x(1)\cdots x(n+\tau))$, входные элементы $x(0), x(1), \ldots, x(n)$ могут быть однозначно вычислены по формуле (3).

Следовательно, конечный автомат, определенный по формуле (3), точно определяет легкий инверсный автомат конечного автомата M_l с задержкой τ.

3. ЛЕГКО ИНВЕРТИРУЕМЫЕ НЕЛИНЕЙНЫЕ АВТОМАТЫ

Нелинейный автомат представляется в виде набора пяти компонентов $M_{nl} =< X, Y, S_{nl}, \delta_{nl}, \lambda_{nl} >$, где X – входной алфавит, Y – выходной алфавит, S_{nl} – алфавит состояний, $\delta_{nl} : S_{nl} \times F(X) \to S_{nl}$ - функция переходов, а $\lambda_{nl} : S_{nl} \times F(X) \to Y$ - функция выходов. X и Y являются l-мерными линейными пространствами над полем GF(2)={0,1}, и функция F(X) отображает нелинейную операцию, определенную над полем GF(2). Формула, определяющая автомат M_{nl}, представляет:

$$y(i) = \sum_{j=0}^{r} B_j x(i-j) + \sum_{j=1}^{r-1} \widetilde{B}_j x(i-j) \circ x(i-j-1), \quad i = 0,1,2,\ldots \quad (4)$$

где $B_j\ (j = 0,1,2...,r)$ и $\widetilde{B}_j\ (j = 1,2...,r-1)$ являются $l \times l$ коэффициентные метрици над полем GF(2), и B_0 является инвертируемый матрицой.

Автомат M_{nl}, определенной по формуле (4), является конечным автоматом с памятю, зависевший от r количества входных элементов. Так как существует матрица B_0^{-1}, то формула определяющая автомат M_{nl}^{-1} будет иметь вид:

$$x(i) = B_0^{-1}(y(i) + \sum_{j=0}^{r} B_j x(i-j) + \sum_{j=1}^{r-1} \widetilde{B}_j x(i-j) \circ x(i-j-1), \quad i = 0,1,2... \quad (5)$$

Конечный автомат M_{nl}^{-1}, зависевший от r количества выходных элементов, из себя представляет несложный инверсный автомат задержкой 0 конечного автомата M_{nl}. Для прозволного начального состояния $s =< x(-1), x(-2), \ldots, x(-r) >$ конечного автомата M_{nl} существует состояние s' конечного автомата M_{nl}^{-1}, такой, что $\lambda'_{nl}(s', \lambda_{nl}(s, x)) = x$, где s' является состояние совподения s и так же определяется от множество $< x(-1), x(-2), \ldots, x(-r) >$.

4. ОСНОВНОЙ ПРИНЦИП ПОСТРОЕНИЯ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА ОСНОВЕ КОНЕЧНЫХ АВТОМАТОВ

Для проектирования асимметричной криптосистемы на основе конечных автоматов предлагается пара конечных автоматов. В паре конечных автоматов один является нелинейным легкоинвертируемым конечным автоматом с задержкой 0, а другой – линейным легкоинвертируемым конечным автоматом с задержкой τ. Обозначим через M_{nl} и M_l нелинейный и линейный автоматы соотвественно, композиция которых представляет из себя автомат шифрования. Композиционный автомат $M = M_{nl} \circ M_l$ также является нелинейным легкоинвертируемым конечным автоматом с задержкой $0+\tau=\tau$ [4].

Дешифрование прозводится с помощью автоматов M_{nl}^{-1} и M_l^{-1}, первый из которых является легким инверсным автоматом M_{nl} с задержкой 0, а второй - легким инверсным автоматом M_l с задержкой τ. Композиционный конечный автомат M является открытым ключом асимметричной криптосистемы на основе конечных автоматов, а конечные автоматы M_l^{-1}, M_{nl}^{-1} и порядок их соединения являются секретным ключом.

Асимметричная криптосистема на основе конечных автоматов работает следующим образом:

1. Сначала создаются два конечных автомата M_{nl} и M_l по вышеизложенному.
2. Подставляя Формулу (2) в Формулу (4), строится композиционный автомат $M = M_{nl} \circ M_l$.

Формула, определяющая конечный автомат M, будет переписана таким образом:

$$z(i) = \sum_{t=0}^{\tau} A_t \left(\sum_{j=0}^{r} B_j x(i-j-t) + \sum_{j=1}^{r-1} \widetilde{B}_j x(i-j-t) \circ x(i-j-t-1) \right), \quad i = 0,1,2... \quad (6)$$

Операцию $M_{nl} \circ M_l$ не нужно путать с обыкновенным умножением полиномов - $M_{nl} \cdot M_l$.

Каждое состояние конечного автомата $M = M_{nl} \circ M_l$ эквивалентно состоянию $< s_{nl}, s_l >$, где $s_{nl} =< x(-1), x(-2), \ldots, x(-r) >$ и $s_l =< y(-1), y(-2), \ldots, y(-\tau) >$ являются состояниями конечных автоматов M_{nl} и M_l соответственно.

Формула (6) в упрощенном виде будет выглядеть:

$$z(i) = \sum_{j=0}^{r+\tau} C_j x(i-j) + \sum_{j=1}^{r+\tau-1} \widetilde{C}_j x(i-j) \circ x(i-j-1), \quad i = 0,1,2... \quad (7)$$

где

$$C_j = \sum_{\substack{t=0 \\ j=0}}^{\substack{t=\tau \\ j=r}} A_t B_j, \qquad \widetilde{C}_j = \sum_{\substack{t=0 \\ j=1}}^{\substack{t=\tau \\ j=r-1}} A_t \widetilde{B}_j, \quad (8)$$

$l \times l$-мерные матричные полиномы над полем GF(2), которые однозначно определяют конечный автомат M.

Автомат M делается открытым для всех.

3. Строятся инверсные автоматы M_{nl}^{-1}, M_l^{-1}, которые держатся в секрете.

4. Берется произвольная последовательность $x(m+1)x(m+2)\ldots x(m+\tau)$, для того чтобы шифровать открытый текст $x(0)x(1)\ldots x(m)$. Произвольная последовательность добавляется с конца открытого текста, и полученная последовательность $x(0)x(1)\ldots x(m+\tau)$ дается на вход автомата $M = M_{nl} \circ M_l$ с начального состояния s.

На выходе автомата M получается шифрованный текст $z(0)z(1)\ldots z(m+\tau)$.

5. Для дешифрования шифрованного текста $z(0)z(1)\ldots z(m+\tau)$ сначала используется автомат M_l^{-1} с начального состояния s_l. Текст $y(0)y(1)\ldots y(m)$, полученный на выходе автомата M_l^{-1}, подается на вход автомата M_{nl}^{-1} с начального состояния s_{nl} для получения открытого текста $x(0)x(1) \ldots x(m)$ на выходе.

Описанную асимметричную криптосистему на основе конечных автоматов можно взломать:
1) решив Формулу (4) над полем GF(2);
2) методом полного перебора открытого текста от его конца к началу [5].
Методы взлома и их предотвращение представлены в следующих главах.

5. АТАКА НА ОСНОВЕ ВЫБРАННОГО ОТКРЫТОГО ТЕКСТА

Недостатки асимметричных криптосистем против атак выбраного открытого текста обусловлены использованием нелинейного легкоинвертируемого конечного автомата с задержкой 0 и линейного легкоинвертируемого конечного автомата с задержкой τ.
Атака выбранного открытого текста на асимметричную криптосистему на основе конечных автоматов приводится к задаче решения системы нелинейных уравнений в виде Формулы (6) над полем GF(2). Последняя известна как трудноразрешимая задача при большом количестве аргументов.
Количество аргументов в Формуле (6) можно увеличить, увеличивая задержку τ конечного автомата шифрования.
τ задержка конечного автомата шифрования равна $\tau=0+\tau$, где 0 – задержка нелинейного компонентного автомата, а τ - задержка линейного компонентного автомата.
Первый способ увеличить τ задержку автомата шифрования - это заменить нелинейный компонентный автомат с легкоинвертируемым нелинейным конечным автоматом с задержкой τ_1. Второй способ – сделать задержку слабоинвертируемого линейного автомата длительней, добавляя новые состояния к множеству состояний автомата.

5.1. Модификация нелинейного автомата

Автомат M_{nl} определяется по формуле

$$y(i)=\sum_{j=0}^{r} B_j x(i-j)+\sum_{j=1}^{r-1} \widetilde{B}_j x(i-j)\circ x(i-j-1),$$

где $B_j\ (j=0,1,2...,r)$ и $\widetilde{B}_j\ (j=1,2...,r-1)$ являются 1×1 коэффициентными матрицами над полем GF(2), и B_0 – инвертируемой матрицей. Операция ° представляет из себя нелинейную операцию, определенную над полем GF(2).
Легкоинвертируемый нелинейный автомат с задержкой 0 модифицируется к легкоинвертируемому нелинейному автомату с задержкой τ, переопределяя операцию ° над полем GF(2). Определяющая формула автомата будет иметь вид:

$$y(i)=\sum_{j=0}^{r} B_j x(i-j)+\sum_{j=1}^{r+\tau} \widetilde{B}_j x(i-j)\circ\cdots\circ x(i-j-\tau)$$

$$i=0,1,2... \quad (7)$$

Очевидно, что M_{nl} теперь является легкоинвертируемым нелинейным автоматом с задержкой τ. Формулу (6) можно переписать следующим образом:

$$z(i)=\sum_{j=0}^{r+\tau} C_j x(i-j)+\sum_{j=1}^{r+2\tau} \widetilde{C}_j x(i-j)\circ\cdots\circ x(i-j-\tau),$$

$$i=0,1,2... \quad (8)$$

5.1. Модификация линейного автомата

С целью увеличения задержки линейного автомата M_1, между двумя состояниями автомата добавляются новые состояния.
В результате полученный автомат является эквивалентным начальному автомату согласно ***Определению 1***.
Определение 1. Пускай $M_1=<X,Y,S_1,\delta_1,\lambda_1>$ и $M_2=<X,Y,S_2,\delta_2,\lambda_2>$ являются парой конечных автоматов. Состояния $s_1\in S_1$ и $s_2\in S_2$ называются эквивалентными, если для произвольного $x(0)x(1)\ldots x(m)\in X$, имеет место следующее:

$$\lambda_1(s_1,x(0),x(1),...,x(m))=\lambda_2(s_2,x(0),x(1),...,x(m))$$

Конечные автоматы M_1 и M_2 называются эквивалентными, если для произвольного состояния $s_1\in S_1$ существует эквивалентное состояние $s_2\in S_2$, и для произвольного состояния $s_2\in S_2$ существует эквивалентное состояние $s_1\in S_1$.
Известно, что линейный автомат является легкоинвертируемым с максимальной задержкой

$$\tau=\frac{|S|(|S|-1)}{2}, \quad (9)$$

где S – множество состояний автомата [6].
По Формуле (9) очевидно, что с увеличением количества состояний |S|, значение задержки τ квадратично увеличивается.
Таким образом, заменяя линейный автомат M_1 эквивалентным автоматом с более увеличенным множеством состояний, мы можем получить более длительную задержку τ. Вышеприведенная модификация увеличивает задержку τ конечного автомата шифрования.

6. АТАКА МЕТОДОМ ПОЛНОГО ПЕРЕБОРА

Асимметричная криптосистема, представленная в Главе 4, уязвима к атаке, где противнику известно окончание открытого текста.
Предположим, что автоматы M_1, M_{nl} и M определены по Формулам (1),(3) и (6) соотвественно.
Если противник знает или может угадать $r+\tau$ количество входных элементов $x(i-r-\tau+1),\ldots,x(i)$, тогда он может вычислить состояние $s(i+1)=<x(i),x(i-1),...,x(i-r-\tau+1)>$ автомата M. Такая информация позволяет находить то состояние s(i), из которого автомат M при получении элемента x(i) на входе переходил к состоянию s(i+1), и на выходе порождал элемент z(i). Для вычисления состояния $s(i)=<x(i-1),x(i-2),...,x(i-r-\tau)>$ единственным неизвестным является входной элемент $x(i-r-\tau)$.
Используя знание открытого ключа и зашифрованого текста, можно генерировать систему уравнений из Формулы (6) таким образом, чтобы было возможно однозначно определить элемент $x(i-r-\tau)$.

6.1. Модификация автомата шифрования

Для усложнения взлома методом полного перебора от конца к началу открытого текста над полем GF(2) определяется нелинейная операция для двух последовательных входных элементов конечного автомата M_l.

Формула (1), определяющая автомат M_l, переопределяется следующим образом:

$$y(i) = \sum_{j=0}^{\tau} A_j x(i-j) + \sum_{j=1}^{\tau-1} \tilde{A}_j x(i-j) \circ x(i-j-1)$$

$$i = 0,1,2..., \quad (10)$$

Подставляя Формулу (8) в Формулу (3), результат в упрощенном виде будет таким:

$$z(i) = \sum_{j=0}^{r+\tau} C_j x(i-j) + \sum_{j=1}^{2(r+\tau)} \tilde{C}_j x(i-j) \circ x(i-j-1),$$

$$i = 0,1,2... \quad (11)$$

где

$$C_j = \sum_{\substack{t=0 \\ j=0}}^{\substack{t=\tau \\ j=r}} A_t B_j, \qquad \tilde{C}_j = \sum_{\substack{t=1 \\ j=1}}^{\substack{t=\tau-1 \\ j=r-1}} \tilde{A}_t \tilde{B}_j, \qquad i = 0,1,2...$$

Исползование переопределенного автомата шифрования затрудняет восстановление открытого текста методом перебора от конца к началу, настолько насколько трудно восстановление от начала к концу. Последнее по принципу проектирования автоматов является трудной задачей.

7. ЗАКЛЮЧЕНИЕ

Представленная асимметричная криптосистема на основе конечных автоматов является стойкой по отношению к атакам на основе выбранного открытого текста и методом полного перебора. Стойкость асимметричной криптосистемы на основе конечных автоматов главным образом обусловлена увеличиванием задержки компонентых автоматов. Предложенные модификации обеих компонентных линейных и нелинейных автоматов затрудняют процесс взлома криптосистемы и позволяют проектировать более стойкую асимметричную криптосистему на основе конечных автоматов.

ЛИТЕРАТУРА

[1] Garey, M.R., D.S. Johnson, *Computer and intractability (a guide to the theory of NP-completeness),* W. H. Freeman and Co., San Francisco, 1979.

[2] Papadimitriou, C. H. Papadimitriou, *Computational Complexity*, First Edition, Addison Wesley, 1993.

[3] Arbib, M. A., *Theories of Abstract Automat,* Prentice-Hall, Englewood Cliffs, NJ, 1969.

[4] G. I. Margarov, S. H. Chopuryan, Y. Alaverdyan, "Fast Public Key Algorithm Based on Finite Automata", *In Proc. of the Int' Conf. on Computer Science and Information Technologies (CSIT'07),* Yerevan, September 2007, pp. 112-115.

[5] F. Bao, Y. Igarashi, "Break Finite Automata Public Key Cryptosystem", *ICALP*, 1995, pp. 147-158.

[6] R. Tao, Sh. Chen, X. Chen, "FAPKC3: a new automaton public key cryptosystem", *Technical Report No. ISCAS-LCS-95-07*, Laboratory for Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, June 1995.