ОТЗЫВ

официального оппонента о диссертационной работе Радюкевич Марины Львовны «Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19: Методы и системы защиты информации, информационная безопасность

1. *Соответствие диссертации специальности и отрасли науки, по которым она представлена к защите.*

Диссертация соответствует специальности 05.13.19: Методы и системы защиты информации, информационная безопасность по п.п. Паспорта данной специальности:

П.3. Методы и алгоритмы для анализа и синтеза криптографических, стеганографических преобразований информации, криптографические и стеганографические протоколы. Разработка новых и повышение эффективности существующих средств криптографической защиты информации на основе шифрования, применения электронной цифровой подписи, управления доступом, контроля целостности, генерации и использования ключевой информации.

П.5. Разработка новых и повышение эффективности существующих технических и программных средств защиты информации, средств контроля защищенности информации и обеспечения информационной безопасности.

Диссертация соответствует отрасли «технические науки».

2. *Актуальность темы диссертации.*

Как подчеркивается в Концепции информационной безопасности Республики Беларусь (утверждена Постановлением Совета Безопасности Республики Беларусь18.03.2019, №1), «Национальная система обеспечения кибербезопасности должна реализовывать весь возможный комплекс правовых, организационных и технических мер по обеспечению безопасности национальной информационной инфраструктуры, в том числе информационных систем, обеспечивать конфиденциальность, доступность и целостность информации, а также легко трансформироваться и адаптироваться в изменяющейся обстановке за счет постоянного анализа на предмет соответствия актуальным рискам кибербезопасности» (п. 63).

Цели и задачи анализируемой диссертационной работы сформулированы в полном соответствии с требованиями Концепции.

Кроме того, тема диссертации соответствует приоритетным направлениям научной, научно-технической и инновационной деятельности на 2021-2025 гг. по п. 6: Обеспечение безопасности человека, общества и государства: средства технической и криптографической защиты

информации, криптология и кибербезопасность.

Указанное соответствует п. 21 Положения «О присуждении ученых степеней и присвоении ученых званий» (Указ Президента Республики Беларусь от 23 июня 2023г. №180).

В силу указанных обстоятельств тему диссертации следует отнести к актуальным.

3. *Степень новизны результатов диссертации и научных положений, выносимых на защиту.*

Диссертационная работа Радюкевич М. Л. содержит новые, научно обоснованные результаты, заключающиеся в следующем.

3.1 Предложен новый подход в выборе диапазона изменения весовых коэффициентов в скрытом слое нейронов двух нейронных сетей в виде известной трехуровневой древовидной машины четности (TPM – Tree Parity Machine), используемой для согласования двумя абонентами общего секрета (криптографического ключа): вместо [–L, L] предложено использовать [–L+1, L], где L – целые числа, что снижает ожидаемое время (количество шагов) наступления состояния синхронизации при сохранении равномерного характера распределения чисел в сформированной сторонами общей секретной последовательности и тем самым, должно обеспечить повышение устойчивости процедуры синхронизации к атакам третьей стороны (глава 2 диссертации).

3.2 Обоснованы и разработаны новые методы синхронизации двух сетей TPM, отличающиеся использованием двухэтапных алгоритмов реализации процесса синхронизации, в частности:

- метод, предусматривающий выполнение нескольких (r) неполных процедур синхронизации сетей TPM за фиксированное число шагов – на первом этапе, и применение специальной функции отображения (сжатия) для формирования общей ключевой последовательности, состоящей из r блоков – на втором этапе, что позволяет сократить общее количество шагов всего процесса синхронизации сетей (глава 3 диссертации);

- метод, основанный на выполнении заведомо недостаточного для синхронизации сетей TPM числа шагов – на первом этапе, и поиск (с исключением) несовпадающих символов в сформированных на первом этапе ключевых последовательностях двоичного вида в обеих сетях, что обеспечивает повышение устойчивости процесса синхронизации к некоторым видам атак (глава 4 диссертации).

При этом оценка процесса синхронизации сетей выполняется на основе математического аппарата корреляционного анализа.

4. *Обоснованность и достоверность выводов и рекомендаций, сформулированных в диссертации.*

4.1 Основные выводы диссертационного исследования, касающиеся сущности предложенных методов согласования общего секрета двумя нейронными сетями на основе архитектуры TPM, а также формального описания основных преобразований, касающихся процесса синхронизации сетей, являются обоснованными и достоверными.

4.2 Принципиально новым является использование корреляционного анализа для оценки криптостойкости процесса синхронизации сетей TPM; традиционная практика – анализ отношения времени синхронизации легитимных сетей TPM (t_{synch}) ко времени успешной атаки третьей стороны (t_{learn}), либо – наоборот.

4.3 Математической и алгоритмической основой метода, описанного в гл. 3, является содержание статьи (п. 57 списка использованных источников)

Generalized privacy amplification / C. H. Bennett [et al.] // IEEE Transaction on Information Theory. – 1995. – Vol. 41, № 6. – P. 1915–1923,

что автор собственно косвенно и подтверждает ссылкой на эту публикацию на с. 52.

4.3 Отдельные выводы повторяют известные либо не требуют доказательств, например:

- все выводы после гл.1;
- выводы 1-3 после гл 2; их можно найти (частично или в полном объеме), например, в работах [23, 26, 29, 30,–39, 43] и др.

5. *Научная, практическая, экономическая и социальная значимость результатов диссертации с указанием рекомендаций по их использовании.*

Научная значимость. Результаты диссертации являются расширением существующей теории построения и функционирования связанных единой задачей двух нейронных сетей на основе архитектуры TPM на основе алгебры действительных чисел.

Практическая значимость. Предложенные методы доведены до уровня практической реализации в виде законченного программного продукта.

Экономическая и социальная значимость. Заключаются в подтвержденном использовании результатов работы в учебном процессе при подготовке специалистов в области информационной безопасности.

6. *Опубликованность результатов диссертации в научной печати.*

По результатам выполненных исследований опубликовано 12 научных работ общим объемом 4,6 авторского листа (а. л.). Из них 4 статьи объемом 2,3 а. л. – в рецензируемых научных журналах в соответствии с

п. 19 Положения о присуждении ученых степеней и присвоении ученых званий, 6 публикаций – в материалах и сборниках трудов научно-технических конференций объемом 2,15 а. л., тезисы 2 докладов на НТК объемом 0,15 а. л.

К числу наиболее значимых следует отнести:

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. 102–108.

Радюкевич, М. Л. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Доклады Белорус. гос. ун-та информатики и радиоэлектроники. – 2021. – Т. 19, № 1. – С. 79–87.

Опубликованные работы отражают сущность основных результатов диссертационного исследования и положений, выносимых на защиту.

Указанное соответствует требованиям п.19 Положения «О присуждении ученых степеней и присвоении ученых званий».

7. *Соответствие оформления диссертации требованиям ВАК.*

Рукопись диссертации оформлена в соответствии с основными требованиями ВАК.

Содержание автореферата соответствует содержанию рукописи диссертации.

8. *Замечания по диссертации.*

8.1 Выбор и обоснование вероятностных характеристик безопасности процессов синхронизации сетей ТРМ (п. 2.1, с. 36-38) выполняются автором на основе анализа *сложных событий* (термин, используемый автором диссертации) при наличии между ними «корреляции» (второй абзац на с. 37). Речь идет о распределении случайной величины t_{AB} (t_{synch} – период времени, за который наступает состояние синхронизации двух легитимных ТРМ: А и В) и распределении случайной величины t_{AE} (t_{learn} – период времени, за который наступает состояние синхронизации одной из легитимных ТРМ, А, и атакующей сети, Е). При этом автор ссылается на известную книгу:

Вентцель, Е. С. Теория вероятностей : учебник для вузов /Е. С. Вентцель. – 4-е изд., стер. – М.: Наука, 1969.

В основе анализа – соотношение (2.1), определяющее вероятность сложного события:

$$P(t_{AB} \le d,\ t_{AE} > d) = P(t_{AB} \le d)\ P(t_{AE} > d \mid t_{AB} \le d\ ).$$

Далее автор рассматривает «сильную (100%-ю) корреляцию».

Здесь следует подчеркнуть, что у Вентцель Е.С. корреляционный анализ вероятностных (стохастических) зависимостей, как это принято обычно, выполняется на основе рассмотрения корреляционных моментов или коэффициента корреляции.

Надо полагать, что 100%-я корреляция у автора диссертации соответствует коэффициенту корреляции равному 1. В этом случае наступление события $t_{AB} \le d$ обязательно ведет к наступлению события $t_{AE} > d$. А это означает, что условная вероятность $P(t_{AE} > d \mid t_{AB} \le d\ ) = 1$. И тогда

$$P(t_{AB} \le d,\ t_{AE} > d) = P(t_{AB} \le d),$$

а не $P(t_{AB} \le d,\ t_{AE} > d) \sim 0$ (см. формулу (2.2) в диссертации).

При «слабой корреляции» (видимо, при коэффициенте корреляции близком к 0 или равном 0: наступление события $t_{AB} \le d$ практически исключает наступление события $t_{AE} > d$) условная вероятность равна 0:

$$P(t_{AE} > d \mid t_{AB} \le d\ ) = 0.$$

И тогда $P(t_{AB} \le d,\ t_{AE} > d) \sim 0$, а не

$$P(t_{AB} \le d,\ t_{AE} > d) = P(t_{AB} \le d)\ P(t_{AE} > d),$$

как в диссертации (см. (2.3)).

Рассмотренное касается также соотношений (2.4) – (2.6).

8.2 Известны, помимо проанализированных в диссертации, также генетическая и вероятностные атаки на синхронизируемые TPM (см., например, [23] списка источников в диссертации:

Klimov, A. Analysis of neural cryptography / A. Klimov, A. Mityagin, A. Shamir // Advances in Cryptology - ASIACRYPT 2002 : 8th Intern. Conf. on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1–5, 2002. – Berlin, 2002. – P. 288–298;

а также [39]:

Ruttor, A. Neural Synchronization and Cryptography : diss. …naturwissenschaftlichen Doktorgrades / A. Ruttor; Bayerischen Julius-Maximilians-Universit¨at W¨urzburg. – Wurzburg, 2006. – 121 p.

Автор диссертации ограничился рассмотрением только простой и геометрической атак (из достаточно подробно изученных) применительно к

предложенным методам. При этом автором не проводился сравнительный анализ эффективности (или неэффективности) атак на сети TPM при определенных и изменяющихся параметрах (*K-N-L*) этих сетей на основе правил обучения, отличных от обучения по Хэббу.

8.3 В литературе (см., например, [43] списка источников:

Плонковски, М. Модели передачи и криптографического преобразования информации на основе нейросетевых технологий и расширения поля используемых чисел : дис. … канд. техн. наук : 05.13.19 / М. Д. Плонковски; Белорус. гос. технолог. ун-т. – Минск, 2008,

а также

Ying Zhang, Weihua Wang and Huisheng Zhang. Neural Cryptography Based on Quaternion-Valued Neural Network/ International J. of Innovative Computing, Information and Control. – 2022. – V.6, no.22, pp. 1871–1883. DOI: 10.24507/ijicic.18.06.1871,

Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович; Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – Минск: БГТУ. – 2005. – С. 161–164),

рассмотрены архитектуры TPM на основе расширения алгебры действительных чисел (комплексные числа, кватернионы и октонионы), которые обеспечивают более высокий уровень устойчивости ко всем видам атак в сравнении с архитектурами на основе алгебры действительных чисел, которую использует автор диссертации.

В диссертации никак не сравниваются предложенные автором решения с известными из указанных в данном пункте архитектурами TPM.

Указанные замечания влияют на общую оценку рецензируемой диссертационной работы, которая, тем не менее, в целом является положительной.

9. *Соответствие научной квалификации соискателя ученой степени, на которую он претендует.*

На основе анализа содержания диссертации, автореферата и других материалов (содержание публикаций соискателя, справки об использовании результатов диссертации), а также личной беседы с соискателем можно заключить, что научная квалификация Радюкевич М. Л. Соответствует степени кандидата технических наук.

10. Общее заключение по диссертации.

Диссертационная работа Радюкевич Марины Львовны по содержанию соответствует специальности и отрасли науки, по которой она представлена, является самостоятельно выполненной квалификационной научной работой,

имеющей внутреннее единство и свидетельствующей о личном вкладе автора в науку, посвящена решению актуальной научной задачи по разработке эффективных методов и средств криптографической защиты информации, содержит новые научные результаты и имеет практическую ценность, что соответствует требованиям пп. 19–22 Положения «О подготовке и аттестации научных работников высшей квалификации».

Соискателю может быть присуждена ученая степень кандидата технических наук по специальности 05.13.19: «Методы и системы защиты информации, информационная безопасность» за новые научно обоснованные результаты, совокупность которых имеет важное значение для развития указанного научного направления, включающие:

методы синхронизации двух нейронных сетей, используемых для формирования общего секретного криптографического ключа на основе архитектуры «древовидной машины четности», общее отличие которых от известных состоит в использовании двухэтапных алгоритмов реализации процесса синхронизации и использовании математического аппарата корреляционного анализа для оценки криптостойкости алгоритмов:

- метод, отличающийся также выполнением нескольких (r) неполных процедур синхронизации сетей за фиксированное число шагов – на первом этапе, и применением специальной функции отображения (сжатия) для формирования общей секретной последовательности, состоящей из r блоков – на втором этапе, что позволяет сократить длительность процесса синхронизации сетей и тем самым – повысить криптостойкость алгоритма;

- метод, отличающийся также выполнением сетями заведомо недостаточного для их синхронизации числа шагов – на первом этапе, и поиском (с исключением) в обеих сетях несовпадающих символов в сформированных на первом этапе секретных последовательностях двоичного вида, что обеспечивает повышение устойчивости процесса синхронизации к некоторым видам атак на сети.

Профессор кафедры
информационных систем и технологий
Белорусского государственного
технологического университета
д.т.н., профессор П. П. Урбанович

Подпись Урбановича П.П.
Свидетельствую:
Начальник отдела кадров БГТУ
«27» 09 2023 г.

Ознакомлена /Радюкевич М.М./
02.10.2023

Совет по защите диссертаций при БГУИР
«02» октября 2023 г.
Вх. № 05.02-11/165