УДК 004.056.5

ВОЗМОЖНЫЕ УЯЗВИМОСТИ КОМБИНИРОВАННОГО МЕТОДА ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Радюкевич М.Л.[1], аспирант

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Голиков В.Ф. – доктор тех. наук

Аннотация. В статье рассматриваются возможные уязвимости комбинированного метода формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей. Рассмотрена атака «отложенный перебор» и атака, основанная на знании четностей пар. Полученные результаты показали, что благодаря использованию функции свертки на первом этапе экспоненциально увеличивается объем отложенного перебора, а при атаке на втором этапе криптоаналитик не может однозначно различить значения оставшихся битов. Таким образом 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, атака.

Введение. Одной из задач современной криптографии является формирование общего криптографического ключа у абонентов, обменивающихся информацией через открытый для прослушивания канал связи.

В работе [1] предлагается комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей (СИНС). Использование СИНС для формирования общего криптографического ключа предложено В. Кантером, И. Кинцелем и описано в [2-6]. Предлагаемое комбинированное формирование состоит из двух этапов: формирование частично совпадающих бинарных последовательностей с использованием функции свертки результатов нескольких независимых синхронизаций [7, 8] и устранение несовпадающих битов путем открытого сравнения четностей пар битов [9]. Рассмотрим возможные уязвимости комбинированного метода.

На мой взгляд, предлагаемый метод 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 весовых коэффициентов (ВК), синхронизирует (методом отложенного перебора [10]) свою сеть с сетью, например, A в надежде, что его сеть успеет полностью синхронизоваться за отведенное число тактов, обозначим их как $d_{\text{ус}}$. В этом случае окажется, что ключ абонента E и ключ абонента A за отведенное число тактов равны, обозначим это как $K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})$, и сформированный ключ будет полностью дискредитирован.

На втором этапе знание E объявленных четностей пар битов и тот факт, что за счет синхронизации возникает корреляция между $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$, может позволить ему использовать данную информацию для вычисления некоторых битов в итоговой бинарной последовательности (БП).

Любая из этих атак не может быть успешной без наличия критерия, по которому можно удостовериться, что $K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})$. Однако в данной технологии прямая проверка невозможна, но возможна косвенная.

Атака «отложенный перебор». Атака «отложенный перебор» проводится криптоаналитиком E с помощью его искусственной нейронной сети (ИНС), идентичной ИНС A, в течении $d_{\text{ус}}$ тактов.

Так как, первый этап заканчивается только объявлением четностей пар битов бинарных последовательностей A и B, то это не позволяет E сделать однозначный вывод о совпадении $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$ и это усложняет атаку тем, что каждую синхронизацию нужно проводить до завершения второго этапа. И только, если на всех итерациях наблюдается полная идентичность эволюции четностей БП A с B и A с E, то можно считать, что этому предшествовало $K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})$.

Следовательно, вероятность успеха атаки зависит только от вероятности совпадения $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$, т.е. если E удалось синхронизировать свою сеть за $d_{\text{ус}}$ тактов с сетью A, так как все последующие операции не разрушают совпадения ВК сетей E и A.

В таблице 1 приведены результаты анализа вероятностей синхронизации сетей A и E и корреляции ВК сетей E и A, а также их динамика с увеличением числа тактов синхронизации (d). Корреляция ВК рассматривается как относительное среднее число совпадающих битов, обозначим их как $\overline{n_{AB}^{cb}}/b$ и $\overline{n_{EA}^{cb}}/b$, в БП сетей A и B и E и A соответственно. Приведенные данные рассчитывались имитационным моделированием с количеством экспериментов 10^4, при следующих параметрах сетей $n = 1000, K = 3, L_1 = -7, L_2 = 8$, $r = 5$, где n – количество входов каждого персептрона; K – количество персептронов; $\pm L$ – интервал возможных значений весовых коэффициентов персептронов; r – количество строк для функции свертки. Вероятность синхронизации сетей A и B, обозначим как P_{AB}, а сетей E и A - P_{EA}. Вероятности синхронизации сетей при усилении секретности $P_{AB,r}$, $P_{EA,r}$ рассчитывались аналитически по следующим формулам:

$$P_{AB,r} = (P_{AB})^r, \tag{1}$$

$$P_{EA,r} = (P_{EA})^r. \tag{2}$$

Таблица 1. – Вероятность синхронизации сетей A и E и корреляция ВК

d	1000	1200	1500	1800	2000	2500	3000
P_{AB}	0	0	0,005	0,111	0,273	0,736	0,8117
P_{EA}	0	0	0	0,003	0,006	0,032	0,048
$P_{AB,r}$	0	0	$3{,}1*10^{-4}$	$1{,}6*10^{-5}$	0,0015	0,2469	0,352
$P_{EA,r}$	0	0	0	$3*10^{-15}$	$6*10^{-15}$	$2{,}5*10^{-7}$	$3{,}7*10^{-7}$
$\overline{n_{AB}^{cb}}/b$	0,5175	0,5731	0,6756	0,8063	0,8867	0,976	0,9967
$\overline{n_{EA}^{cb}}/b$	0,507	0,509	0,51	0,5072	0,506	0,5033	0,503

Из таблицы 1 видно, что уже при $d > 2000$ относительное среднее число совпадающих битов $\overline{n_{AB}^{cb}}/b$ приближается к 1, в то время как $P_{AB,r}$ остается относительно небольшой. Это объясняется тем, что многие синхронизации получаются не завершенными из-за того, что в них содержится небольшое количество несовпадающих битов.

Оценим вероятность успеха атаки «отложенный перебор». Вероятность этого события равна $P\left(K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})\right) = P_{EA,r}(d_{\text{ус}})$ и зависит от выбора r и $d_{\text{ус}}$. Выбор $d_{\text{ус}}$ обоснован выше. Влияние r рассматривалось в [8], отметим лишь то, что в комбинированном методе за счет увеличения r ослабляется корреляция между $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$, а это очень важно для второго этапа. При этом корреляция между $K^A(d_{\text{ус}})$ и $K^B(d_{\text{ус}})$тоже ослабляется, но гораздо в меньшей степени (таблица 1). Таким образом, выбрав, например, $r = 5, d_{\text{ус}} = 2000$ для обоснованных ранее значений параметров сетей: $n = 1000, K = 3, L_1 = -7, L_2 = 8$, получим $P_{EA,r} = 6 * 10^{-15}$, $\overline{n_{AB}^{cb}}/b = 0{,}8867$, $\overline{n_{EA}^{cb}}/b = 0{,}506$. Полученные результаты свидетельствуют о значительном сокращении числа необходимых тактов обмена информацией (с 3000 до 2000), снижения за счет этого вероятности дискредитации ФОС на несколько порядков (с 10^{-7} до 10^{-15}).

Атака, основанная на знании четностей пар. На втором этапе метода, когда абоненты A и B оглашают четности пар БП (обозначим их C), сформированных с помощью СИНС, у криптоаналитика E появляется возможность сравнения этих четностей с четностями своей БП и сделать определенные выводы относительно формируемого общего секрета. Оценим эффективность атаки, описанной в [9].

Для этого проведем анализ влияния параметров сетей на процесс устранения несовпадающих битов на втором этапе.

Поскольку процедура устранения несовпадающих 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 [9] или методом статистического моделирования.

Если длина БП, сформированных путем синхронизации сетей A и B это b. Тогда число пар равно $D = b/2$, если b окажется нечетным, то его следует привести к четному, отбросив последний бит. Тогда согласно [9], среднее число совпадающих пар битов в анализируемых БП равно

$$m_{c,c} = \overline{(n_{AB}^{cb}/b)}^2 * D \text{ ,} \tag{3}$$

где $\overline{n_{AB}^{cb}}$ – среднее количество совпадающих битов в БП A и B.

Среднее число пар битов, содержащих один совпадающий бит, равно

$$m_{c,\text{н}} = \frac{\overline{n_{AB}^{cb}}}{b}\frac{\left(b-\overline{n_{AB}^{cb}}\right)}{b} * 2D\text{,} \tag{4}$$

Среднее число пар битов, содержащих два несовпадающих бита, равно

$$m_{\text{н,н}} = \frac{\left(b-\overline{n_{AB}^{cb}}\right)^2}{b^2} * D\text{.} \tag{5}$$

Пары, содержащие один совпадающий бит, в дальнейшем согласовании не участвуют, т.к. подлежат удалению. Поэтому представляет интерес только величины $m_{c,c}$ и $m_{\text{н,н}}$. В таблице 2 приведены значения этих величин в зависимости от среднего количества совпадающих битов для бинарных последовательностей длиной $b = 12000$.

Таблица 2. – Значения величины $m_{c,c}$ и $m_{\text{н,н}}$ в зависимости от количества совпадающих битов

$\overline{n_{AB}^{cb}}/b$	0,500	0,583	0,666	0,750	0,833	0,9166	1,000
$m_{c,c}$	1500	2041	2666	3375	4166	5401	6000
$m_{\text{н,н}}$	1500	1041	666	375	166	41	0
$m_{c,c} + m_{\text{н,н}}$	3000	3082	3332	3750	5832	5442	6000

Четность пар бит обозначим через $C_i^{A/B/E} = k_j \oplus k_{j+1}$, где i – номер пары, k_j – j-й бит БП. После остановки синхронизации и оглашения четностей пар битов E знает, что A и B оставят для дальнейшего рассмотрения только пары, у которых четности совпадают $C_i^A = C_i^B$. Поэтому E будет рассматривать только те свои пары битов, для которых выполняется $C_i^E = C_i^A = C_i^B$. Для битов каждой из этих пар E может выдвинуть следующие гипотезы:

$$H_0\text{: } k_j^E = k_j^A = k_j^B, k_{j+1}^E = k_{j+1}^A = k_{j+1}^B;$$

$$H_1: k_j^E = \overline{k_j^A} = \overline{k_j^B},\ k_{j+1}^E = \overline{k_{j+1}^A} = \overline{k_{j+1}^B};$$

$$H_2: k_j^E = k_j^A = \overline{k_j^B},\ k_{j+1}^E = k_{j+1}^A = \overline{k_{j+1}^B};$$

$$H_3: k_j^E = \overline{k_j^A} = k_j^B,\ k_{j+1}^E = \overline{k_{j+1}^A} = k_{j+1}^B.$$

Гипотеза H_0 означает, что биты пар E равны битам пар A, которые равны битам пар B. Гипотеза H_1 означает, что биты пар E противоположны битам пар A, которые равны битам пар B. Гипотеза H_2 означает, что биты пар E равны битам пар A, которые противоположны битам пар B. Гипотеза H_3 означает, что биты пар E противоположны битам пар A, которые противоположны битам пар B. Например,

$$H_0: C_i^E = 1 \oplus 1; C_i^A = 1 \oplus 1; C_i^B = 1 \oplus 1;$$

$$H_1: C_i^E = 1 \oplus 1; C_i^A = 0 \oplus 0; C_i^B = 0 \oplus 0;$$

$$H_2: C_i^E = 1 \oplus 1; C_i^A = 1 \oplus 1; C_i^B = 0 \oplus 0;$$

$$H_3: C_i^E = 1 \oplus 1; C_i^A = 0 \oplus 0; C_i^B = 1 \oplus 1.$$

Зная параметры сетей и $d_{\text{ус}}$, E может 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

$$P(\vartheta) \approx \frac{n(\vartheta)}{n_\Sigma}, \quad (6)$$

где ϑ – номер гипотезы, $\vartheta = 0,1,2,3$; $n(\vartheta)$ - число пар, соответствующее гипотезе H_ϑ ,n_Σ – общее число пар, у которых $C_i^E = C_i^A = C_i^B$.

В таблице 3 приведены результаты моделирования для $\text{К} = 3, n = 1000, L_1 = -7,\ L_2 = 8, r = 5$.

Таблица 3 – Результаты моделирования при $r = 5$

$P(\vartheta)$	$d_{\text{ус}}$					
	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

В таблице 4 приведены результаты моделирования для $\text{К} = 3, n = 1000, L_1 = -7,\ L_2 = 8, r = 10$.

Таблица 4 – Результаты моделирования при $r = 10$

$P(\vartheta)$	$d_{\text{ус}}$					
	500	1000	2000	2500	3000	10000
$P(0)$	0,2494	0,2584	0,4433	0,4887	0,4991	0,5011
$P(1)$	0,2495	0,2558	0,4404	0,4883	0,4964	0,4988
$P(2)$	0,2496	0,2426	0,0584	0,0147	0,0018	0,000

$P(3)$	0,2451	0,2430	0,0578	0,0153	0,0020	0,000

Для наглядности структуры БП на рисунке 1 представлены диаграммы, поясняющие распределения пар битов с различными свойствами.

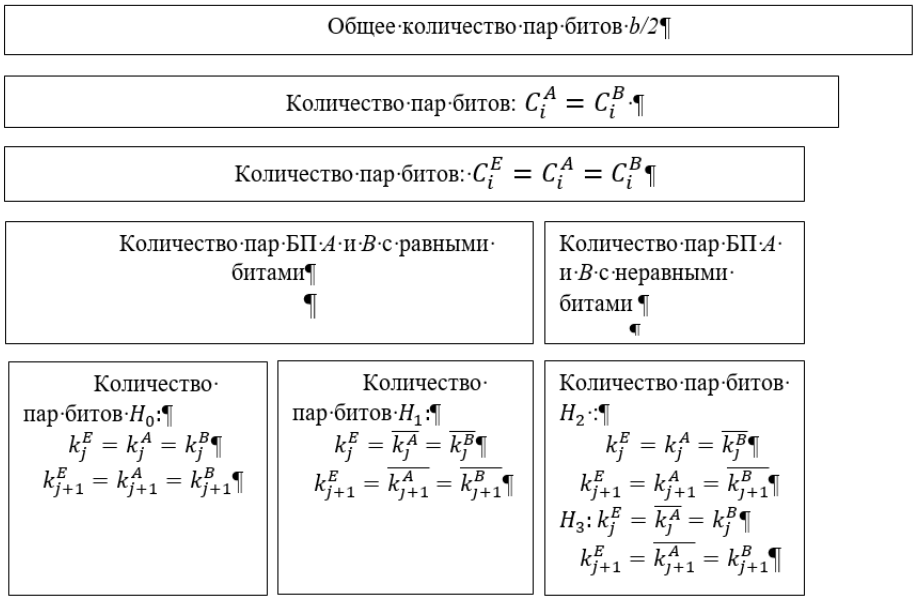

Рисунок 1. – Диаграммы распределения пар битов с различными свойствами

Из всех пар битов, для которых $C_i^A = C_i^B$, в итоговую БП $K^{AB}(d_{\text{ус}})$ пройдут только биты пар, соответствующие гипотезам H_0, H_1. Поэтому E предполагает, что те биты его БП, для которых выполнялось $C_i^E = C_i^A = C_i^B$ 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 таблицы 4 видно, что значения вероятностей $P(0)$ и $P(1)$ в диапазоне предлагаемых значений d и при $r \geq 5$ одинаковы между собой и близки к 0,5, следовательно, для E значения отслеженных битов равновероятны. Данное свойство объясняется, тем, что корреляция БП $K^A(d_{\text{ус}})$, $K^B(d_{\text{ус}})$ и $K^E(d_{\text{ус}})$ очень слабая и с ростом d $K^E(d_{\text{ус}})$ остается практически статистически независимой от $K^A(d_{\text{ус}})$, $K^B(d_{\text{ус}})$ и, следовательно, в ней число пар, соответствующих гипотезам H_0, H_1, остается одинаковым. Следовательно, атака, использующая знание четностей БП, сформированных A и B комбинированным методом, при правильно выбранных параметрах сетей не позволяет дискредитировать ФОС.

Заключение. Рассмотрев возможные уязвимости комбинированного метода формирования криптографического ключа с помощью СИНС можно сделать следующий вывод. На первом этапе при формировании частично совпадающих бинарных последовательностей благодаря использованию функции свертки экспоненциально увеличивается объем отложенного перебора, что позволяет обеспечить требуемую конфиденциальность формируемого общего секрета, а также делает данный способ устойчивым к атаке, основанной на знании четностей пар, на втором этапе. Таким образом комбинированный метод позволяет существенно сократить количество обменов информацией и повысить криптостойкость по отношению к атаке «отложенный перебор» по сравнению с технологией Neural key generation.

Список использованных источников:

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. Kinzel, W. Neural Cryptography / W.Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

3. 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.

4. 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.

5. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.

6. 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.

7. 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.

8. 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.

9. Пивоваров В.Л., Голиков В.Ф. Способ формирования криптографического ключа для слабо совпадающих бинарных последовательностей. Информатика, № 3(51), 2016.Стр. 31-37.

10. Голиков В.Ф. Атака на синхронизируемые исскуственные нейронные сети, формирующие общий секрет, методом отложенного перебора /В.Ф. Голиков, А.Ю. Ксеневич //Доклады БГУИР, №8, 2017. С48-53.

UDC 004.056.5

POSSIBLE VULNERABILITIES OF THE COMBINED METHOD FOR FORMING A CRYPTOGRAPHIC KEY USING SYNCHRONIZED ARTIFICIAL NEURAL NETWORKS

Radziukevich M.L.[1], аспирант

Belarusian State University of Informatics and Radioelectronics[1]

Minsk, Republic of Belarus

Golikov V.F. – doctor of tech. sciences

Annotation. The article discusses possible vulnerabilities of the combined method of generating a cryptographic key using synchronized artificial neural networks. The «delayed enumeration» attack and the attack based on the knowledge of the parity of pairs are considered. The results obtained showed that due to the use of the convolution function at the first stage, the amount of deferred enumeration increases exponentially, and during the attack at the second stage, the cryptanalyst cannot unambiguously distinguish the values of the remaining bits. Thus, the combined method makes it possible to increase the confidentiality of the generated shared secret and significantly reduce the number of information exchanges compared to the Neural key generation technology.

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