http://dx.doi.org/10.35596/1729-7648-2021-19-1-79-87

Оригинальная статья
Original paper

УДК 004.056.5

КОМБИНИРОВАННОЕ ФОРМИРОВАНИЕ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. РАДЮКЕВИЧ[1], В.Ф. ГОЛИКОВ[2]

[1]*Государственное предприятие «НИИ ТЗИ»*
(г. Минск, Республика Беларусь)

[2]*Белорусский национальный технический университет (г. Минск, Республика Беларусь)*

Поступила в редакцию 2 октября 2020

Аннотация. В статье предлагается комбинированный метод формирования криптографического ключа. Предлагаемое 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. В работе рассмотрены возможные уязвимости базового метода формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей, оценена их опасность и предложена коррекция метода с целью обеспечения требуемой конфиденциальности формируемого общего секрета. На первом этапе рассмотрена атака «отложенный перебор». Для нейтрализации данной атаки предлагается использовать функцию свертки результатов нескольких независимых синхронизаций. В качестве функции свертки используется побитовое сложение по модулю двух векторов весовых коэффициентов сетей. Благодаря коррекции первого этапа базового алгоритма экспоненциально увеличивается объем отложенного перебора, а также становится неэффективным частотный анализ бинарных последовательностей. На втором этапе рассмотрена атака, основанная на знании четностей пар, с учетом предложенного метода коррекции первого этапа. Проведен анализ влияния параметров сетей на процесс устранения несовпадения битов на втором этапе. Выполнено статистическое моделирование данного анализа. Полученные результаты показали, что криптоаналитик не может однозначно различить значения оставшихся битов. Предложенный комбинированный метод позволяет повысить конфиденциальность формируемого общего секрета и существенно сократить количество обменов информацией по сравнению с технологией Neural key generation.

Ключевые слова: синхронизируемые искусственные нейронные сети, общий секрет, криптографический ключ, комбинированный метод.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Радюкевич М.Л., Голиков В.Ф. Комбинированное формирование криптографического ключа с помощью синхронизируемых искусственных нейронных сетей. Доклады БГУИР. 2021; 19(1): 79-87.

COMBINED FORMATION OF A CRYPTOGRAPHIC KEY USING SYNCHRONIZED ARTIFICIAL NEURAL NETWORKS

MARYNA L. RADZIUKEVICH[1], VLADIMIR F. GOLIKOV[2]

[1]*State Enterprise "NII TZI" (Minsk, Republic of Belarus)*

[2]*Belarusian National Technical University (Minsk, Republic of Belarus)*

Submitted 2 October 2020

Abstract. A combined method for forming a cryptographic key is proposed in the article. 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. In this paper, possible vulnerabilities of the basic method of forming a cryptographic key using synchronized artificial neural networks are considered, their danger is assessed, and a correction of the method is proposed to ensure the required confidentiality of the generated shared secret. At the first stage, a deferred brute-force attack is considered. To neutralize this attack, it is proposed to use the convolution function of the results of several independent synchronizations. As a convolution function, the bitwise addition modulo 2 of the vectors of the weights of the networks is used. Due to the correction of the first stage of the basic algorithm, the amount of deferred search exponentially increases, and frequency analysis of binary sequences also becomes ineffective. At the second stage, an attack based on the knowledge of pair parities is considered, taking into account the proposed method for correcting the first stage. The analysis of the influence of network parameters on the process of eliminating the bit mismatch at the second stage is carried out. Statistical modeling of this analysis has been performed. The results obtained showed that the cryptanalyst could not uniquely distinguish the values of the remaining bits. The proposed combined method makes it possible to increase the confidentiality of the generated shared secret and significantly reduce the number of information exchanges in comparison with the Neural key generation technology.

Keywords: synchronized artificial neural networks, shared secret, cryptographic key, combined method.

Conflict of interests. The authors declare no conflict of interests.

For citation. Radziukevich M.L., Golikov V.F. Combined formation of a cryptographic key using synchronized artificial neural networks. Doklady BGUIR. 2021; 19(1): 79-87.

Введение

В работе [1] предлагался способ формирования общего секрета путем создания частично совпадающих бинарных последовательностей (БП) с последующим устранением несовпадающих битов. В двух БП, формируемых случайным образом независимо друг от друга, относительное количество несовпадающих битов является случайной величиной с математическим ожиданием $M\left[\frac{n_{ns}}{n}\right]=0,5$, где n_{ns} – количество несовпадающих битов, n – длина БП в битах. Величина $\delta=\frac{n_{ns}}{n}$ получила название «доля несовпадающих битов».

Под частично совпадающими БП понимаются БП, у которых математическое ожидание доли несовпадающих битов δ не равно 0,5. БП, у которых $M[\delta]=0,5$ являются статистически независимыми и не могут быть согласованы никаким методом [2], так как при этом раскрываются все биты согласуемых последовательностей. Основной проблемой описанного способа является задача формирования БП со свойствами частично совпадающих БП. Метод, который был реализован при этом, как выяснилось в дальнейшем исследовании, оказался уязвим к атаке, основанной на вычислении некоторой части битов путем выдвижения гипотез

об их значениях и уточнении вероятностей этих гипотез в процессе итерационного согласования [1]. Причем оказалось, что увеличение совпадений приводит к уменьшению конфиденциальности формируемого секрета. Кроме того, серьезным недостатком была необходимость создания большого начального числа битов в исходных последовательностях для получения итоговой последовательности размером в десяток битов.

В связи с изложенным представляет интерес разработка комбинированного способа формирования общего секрета, в котором в качестве первого этапа (этапа формирования частично совпадающих БП) используются синхронизируемые искусственные нейронные сети (СИНС), которые предложены в [3] и анализировались в [4].

Базовый алгоритм

Первый этап – формирование частично совпадающих БП. Пусть абоненты *A* и *B*, имеют СИНС со структурой и параметрами, описанными в [5]. Подавая на входы своих сетей случайную последовательность $\vec{x}(t)$ и обмениваясь выходными величинами $Z^{A/B}(t)$, где t – номер такта синхронизации $(t = 1,2,3,...)$, *A* и *B* такт за тактом сближают секретные вектора весовых коэффициентов (ВК) своих сетей, т. е. $\vec{W}^A(t) \Leftrightarrow \vec{W}^B(t)$. Процесс останавливается на некотором такте d, при котором вероятность совпадения весовых коэффициентов (ВК) у сетей *A* и *B* гарантированно ниже чем 1, т. е. синхронизация является досрочно прерванной. При этом, поскольку изначально вектора ВК сетей формировались случайно с равномерным законом распределения и независимо друг от друга, то математическое ожидание доли несовпадающих битов было равно $M[\delta] = 0,5$, а в момент остановки синхронизации станет $0,5 < M[\delta] < 1$. Величину *d* следует выбирать из компромиссных соображений, имея в виду, что чем больше *d*, тем меньше n_{ns}, и тем меньше итераций потребуется для окончательного согласования БП на втором этапе.

Второй этап – устранение несовпадающих битов. Этап начинается с преобразования векторов ВК $\vec{W}^A(d)$ и $\vec{W}^B(d)$ в БП $S^A(d)$ и $S^B(d)$ в соответствии с [6], т. е. осуществляется переход от чисел в десятичном формате к числам в двоичном формате. После этого *A* и *B* согласовано разбивают свои БП на пары битов либо случайным образом, либо по порядку номеров [1]. Далее *A* и *B* вычисляют 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-й бит БП *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 $a_{j+1} = b_{j+1}$. 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. В [1] показано, что если БП имеют математическое ожидание доли несовпадающих битов $M[\delta] \leq 0,2$, то число необходимых итераций не превышает 3. При этом длина итоговой БП, по сравнению с начальной, уменьшается как минимум в 2^l раз, где l – число итераций. Таким образом, вся процедура предлагаемого метода составляет d тактов синхронизации и l тактов фильтрации несовпадений.

Если способ согласования слабо совпадающих БП подробно рассмотрен в [1], то вопросы, связанные с выбором параметров сетей и параметров процесса синхронизации требуют обоснования и расчета.

Очевидно, что принимаемые решения зависят не только от действий *A* и *B* в процессе синхронизации, но и от возможных действий криптоаналитика *E*, прослушивающего канал связи и владеющего всей обменной информацией, за исключением значений ВК сетей. Таким образом, необходимо выявить возможные уязвимости предлагаемого метода, оценить их опасность и провести коррекцию базового метода с целью обеспечения требуемой конфиденциальности формируемого общего секрета.

Возможные уязвимости базового метода и методы их устранения

Предлагаемый метод, по мнению авторов, может быть атакован как на первом, так и на втором этапах. На первом этапе, т. е. при синхронизации сетей *A* и *B*, криптоаналитик *E* создает свою сеть, идентичную сетям *A* и *B*, за исключением начальных значений ВК, синхронизирует (в дальнейшем будет рассматриваться только геометрическая атака, как наиболее эффективная) свою сеть с сетью, например, *A*, в надежде, что его сеть успеет полностью синхронизоваться за отведенное число тактов *d*. В этом случае окажется, что $\vec{W}^E(d) = \vec{W}^A(d)$.

На втором этапе знание *E* объявленных четностей пар битов и тот факт, что за счет синхронизации возникает корреляция между $\vec{W}^A(d)$ и $\vec{W}^E(d)$, позволяет ему использовать данную информацию для вычисления некоторых битов в итоговой БП.

Рассмотрим более подробно указанные уязвимости и меры их нейтрализации.

Отложенный перебор. На первом этапе метода наиболее эффективной атакой может оказаться атака «отложенный перебор», предложенная в [7]. Ее суть заключается в запоминании значений $\vec{x}(t)$, имеющих место при синхронизации сетей A и B, и многократном повторении *E* синхронизаций сети 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 окончания перебора является совпадение $S^E(d)$ с $S^A(d)$, фиксируемое по одному из критериев [4]. Очевидно, что объем перебора зависит от степени корреляции случайных величин t_{AB}, t_{EB}, где $t_{AB}, t_{EB}-$ количество тактов до полного совпадения ВК сетей *A* с *B* и *E* с *A* соответственно. С ростом *d* коэффициент корреляции изменяется от 0, при полном несовпадении ВК, до 1 – при полном совпадении ВК. Это свойство существенно зависит от конфигурации и параметров используемых СИНС.

В [6] показано, что для реализации процесса синхронизации, наиболее неблагоприятного для *E*, следует выбрать сети A и B с параметрами $k = 3,\ n = 1000,\ L = 8$. При таком выборе параметров удается получить БП длиной $b = 12000$ и достаточно серьезное отставание синхронизации сетей Е и А от синхронизации А и В, так как имеет место $P(t_{AB} \le d) >> P(t_{AE} \le d)$. Например, при $d = 3500$ получается $P(t_{AB} \le d) \approx 0,95$, а $P(t_{AE} \le d) \approx 0,04$ [5]. Однако, несмотря на кажущееся различие в этих вероятностях, объем отложенного перебора относительно небольшой. Согласно [7], чтобы с вероятностью $\gamma = 0,98$ достичь успеха, необходим объем перебора $m \approx 10^2$. Кроме того, более глубокий анализ показал, что сформированные при этом компоненты векторов $\vec{W}^A(d)$ и $\vec{W}^B(d)$ не имеют равномерного распределения: значения ВК, равные *L* и –*L*, а также близким к ним значениям, встречаются гораздо чаще, чем остальные. Это делает возможным частотный анализ $\vec{W}^A(d)$ и $\vec{W}^B(d)$.

Для успешного противостояния атаке отложенного перебора целесообразно использовать способ, предложенный в [6]. Его суть заключается в том, что при формировании совпадающих БП с помощью СИНС вместо одной синхронизации сетей *A* и *B*, производится *r* независимых синхронизаций с различными начальными значениями ВК, а результирующие вектора $S_r^A(d)$ и $S_r^B(d)$ вычисляются как некоторая свертка результатов каждой синхронизации:

$$S_r^A(d) = S_1^A(d) \oplus S_2^A(d) \oplus ... \oplus S_r^A(d),$$
$$S_r^B(d) = S_1^B(d) \oplus S_2^B(d) \oplus ... \oplus S_r^B(d).$$

В результате получаем бинарные последовательности длиной b, в которых каждый бит – сумма битов по модулю 2 из r слагаемых.

E, осуществляя отложенный перебор, не имеет возможности сопоставлять результаты своих частных синхронизаций с результатами частных синхронизаций сетей A и B. А поскольку при переходе к сверткам взаимная корреляция $S_r^A(d)$ с $S_r^B(d)$ с ростом r ослабляется значительно медленее, чем корреляция $S_r^E(d)$ с $S_r^A(d)$, то объем отложенного перебора существенно возрастает.

В табл. 1 приведены значения $M\left[\delta_{A,B}\right]$, $M\left[\delta_{E,A}\right]$ соответственно в числителе и знаменателе: между $S_r^A(d)$ и $S_r^B(d)$, между $S_r^E(d)$ и $S_r^A(d)$.

Таблица 1. Значения $M\left[\delta_{A,B}\right]$, $M\left[\delta_{E,A}\right]$

Table 1. The values $M\left[\delta_{A,B}\right]$, $M\left[\delta_{E,A}\right]$

r	d				
	500	1000	2000	2500	3500
1	0,61 / 0,59	0,74 / 0,65	0,97 / 0,65	0,99 / 0,65	0,99 / 0,65
5	0,50 / 0,50	0,53 / 0,50	0,89 / 0,51	0,98 / 0,51	0,99 / 0,51
10	0,50 / 0,50	0,51 / 0,50	0,81 / 0,50	0,96 / 0,50	0,99 / 0,51

В данной таблице $\delta_{A,B} = \frac{n_{A,B}}{b}$, $\delta_{E,A} = \frac{n_{E,A}}{b}$, где $n_{A,B}, n_{E,A}$ – количество совпадающих бит в $S_r^A(d)$ и $S_r^B(d)$, $S_r^E(d)$ и $S_r^A(d)$ соответственно. Из таблицы видно, что при $r \geq 5$ величина $M\left[\delta_{A,B}\right]$ близка к 1,0 уже начиная от $d = 2500$, в то время как величина $M\left[\delta_{E,A}\right]$ остается близкой к 0,5 (0,5 свидетельствует о статистической независимости $S_r^E(d)$ и $S_r^A(d)$). В [6] показано, что увеличивая r, можно экспоненциально увеличить объем отложенного перебора (табл. 2).

Таблица 2. Объем отложенного перебора

Table 2. Deferred search volume

P_{EA}	r			
	5	10	20	50
0,001	$3 \cdot 10^{15}$	$3 \cdot 10^{30}$	$3 \cdot 10^{60}$	$3 \cdot 10^{150}$
0,005	$9{,}3 \cdot 10^{12}$	$2{,}9 \cdot 10^{23}$	$2{,}8 \cdot 10^{46}$	$2{,}6 \cdot 10^{115}$
0,010	$3 \cdot 10^{10}$	$3 \cdot 10^{20}$	$3 \cdot 10^{40}$	$3 \cdot 10^{100}$
0,050	$2{,}8 \cdot 10^{7}$	$9{,}7 \cdot 10^{14}$	$2{,}8 \cdot 10^{26}$	$2{,}6 \cdot 10^{65}$

Кроме того, в [6] показано, что с ростом r закон распределения вероятностей $S_r^A(d)$ и $S_r^B(d)$ близок к равномерному, что делает неэффективным частотный анализ этих БП.

Положительным свойством комбинированного метода является и то, что на этапе синхронизации для A и B нет необходимости добиваться совпадения $S_r^A(d)$ с $S_r^B(d)$ и подтверждения этого, следовательно, и E не имеет критерия для остановки перебора.

Атака, основанная на знании четностей пар. На втором этапе метода, когда абоненты A и B оглашают четности пар БП, сформированных с помощью СИНС, у криптоаналитика E появляется возможность сравнить эти четности с четностями своей БП и сделать определенные выводы относительно формируемого общего секрета. Оценим эффективность атаки, описанной в [1]. Для этого проведем анализ влияния параметров сетей на процесс устранения несовпадений битов на втором этапе.

Поскольку процедура устранения несовпадений битов оперирует с парами битов, то целесообразно проводить анализ на уровне пар, а не отдельных битов. Анализ может быть выполнен аналитически с использованием результатов, полученных в [1], или методом статистического моделирования.

Обозначим длину БП, сформированных путем синхронизации сетей A и B через b. Тогда число пар равно $D=\frac{b}{2}$, если b окажется нечетным, то его следует привести к четному, отбросив последний бит. Тогда, согласно [1], среднее число совпадающих пар битов в анализируемых БП равно $m_{c,c}=\frac{b_{A,B}^2}{b^2}\cdot D=\frac{b_{A,B}^2}{2b}$, где $b_{A,B}$ – количество совпадающих битов в БП A и B.

Среднее число пар битов, содержащих один совпадающий бит, равно $m_{\text{с,с}}=2D\frac{b_{A,B}}{b}\frac{(b-b_{A,B})}{b}=\frac{b_{A,B}(b-b_{A,B})}{b}$.

Среднее число пар битов, содержащих два несовпадающих бита, равно $m_{\text{н,н}}=D\frac{(b-b_{A,B})^2}{b^2}=\frac{(b-b_{A,B})^2}{2b}$.

Пары, содержащие один совпадающий бит, в дальнейшем согласовании не участвуют, так как подлежат удалению. Поэтому представляет интерес только величины $m_{\text{с,с}}$ и $m_{\text{н,н}}$. В табл. 3 приведены значения этих величин в зависимости от количества совпадающих битов для b=12000.

Таблица 3. Значения величины $m_{\text{с,с}}$ и $m_{\text{н,н}}$ в зависимости от количества совпадающих битов
Table 3. The value of $m_{\text{с,с}}$ and $m_{\text{н,н}}$ in depending on the number of matching bits

$b_{A,B}/b$	0,500	0,583	0,666	0,750	0,833	0,9166	1,000
$m_{\text{с,с}}$	1500	2041	2666	3375	4166	5401	6000
$m_{\text{н,н}}$	1500	1041	666	375	166	41	0
$m_{\text{с,с}}+m_{\text{н,н}}$	3000	3082	3332	3750	5832	5442	6000

Обозначим БП абонентов A и B, получившиеся после прерванной синхронизации, через $S_r^A(d)$ и $S_r^B(d)$, а итоговую БП $S_r^{AB}(d)$.

После остановки синхронизации и оглашения четностей пар битов E знает, что A и B оставят для дальнейшего рассмотрения только пары, у которых четности совпадают $C_A^{(i)}=C_B^{(i)}$. Поэтому E будет рассматривать только те свои пары битов, для которых выполняется $C_E^{(i)}=C_A^{(i)}=C_B^{(i)}$. Для битов каждой из этих пар можно выдвинуть следующие гипотезы:

$$H_0: e_j=a_j=b_j, e_{j+1}=a_{j+1}=b_{j+1};$$
$$H_1: e_j=\overline{a}_j=\overline{b}_j, e_{j+1}=\overline{a}_{j+1}=\overline{b}_{j+1};$$
$$H_2: e_j=a_j=\overline{b}_j, e_{j+1}=a_{j+1}=\overline{b}_{j+1};$$
$$H_3: e_j=\overline{a}_j=b_j, e_{j+1}=\overline{a}_{j+1}=b_{j+1}.$$

Например,

$$H_0: C_E^{(i)}=1\oplus 1; C_A^{(i)}=1\oplus 1; C_B^{(i)}=1\oplus 1;$$
$$H_1: C_E^{(i)}=1\oplus 1; C_A^{(i)}=0\oplus 0; C_B^{(i)}=0\oplus 0;$$
$$H_2: C_E^{(i)}=1\oplus 1; C_A^{(i)}=1\oplus 1; C_B^{(i)}=0\oplus 0;$$
$$H_3: C_E^{(i)}=1\oplus 1; C_A^{(i)}=0\oplus 0; C_B^{(i)}=1\oplus 1.$$

Зная параметры сетей и d, можно априорно оценить вероятности этих гипотез путем моделирования, многократно повторяя первый этап метода и подсчитывая количество исходов, в которых имело место событие, соответствующее той или иной гипотезе $P(k)\approx\frac{n(k)}{n_c}$, где $k-0,1,2,3$; $n(k)-$ число пар, соответствующее гипотезе H_k, n_c- общее число пар, у которых

$C_E^{(i)} = C_A^{(i)} = C_B^{(i)}$. Для наглядности описываемого процесса на рис. 1 представлены диаграммы, поясняющие распределения пар битов с различными свойствами.

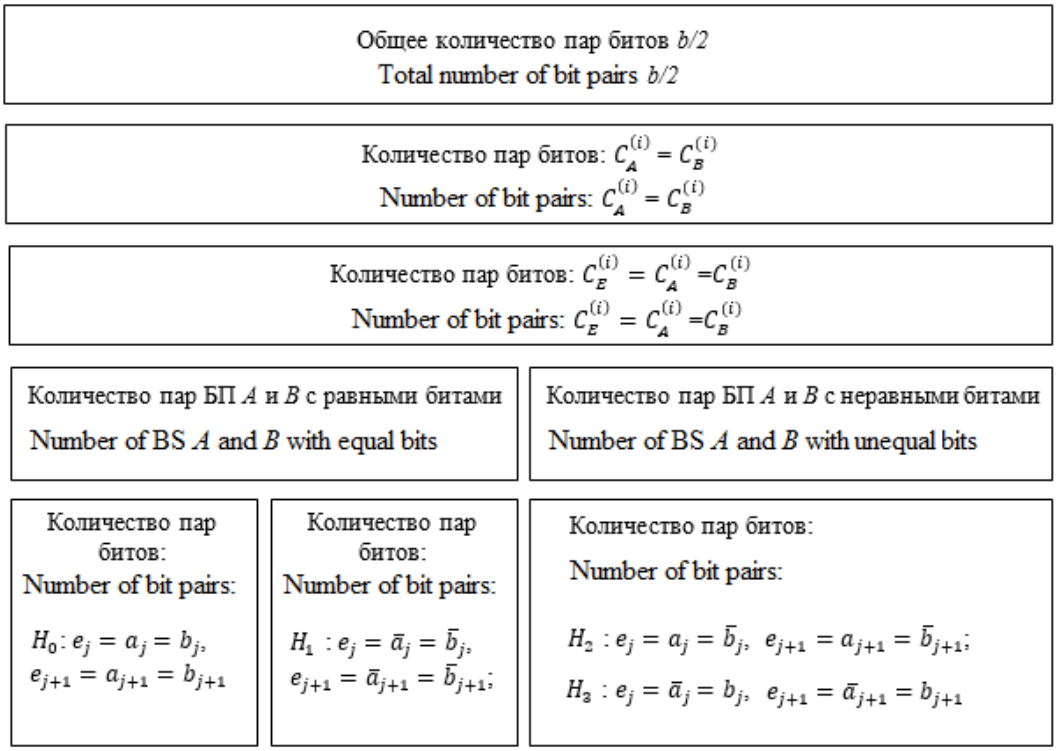

Рис. 1. Диаграммы распределения пар битов с различными свойствами
Fig. 1. Distribution diagrams of couples of bits with the different properties

В табл. 4 приведены результаты моделирования для $K = 3, n = 1000, L = 8, r = 5$.

Таблица 4. Результаты моделирования
Table 4. Simulation results

$P(k)$	d					
	500	1000	2000	2500	3000	10000
$P(0)$	0,257	0,302	0,483	0,501	0,505	0,506
$P(1)$	0,267	0,363	0,457	0,490	0,495	0,493
$P(2)$	0,245	0,214	0,029	0,003	0,001	0,000
$P(3)$	0,245	0,215	0,029	0,003	0,001	0,000

Из всех пар битов, для которых $C_A^{(i)} = C_B^{(i)}$, в итоговую БП $S_r^{AB}(d)$ пройдут только пары, соответствующие гипотезам H_0, H_1. Поэтому E предполагает, что те биты его БП, для которых выполнялось $C_E^{(i)} = C_A^{(i)} = C_B^{(i)}$ и которые у A и B прошли в итоговую БП, с вероятностью $P(0)$ равны битам последовательностей A и B, а с вероятностью $P(1)$ – противоположны им. Однако из табл. 2 видно, что значения вероятностей $P(0)$ и $P(1)$ в диапазоне предлагаемых значений d близки к 0,5, и, следовательно, E не может различить свои отслеживаемые биты. Данное свойство объясняется тем, что корреляция БП $S_r^A(d)$, $S_r^B(d)$ и $S_r^E(d)$ очень слабая и с ростом d $S_r^E(d)$ остается практически статистически независимой от $S_r^A(d)$, $S_r^B(d)$, и, следовательно, в ней число пар, соответствующих гипотезам H_0, H_1, остается одинаковым.

Заключение

По результатам анализа и нейтрализации уязвимостей базового алгоритма формирования криптографического ключа с помощью СИНС удалось создать комбинированный метод. На первом этапе при формировании бинарной последовательности с математическим ожиданием доли несовпадающих битов менее 0,5 добавляется функция свертки, что позволяет обеспечить требуемую конфиденциальность формируемого общего секрета, а также делает данный способ устойчивым к атаке, основанной на знании четностей пар, на втором этапе. Изложенная двухэтапная процедура является, по мнению авторов, достаточно эффективным методом формирования общего секрета. В его основе лежит комбинация полученных ранее результатов. Это позволило существенно сократить количество обменов информацией и повысить криптостойкость по отношению к атаке «отложенный перебор».

Список литературы

1. Пивоваров В.Л., Голиков В.Ф. Способ формирования криптографического ключа для слабо совпадающих бинарных последовательностей. *Информатика*. 2016;3(51):31-37.
2. Shannon C.E. Communication theory of secrecy systems. *Bell system technical journal.* 1949;28(4):656-715.
3. Kanter I., Kinzel W. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing. 2005;5(1):130-140.
4. Ruttor A., Kanter I., Kinzel W. Dynamics of neural cryptography. *Phys. Rev. E.* 2007;75(5):056104.
5. Голиков В.Ф., Радюкевич М.Л. Формирование общего секрета с помощью искусственных нейронных сетей. *Системный анализ и прикладная информатика*. 2019;(2):49-56.
6. Радюкевич М.Л., Голиков В.Ф. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей. *Информатика.* 2020;17(1):102-108.
7. Голиков В.Ф., Ксеневич А.Ю. Атака на синхронизируемые искусственные нейронные сети, формирующие общий секрет, методом отложенного перебора. *Доклады БГУИР*. 2017;(8):48-53.

References

1. Pivovarov V.L., Holikau U.F. [Method of generating common cryptographic keys for loosly coincident binary sequences]. *Informatics*. 2016; 3(51):31-37. (In Russ.)
2. Shannon C.E. Communication theory of secrecy systems. *Bell system technical journal.* 1949;28(4):656-715.
3. Kanter I., Kinzel W. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing. 2005;5(1):130-140.
4. Ruttor A., Kanter I., Kinzel W. Dynamics of neural cryptography. *Phys. Rev. E.* 2007;75(5):056104.
5. Golikov V.F., Radziukevich M.L. [The formation of a common secret using artificial neural networks]. *Sistemnyy analiz i prikladnaya informatika.* 2019;(2):49-56. (in Russ.).
6. 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.)
7. Golikov V.F., Ksenevich A.Y. [Attack on synchronized artificial neural networks, forming a common secret by deferred search]. *Doklady BGUIR = Doklady BGUIR*. 2017;(8):48-53. (In Russ.)

Вклад авторов

Все авторы в равной степени внесли вклад в написание статьи.

Authors' contribution

All authors equally contributed to the writing of the article.

Сведения об авторах

Радюкевич М.Л., м.т.н., начальник испытательной лаборатории по требованиям безопасности информации Государственного предприятия «НИИ ТЗИ».

Голиков В.Ф., д.т.н., профессор кафедры информационных технологий в управлении Белорусского национального технического университета.

Адрес для корреспонденции

220088, Республика Беларусь,
г. Минск, ул. Первомайская, 26, корп. 2,
Государственное предприятие «НИИ ТЗИ»
тел. +375-17-294-01-71;
e-mail: 1218a@list.ru
Радюкевич Марина Львовна

Information about the authors

Radziukevich M.L., M. Sci., Head of the Testing Laboratory for Information Security Requirements of State Enterprise “NII TZI”.

Golikov V.F., D.Sci, Professor of the Information Technologies in Management Department of the Belarusian National Technical University.

Address for correspondence

220088, Republic of Belarus,
Minsk, Pervomayskaya str. 26, bldg. 2,
State Enterprise “NII TZI”
tel. +375-17-294-01-71;
e-mail: 1218a@list.ru
Radziukevich Maryna Lvovna