УДК 004.056.5

М.Л. РАДЮКЕВИЧ

КОМБИНИРОВАННЫЙ МЕТОД ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С СЕКРЕТНОЙ МОДИФИКАЦИЕЙ РЕЗУЛЬТАТОВ СИНХРОНИЗАЦИИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

В данной статье рассматривается один из способов формирования общего криптографического ключа с использованием синхронизируемых искусственных нейронных сетей. В основу данного варианта выбран комбинированный метод формирования криптографического ключа [1]. Предложенное комбинированное формирование состоит из двух этапов: формирование частично совпадающих бинарных последовательностей с помощью синхронизируемых искусственных нейронных сетей и устранение несовпадающих битов путем открытого сравнения четностей пар битов. Целью данной статьи является повышение криптостойкости данного метода по отношению к криптоаналитику. В связи с этим предложено досрочное прерывание процесса синхронизации на первом этапе комбинированного метода и внесение изменений в полученную бинарную последовательность путем инвертирования случайным образом некоторого количества битов. Для подтверждения качества данного метода рассмотрены возможные атаки и проиллюстрирован масштаб перебора возможных значений. Полученные результаты показали, что комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей, предложенный в данной статье, обеспечивает высокую его криптостойкость, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования, при относительно простой реализации.

Ключевые слова: *синхронизируемые искусственные нейронные сети, криптостойкость, общий криптографический ключ, секретная модификация, комбинированный метод.*

Введение

Одной из важных задач современной криптографии является формирование общего криптографического ключа у абонентов, обменивающихся информацией через открытый для прослушивания канал связи. В более общей постановке говорят о формировании общего секрета, подразумевая под ним некое число.

В работе [1] предлагается комбинированный метод формирования криптографического ключа. Предлагаемое комбинированное формирование состоит из двух этапов: формирование частично совпадающих бинарных последовательностей с помощью синхронизируемых искусственных нейронных сетей (СИНС) [2] и устранение несовпадающих битов путем открытого сравнения четностей пар битов [3].

Использование СИНС для формирования общего криптографического ключа предложено В. Кантером, И. Кинцелем и описано в [4–8].

Алгоритм формирования общего секретного числа с помощью СИНС следующий. Абоненты *A* и *B*, имеют идентичные ИНС, соединенные открытым каналом связи [1, 2] (рис. 1). Каждая ИНС, состоит из одного слоя персептронов. Каждый персептрон имеет n входов и прямоугольную функцию активации $\sigma(*)$ (рис.2).

До начала синхронизации абоненты *A* и *B* независимо друг от друга формируют вектор весовых коэффициентов (ВК)

$$\vec{w}\mathrm{a} = wa_{11}, wa_{12}, \ldots, wa_{1n}, wa_{21}, wa_{22}, \ldots, wa_{2n}, \ldots, wa_{K1}, wa_{K2}, \ldots, wa_{Kn},$$

$$\vec{w}b = wb_{11}, wb_{12}, \ldots, wb_{1n}, wb_{21}, wb_{22}, \ldots, wb_{2n}, \ldots, wb_{K1}, wb_{K2}, \ldots, wb_{Kn},$$

где $wa_{ij}, wb_{ij} \in [-L, L]$; $i = 1, 2, \ldots, K$; $j = 1, 2, \ldots, n$; L – целое число.

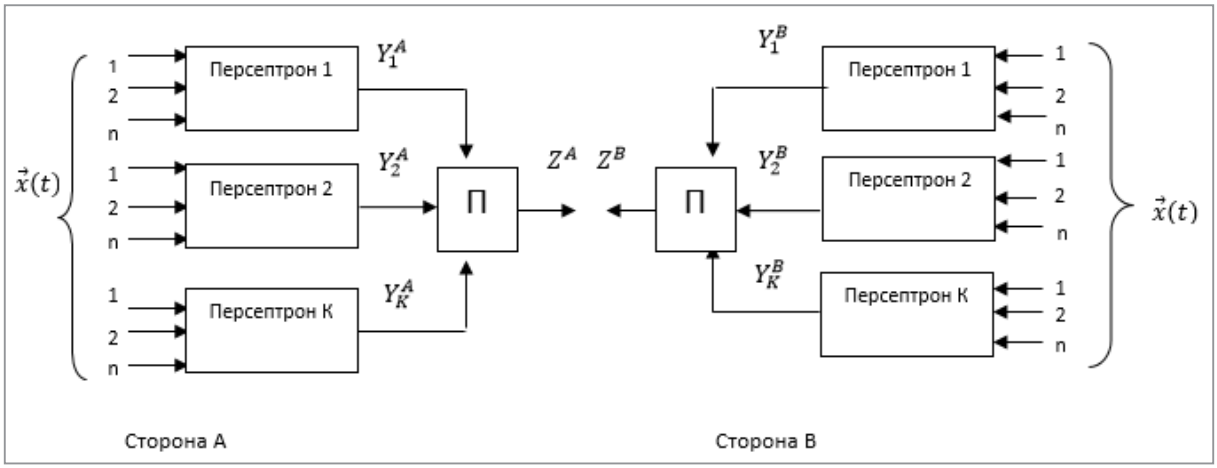

Рис. 1. Синхронизируемые ИНС

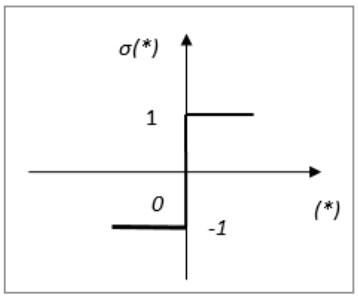

Рис. 2. Функция активации

Каждый элемент этих векторов w_{ij} есть случайное целое число с дискретным равномерным законом распределения

$$P\left(w_{ij}=s_{ij}\right)=\frac{1}{2L+1},$$

где $s_{ij}=-L,-L+1,\ldots,-1,0,1,\ldots,L-1,L.$

Каждый шаг синхронизации начинается с подачи на входы обеих сетей выбранного случайным образом вектора

$$\vec{x}\left(t\right)=x_{11},x_{12},\ldots,x_{1n},$$

$$x_{21},x_{22},\ldots,x_{2n},\ldots,x_{K1},x_{K2},\ldots,x_{Kn},$$

где $x_{ij}\in\left[-1,1\right]$ – дискретная случайная величина с равномерным распределением, t =1, 2,. . .– номер такта (далее все рассматриваемые величины зависят от t, но для упрощения записи эта зависимость в обозначениях отсутствует) Для каждого персептрона выходная величина равна

$$Y_i^{A/B}=\sigma\left(\sum_{j=1}^{n}w_{ij}^{A/B}x_{ij}\right).$$

Индекс *A/B* означает, что операция касается обеих сетей A и B, а единичный индекс – что операция касается одной сети соответственно. Функция активации $\sigma\left(*\right)$ имеет вид

$$\sigma\left(*\right)=\begin{cases}1,\ \sigma\left(*\right)\geq 0,\\ -1,\ \sigma\left(*\right)<0.\end{cases}$$

Затем вычисляется выходная величина Z для каждой из сетей

$$Z^{A/B}=\prod_{i=1}^{K}Y_i^{A/B}=\prod_{i=1}^{K}\sigma\left(\sum_{j=1}^{n}w_{ij}^{A/B}x_{ij}\right).$$

На основании сравнения обоих полученных выходных величин реализован процесс синхронизации. Коррекция векторов весов обеих сетей происходит только тогда, когда обе выходные величины равны друг другу ($Z^A=Z^B$). Внутри данной сети корректируются веса только тех персептронов, выходная величина которых равна величине Z всей сети. Процесс коррекции идет по правилу Хэбба

$$w_{ij}^{A/B}=\begin{cases}w_{ij}^{A/B}+Z^{A/B}*x_{ij},\\ \qquad\text{если } Z^A=Z^B \text{ и } Z^{A/B}=Y_i^{A/B},\\ w_{ij}^{A/B},\ \text{в противном случае.}\end{cases}$$

Кроме того, учитывается ограничение $w_{ij}^{A/B}\in\left[-L,L\right]$

$$w_{ij}^{A/B}=\begin{cases}\pm L,\ \text{если}\left|w_{ij}^{A/B}\right|>L\\ w_{ij}^{A/B},\ \text{в противном случае.}\end{cases}$$

Процесс синхронизации продолжается до полного совпадения векторов $\bar{w}a,\bar{w}b$, после чего абоненты A и B имеют общую секретную информацию, представляющую собой последовательность десятичных чисел вида

$$\bar{w}^{A/B}=w_{11},w_{12},\ldots,w_{1n},$$

$$w_{21},w_{22},\ldots,w_{2n},\ldots,w_{K1},w_{K2},\ldots,w_{Kn}.$$

Далее эта последовательность преобразуется в бинарную последовательность S путем конкатенации значений ВК.

Для повышения криптостойкости метода по отношению к действиям криптоаналитика E, синхронизирующего свою сеть E с сетью A, в [9] предложено окончательную БП формировать как свертку r независимых результатов синхронизаций ИНС A и B, эффективно разрушающую корреляцию между S^E и S^A, в виде $S_r(d) = S_r^A(d) = S_r^B(d)$, где $r = 2,3,4,\ldots$.

Тем не менее, $S_r(d)$ с некоторой вероятностью может стать известной E. Для уменьшения этой вероятности в комбинированном методе предлагается процесс синхронизации ИНС A и B останавливать на некотором такте $t = d_{\text{ус}}$, $(d_{\text{ус}} < d)$ при котором еще не достигнуто полного равенства $\vec{w}a(d_{\text{ус}})$ и $\vec{w}b(d_{\text{ус}})$. Устранение оставшихся несовпадений производится после преобразования $\vec{w}a, \vec{w}b$ в двоичный формат $S_r^A(d_{\text{ус}})$ и $S_r^E(d_{\text{ус}})$, вычисления «четности» каждой пары битов $C_A^{(i)} = a_j \oplus a_{j+1}$, $C_B^{(i)} = b_j \oplus b_{j+1}$, где i-номер пары, $a_j, b_j - j$ -тый бит A и B соответственно. Абоненты A и B сообщают четности пар друг другу по открытому каналу связи и каждый сравнивает четности соответствующих пар $C_A^{(i)}$ с $C_B^{(i)}$. Пары битов имеющие одинаковую четность остаются в БП, а пары с несовпадающими четностями удаляются. В оставшихся парах имеет место либо 0 несовпадающих битов, т.е. $a_j = b_j$ и $a_{j+1} = b_{j+1}$, либо 2, т.е. $a_j \neq b_j$ и $a_{j+1} \neq b_{j+1}$. Так как оглашение четности пары позволяет выразить один неизвестный бит через четность и другой бит $a_j = C_A^{(i)} - b_j$ и $a_{j+1} = C_B^{(i)} - b_{j+1}$, то для сохранения секретности из каждой пары удаляется по договоренности один бит. Отобранные таким образом биты объединяются в промежуточные БП, которые содержат меньшую долю несовпадающих битов. Повторяя описанную процедуру еще несколько раз, можно получить полностью совпадающие бинарные последовательности.

Таким образом, досрочное прерывание процесса синхронизации в комбинированном методе формирования общего секрета [4], приводит к существенному уменьшению $P(t_{AE} \le d_{\text{ус}})$, где $d_{\text{ус}}$ – число тактов синхронизации, при котором гарантировано не достигается равенства $\vec{w}a$ и $\vec{w}b$, что обеспечивает большую его криптостойкость за счет существенного увеличения объема отложенного перебора. Например, при K=3, n=1000, L=8, r =5 переход от d=3500, при котором $P_{AE,r}(d) = 1,5 * 10^{-7}$ к $d_{\text{ус}}$=2500, при котором $P_{AE,r}(d_{\text{ус}}) = 1,6 * 10^{-10}$.

Кроме того, дополнительно появляется возможность существенно снизить количество обменов информацией т.к. $d_{\text{ус}} < d$, а необходимое количество тактов обмена четностями составляет всего несколько единиц. В рассматриваемом примере число тактов синхронизации уменьшается на 1000, при количестве тактов обмена четностями 4.

Несмотря на указанные положительные свойства комбинированного метода представляет научный и практический интерес исследование криптостойкости метода к полному отложенному перебору и возможностей ее увеличения.

Полный отложенный перебор

Полным отложенным перебором назовем атаку на комбинированный метод формирования общего секрета, заключающуюся в запоминании значений $\vec{x}(t)$, $Z^{A/B}(t)$, где $t = 1,2,3,\ldots,d_{\text{ус}}$, имеющих место при синхронизации сетей A и B, и многократном повторении синхронизаций сети E с различными начальными значениями ВК с одними и теми же сетями A и B, на входы которых подается записанный $\vec{x}(t)$, а выходы равны $Z^{A/B}(t)$. Критерием успешного перебора является совпадение $C_E^{(i)}$ с $C_A^{(i)}$ по окончании синхронизации, как промежуточный успех, и полное совпадение процесса отсеивания несовпадающих битов в $S_r^A(d_{\text{ус}})$ и $S_r^E(d_{\text{ус}})$ на втором этапе метода. Окончательным подтверждением успеха атаки является совпадения секрета, сформированного A и B с секретом E, фиксируемое по одному из критериев [9]. Очевидно, что вероятность успеха рассматриваемой атаки равна $P_{AE,r}(d_{\text{ус}})$. Действительно, если для некоторого набора начальных значений ВК сети E окажется, что она достигла полного синхронизма с сетью A до наступления такта $d_{\text{ус}}$, то в дальнейшем будет выполнено $S_r^A(d_{\text{ус}}) = S_r^E(d_{\text{ус}})$ и $C_E^{(i)} = C_A^{(i)}$, что означает успех атаки.

Известно, что количество возможных комбинаций значений ВК ИНС E равно $M=(2L+1)^{K*n}$. При предлагаемых значениях L,K,n осуществить полный перебор значений технически не представляется возможным даже в ближайшем будущем. Однако, как показано в [10] при отложенном переборе абоненту E совершенно необязательно угадать истинное начальное значение вектора весовых коэффициентов ИНС A или B, т.к. существует достаточно большое множество начальных значений вектора весовых коэффициентов ИНС E, движение из которых при благоприятных траекториях $\vec{x}(t)$ позволяет обеспечить пересечение траекторий движения $S_r^A(t)$ и $S_r^E(t)$, в смысле равенства всех их элементов. После такого пересечения траектории движения $S_r^A(d)$ и $S_r^E(d)$ совпадают при всех последующих тактах синхронизации. В результате обязательно наступит $S_r^A(d_{\text{ус}}) = S_r^E(d_{\text{ус}})$. Таким образом, если при классическом полном переборе значений успех атаки наступает при единственно правильном наборе ВК ИНС E, то в атаке отложенным перебором успех атаки наступает при всех наборах для которых ВК ИНС E пересеклись с ВК ИНС A на участке от $t=0$ до $t=d_{\text{ус}}$. Этот эффект качественно поясняется на рис. 3.

На этом рисунке показаны условные траектории изменения векторов весовых коэффициентов сетей A, B в процессе синхронизации. Сеть E представлена тремя типами траекторий.

Для траекторий типа $S_{r1}^E(t)$, пересекающихся с $S_r^A(t)$ на участке от $t=0$ до $t=d_{\text{ус}}$ обязательно выполняется $S_r^A(d_{\text{ус}}) = S_r^E(d_{\text{ус}})$, что обнаруживается E по равенству объявленных значений $C_E^{(i)}, C_A^{(i)}$ и полному совпадению процесса отсеивания несовпадающих битов между $S_r^A(d_{\text{ус}})$, $S_r^B(d_{\text{ус}})$ и $S_r^A(d_{\text{ус}})$, $S_r^E(d_{\text{ус}})$, при этом вероятность успеха такой атаки равна $P_{AE,r}(d_{\text{ус}})$.

Траектории типа $S_{r2}^E(t)$, не пересекаются с $S_r^A(t)$ на участке от $t=0$ до $t=d$. Траектории этого типа составляют большинство, их вероятность равна $1-P_{AE,r}(d_{\text{ус}})$.

Траектория типа $S_{r3}^E(t)$ в процессе синхронизации пересеклась с $S_r^A(t)$ в точке $t=d_{\text{ус}}$. Вероятность получения такой траектории близка к вероятности независимого перебора всех возможных значений $S_r^A(d_{\text{ус}})$, которая равна $(2L+1)^{-K*n}$.

Таким образом, несмотря на то, что за счет выбора минимально возможного значения $d_{\text{ус}}$ и усложнения процесса синхронизации за счет увеличения r, вероятность успеха атаки отложенного перебора намного больше, чем $(2L+1)^{-K*n}$. Этот факт может быть объяснен тем, что в одном случае успех атаки обусловлен тем, что достаточно найти хотя бы одну траекторию $S_r^E(t)$, пересекающуюся с траекторией $S_r^A(t)$ на интервале [0, $d_{\text{ус}}$], а во втором случае нужно найти единственную траекторию $S_r^E(t)$, проходящую через точку $S_r^A(d_{\text{ус}})$. Это свойство может быть использовано для модификации комбинированного метода с целью повышения его криптостойкости.

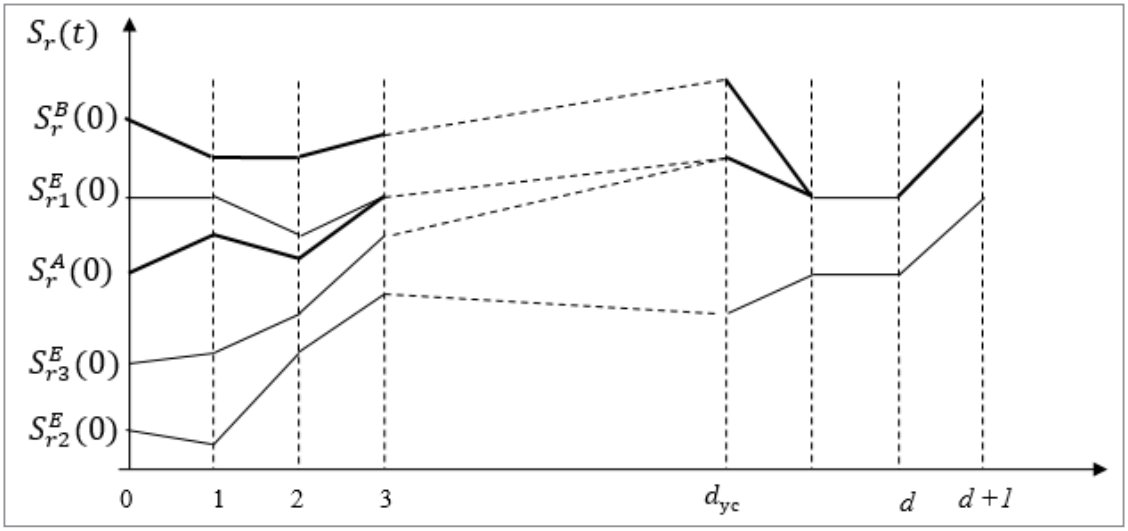

Рис. 3. Условное графическое отображение синхронизаций

Секретная модификация результатов синхронизации

Необязательность продолжать синхронизацию ИНС *A* и *B* до полного совпадения ВК этих сетей в комбинированном методе позволяет до оглашения четностей пар битов $C_A^{(i)}$, $C_B^{(i)}$ внести некоторые изменения в бинарную последовательность $S_r^A\left(d_{\text{ус}}\right)$ абонентом *A* и в $S_r^B\left(d_{\text{ус}}\right)$ абонентом *B*, например, инвертировав случайным образом независимо друг от друга некоторое количество битов. При этом количество несовпадающих битов увеличится и несколько уменьшится длина окончательно сформированной общей секретной последовательности, однако значительно повысится криптостойкость по отношению к атаке отложенного перебора. На рис. 4 условно отображена описанная модификация.

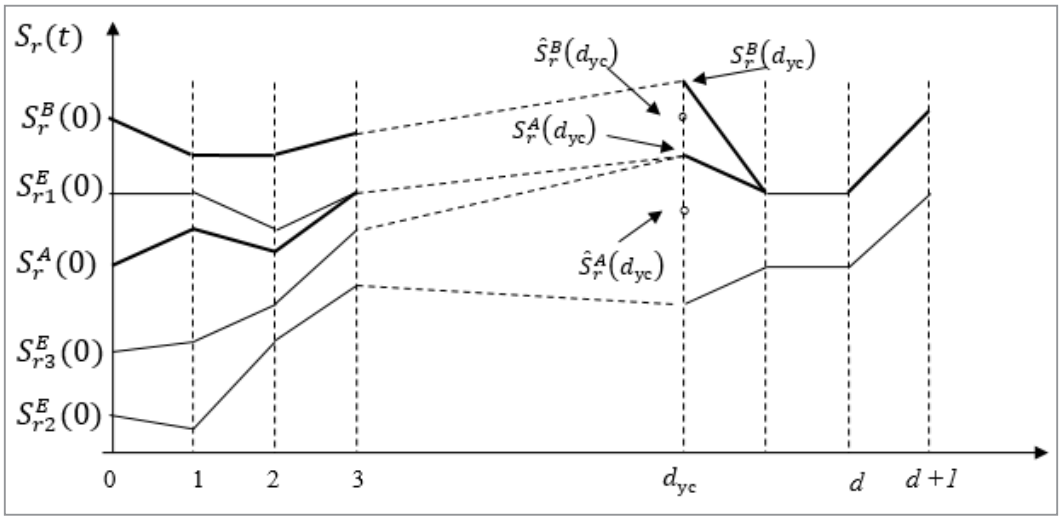

Рис. 4. Модификация результата синхронизации

Действительно, внесение случайного секретного изменения некоторых битов в $S_r^A\left(d_{\text{ус}}\right)$ и $S_r^B\left(d_{\text{ус}}\right)$ превращает атаку отложенный перебор из поиска траекторий $S_r^E(t)$, пересекающихся с траекторией $S_r^A(t)$, в поиск траектории $S_r^E(t)$, проходящей через точку $\hat{S}_r^A\left(d_{\text{ус}}\right)$, где $\hat{S}_r^A\left(d_{\text{ус}}\right)$ – случайно модифицированная точка $S_r^A\left(d_{\text{ус}}\right)$. Рассмотрим возможные варианты отложенного перебора и оценим вероятности успешных атак.

Одна из возможных атак аналогична уже рассмотренной. Абонент *E* повторяет синхронизации своей сети с зафиксированной синхронизацией ИНС *A* и *B*, перебирая начальные значения ВК своих сетей, и останавливает процесс, если оказалось, что $C_E^{(i)} = \hat{C}_A^{(i)}$, где $\hat{C}_A^{(i)}$ соответствует $\hat{S}_r^A\left(d_{\text{ус}}\right)$, и процесс удаления несовпадающих битов в $S_r^E\left(d_{\text{ус}}\right)$ полностью совпал с процессом удаления несовпадающих битов в $\hat{S}_r^A\left(d_{\text{ус}}\right)$. Так как при относительно небольших выбранных значениях $d_{\text{ус}}$ корреляция между $S_r^E(t)$ и $S_r^A(t)$ довольно слабая, то различные траектории $S_r^E(t)$ можно считать независимыми между собой, а перебор в данном случае эквивалентен поиску такой единственной совокупности начальных значений ВК своей сети, которые приведут ИНС *E* к попаданию в точку $\hat{S}_r^A\left(d_{\text{ус}}\right)$. Следовательно, вероятность успеха такого перебора P_{op1} близка к величине $(2L+1)^{-K*n}$. Например, для L=8, K=3, n=1000 имеем $P_{op1} = P_{AE,r}\left(d_{\text{ус}}\right) = 4{,}5*10^{-3692}$.

Второй вариант атаки заключается в том, что абонент *E*, перебирая начальные значения ВК своих сетей, доводит каждую синхронизацию $S_r^E(t)$ до $t = d_{\text{ус}}$, затем модифицирует полученную БП по аналогии с модификацией, проделанной *A* и *B*, перебирая все возможные варианты инвертирования битов. Если для какой-то модификации окажется, что $\hat{C}_E^{(i)} = \hat{C}_A^{(i)}$ и процесс удаления несовпадающих битов $\hat{S}_r^E\left(d_{\text{ус}}\right)$ полностью совпал с процессом удаления несовпадающих битов в $\hat{S}_r^A\left(d_{\text{ус}}\right)$, то атака является успешной. Оценим вероятность успеха этой атаки, обозначив ее через P_{op2}.

Атака будет успешной, если произойдут события при которых окажется, что $\hat{S}_r^E\left(d_{\text{ус}}\right) = \hat{S}_r^A\left(d_{\text{ус}}\right)$. Обозначим это событие через *U*. Событие *U* произойдёт, если при

синхронизации ИНС E и A произойдёт событие $S_r^E\left(d_{\text{ус}}\right)=S_r^A\left(d_{\text{ус}}\right)$, обозначим его A, и при переборе некого числа битов в $S_r^E\left(d_{\text{ус}}\right)$ будет найдена комбинация битов, инвертированных в $S_r^A\left(d_{\text{ус}}\right)$ (событие B). Кроме того, событие U будет иметь место, если произойдет событие $\overline{A}$ и будет найдена комбинация битов несовпадающих в $S_r^E\left(d_{\text{ус}}\right)$ и $\hat{S}_r^A\left(d_{\text{ус}}\right)$, возникшая за счет различия начальных значений ВК ИНС E и A и последующего инвертирования некого числа битов в $S_r^A\left(d_{\text{ус}}\right)$, т.е. события C.

С учетом введенных обозначений имеем

$$P_{op2}\left(U\right)=P\left(A\right)P\left(B\right)+P\left(\overline{A}\right)P\left(C\right).$$

В данном выражении

$$P\left(A\right)=P(S_r^E\left(d_{\text{ус}}\right)=S_r^A\left(d_{\text{ус}}\right))=P_{AE,r}\left(d_{\text{ус}}\right),$$

$$P\left(B\right)=\left(\sum_{v=1}^{V}C_b^v\right)^{-1},$$

где b – длина БП $S_r^E\left(d_{\text{ус}}\right)$ и $S_r^A\left(d_{\text{ус}}\right)$ в битах; V – максимальное количество битов, которое может быть инвертировано (по договоренности, V может быть известно E), C_b^v – число сочетаний из b по v;

$$P\left(\overline{A}\right)=1-P\left(A\right)=1-P_{AE,r}\left(d_{\text{ус}}\right);$$

$$P\left(C\right)\approx\left(\sum_{v=\frac{b}{2}-V}^{\frac{b}{2}+V}C_b^v\right)^{-1}.$$

Пределы перебора в $P\left(C\right)$ определены приближенно, исходя из следующих соображений. Моделированием установлено, что для синхронизаций, у которых $S_r^E\left(d_{\text{ус}}\right)\neq S_r^A\left(d_{\text{ус}}\right)$, математическое ожидание числа несовпадающих битов равно $b/2$. Дополнительное инвертирование некого числа битов может лишь незначительно увеличить или уменьшить число несовпадающих битов. Исходя из вышесказанного окончательно имеем

$$P_{op2}=P\left(U\right)\approx P_{AE,r}\left(d_{\text{ус}}\right)\left(\sum_{v=1}^{V}C_b^v\right)^{-1}+$$

$$+\left(1-P_{AE,r}\left(d_{\text{ус}}\right)\right)\left(\sum_{v=\frac{b}{2}-V}^{\frac{b}{2}+V}C_b^v\right)^{-1}.$$

Так как $\left(\sum_{v=\frac{b}{2}-V}^{\frac{b}{2}+V}C_b^v\right)^{-1}\ll\left(\sum_{v=1}^{V}C_b^v\right)^{-1}$, то вторым слагаемым можно пренебречь и в результате получаем

$$P_{op2}\approx P_{AE,r}\left(d_{\text{ус}}\right)\left(\sum_{v=1}^{V}C_b^v\right)^{-1}.$$

Проиллюстрируем масштаб перебора на рассмотренном ранее примере. При заданных следующих значениях K=3, n=1000, L=8, r =5, $d_{\text{ус}}$=2500, b=12000, V=50, получаем $P_{AE,r}\left(d_{\text{ус}}\right)=1,6*10^{-10}$, $\left(\sum_{v=1}^{V}C_b^v\right)^{-1}\approx 2,7*10^{-139}$, и итоговое значение $P_{op2}=1,6*10^{-10}*0,36*10^{-139}\approx 0,6*10^{-149}$.

Заключение

Комбинированное формирование криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей, предложенное в данной статье, обеспечивает высокую его криптостойкость, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования, при относительно простой реализации.

ЛИТЕРАТУРА

1. **Радюкевич М.Л., Голиков В.Ф.** Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей. Доклады БГУИР. 2021; 19(1): 79–87.
2. **Голиков, В.Ф.** Формирование общего секрета с помощью искусственных нейронных сетей / В.Ф. Голиков, М.Л. Радюкевич // Системный анализ и прикладная информатика.– 2019.– № 2.– С. 49–56.
3. **Пивоваров В.Л., Голиков В.Ф.** Способ формирования криптографического ключа для слабо совпадающих бинарных последовательностей. Информатика, № 3(51), 2016. Стр. 31–37.
4. **Kinzel, W.** Neural Cryptography / W. Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.
5. **Kanter, I.** Secure exchange of information by synchronization of neural networks / I. Kanter, W. Kinzel, E. Kanter//arxiv: cond/0202112v1, [cond-mat.stat-mech], 2002.
6. **Kanter, I.** The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel.–2005. Vol. 5, n.1.– P. 130–140.

7. **Ruttor, A.** Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.
8. **Плонковски, М.** Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика; под ред. И. М. Жарского.– Минск: БГТУ, 2005.
9. **Радюкевич, М. Л.** Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Информатика.– 2020.– Т. 17, № 1.– С. 75–81. https://doi.org/10.37661/1816–0301–2020–17–1–75–81.
10. **Голиков, В. Ф.** Атака на синхронизируемые исскуственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В. Ф. Голиков, А. Ю. Ксеневич // Доклады БГУИР.– 2017.– № 8.– С. 48–53.

REFERENCES

1. **Radziukevich M. L., Golikov V. F.** Combined formation of a cryptographic key using synchronized artificial neural networks. Doklady BGUIR. 2021; 19(1): 79–87.
2. **Golikov V. F., Radziukevich M. L.** [The formation of a common secret using artificial neural networks]. Sistemnyy analiz i prikladnaya informatika [System Analysis and Applied Informatics], 2019, no. 2, pp. 49–56 (in Russian).
3. **Pivovarov V. L., Holikau U. F.** [Method of generating common cryptographic keys for loosly coincident binary sequences]. Informatics. 2016;(3):31–37. (In Russ.).
4. **Kinzel, W.** Neural Cryptography / W. Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.
5. **Kanter, I.** Secure exchange of information by synchronization of neural networks / I. Kanter, W. Kinzel, E. Kanter//arxiv: cond/0202112v1, [cond-mat.stat-mech], 2002.
6. **Kanter, I.** The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel.–2005. Vol. 5, n.1.– P. 130–140.
7. **Ruttor, A.** Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.
8. **Plonkovski, M.** Cryptographic transformation of information based on neural network technology / M. Plonkovski, P. P. Urbanovich // Proceedings of BSTU. Series VI. Physics and Mathematics and Informatics; by ed. I. M. Zharsky.– Minsk: BSTU, 2005.
9. **Radziukevich M. L., Golikov V. F.** [Enhancing the secrecy of a cryptographic key generated using synchronized artificial neural networks]. Informatics. 2020;17(1):102–108. (In Russ.).
10. **Golikov V. F., Ksenevich A. Y.** [Attack on synchronized artificial neural networks, forming a common secret by deferred search]. Doklady BGUIR. 2017;(8):48–53. (In Russ.).

Поступила	*После доработки*	*Принята к печати*
17.06.2021	*30.08.2021*	*01.09.2021*

RADZIUKEVICH M. L.

A COMBINED METHOD OF FORMATION OF A CRYPTOGRAPHIC KEY WITH SECRET MODIFICATION OF THE RESULTS OF SYNCHRONIZATION OF ARTIFICIAL NEURAL NETWORKS

Scientific Production Republican Unitary Enterprise
"Research Institute for the Technical Protection of Information"

This article discusses one of the ways to generate a common cryptographic key using synchronized artificial neural networks. This option is based on a combined method of forming a cryptographic key [1]. The proposed combined formation consists of two stages: the formation of partially coinciding binary sequences using synchronized artificial neural networks and the elimination of mismatched bits by open comparison of the parities of bit pairs. The purpose of this article is to increase the cryptographic strength of this method in relation to a cryptanalyst. In this regard, it is proposed to prematurely interrupt the synchronization process at the first stage of the combined method and make changes to the resulting binary sequence by randomly inverting a certain number of bits. To confirm the quality of this method, possible attacks are considered and the scale of enumeration of possible values is illustrated. The results obtained showed that the combined method of forming a cryptographic key with a secret modification of the synchronization results of artificial neural networks, proposed in this article, provides its high cryptographic strength, commensurate with the cryptographic strength of modern symmetric encryption algorithms, with a relatively simple implementation.

Keywords: *synchronized artificial neural networks, cryptographic strength, common cryptographic key, secret modification, combined method.*

Радюкевич Марина Львовна, магистр технических наук. Начальник испытательной лаборатории по требованиям безопасности информации научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации». Победитель конкурса молодых ученых на XXIV научно-практической конференции «Комплексная защита информации».

E-mail: 1218a@list.ru

Radziukevich Maryna Lvovna, M. Sci. (Eng.), Head of the Testing Laboratory for Information Security Requirements, the Scientific-Production Republican Unitary Enterprise “Research Institute for Technical Protection of Information”, Minsk, Belarus, Winner of the competition of young scientists at the XXIV scientific-practical conference “Comprehensive information protection”.
E-mail: 1218a@list.ru