УТВЕРЖДАЮ
Директор
Научно-исследовательского
учреждения «Институт
прикладных физических проблем
имени А.Н.Севченко»
Белорусского государственного
университета, д.ф.-м.н.
_____ П.В.Кучинский
«06» 10 _____ 2023г.

Отзыв

оппонирующей организации на диссертационную работу и автореферат Радюкевич Марины Львовны «Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для криптографических применений», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность

Цифровизация всех направлений деятельности общества, широкое развитие и использование информационных технологий требует обеспечения подлинности, целостности и доступности информационных ресурсов. Для решения этой задачи широко используются криптографические методы. Как правило, алгоритмы криптопреобразования не являются секретными, а стойкость информационных систем к атакам определяется криптостойкостью ключа. В этой связи изучение возможности формирования секретного ключа с помощью синхронизируемых искусственных нейронных сетей представляется актуальной задачей.

Соответствие содержания диссертации заявленной специальности и отрасли науки

Содержание диссертационной работы полностью соответствует отрасли «технические науки» и паспорту специальности 05.13.19 – методы и системы защиты информации, информационная безопасность. Представленные в ней результаты входят в области исследований, предусмотренные паспортом данной специальности, раздела III, пункты:

3. Методы и алгоритмы для анализа и синтеза криптографических, стеганонографических 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.

6. Модели, методы, средства обеспечения аудита и мониторинга безопасности информации в системах различного назначения. Методы и системы противодействия угрозам информационной безопасности в открытых компьютерных сетях. Обеспечение безопасности информационных технологий, включая электронный документооборот, электронную коммерцию, электронную почту, электронные платежные системы, телекоммуникационные и информационные системы.

Научный вклад соискателя в решение научной задачи

Важной задачей при использовании криптографических методов защиты информации является задача обеспечения секретными ключами абонентов системы. Эта задача решается в настоящее время методами асимметричной криптографии, однако ведутся исследования по поиску других методов, использующие иные принципы. Таким направлением является метод формирования общего секретного ключа с помощью синхронизируемых искусственных нейронных сетей (СИНС).

В диссертационной работе Радюкевич М.Л. предложено решение важной научно-технической задачи связанной с повышением конфиденциальности общего секрета для криптографических применений, формируемого с использованием СИНС. Разработаны методы повышения конфиденциальности формирования общего секрета, которые обеспечивают существенное уменьшение корреляции между результатами синхронизации сетей аутентифицированных абонентов и атакующей сетью, путем применения либо интеграции результатов многократно повторяемых синхронизаций, либо двухэтапной процедуры, включающей неполную синхронизацию искусственных нейронных сетей аутентифицированных абонентов на первом этапе и согласование этих последовательностей по методу согласования слабо совпадающих бинарных последовательностей на втором этапе. Данные методы являются новыми.

Практическое значение результатов исследований

Практическая значимость заключается в разработке алгоритмов формирования ключевой информации на основе СИНС, отличающихся простотой реализации, не требующих большого объема предварительных вычислений.

Предложенный комбинированный метод с секретной модификацией результатов синхронизации для формирования общего секрета (ФОС) с помощью СИНС может использоваться как метод распределения ключевой информации абонентам сети без применения классических односторонних функций. Реализация данного метода может служить основой при разработке криптографических приложений.

Внедрение результатов диссертации подтверждено актом о практическом использовании результатов исследований в ОКР «Невод» и актом внедрения результатов исследования в учебный процесс.

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

Научная квалификация Радюкевич М.Л. соответствует ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность. Это подтверждается уровнем и результатами проведенных им исследований, приведенных в диссертации и научных публикациях. По материалам диссертационной работы опубликовано 4 статьи в рецензируемых научных журналах в соответствии с пунктом 19 Положения о присуждении ученых степеней и присвоении ученых званий, 6 публикаций в материалах и сборниках трудов научных конференций, 2 тезиса докладов на научных конференциях. В опубликованных работах полностью отражены выносимые на защиту положения и выводы, которые сформулированы в диссертации.

Замечания:

1. В диссертации соискатель реализует метода формирования общего секрета с использованием синхронизируемых нейронных сетей простой архитектуры – многослойного персептрона с одним скрытым слоем с дискретными весами. Данный метод синхронизации нейронных сетей был предложен в 2002 году, и в последнее время неоднократно подвергался критике ввиду слабой устойчивости к атакам различного рода. Соискатель также отмечает, что «многие авторы пошли по пути серьезной модификации метода, используя более сложные искусственные нейронные сети и алгоритмы обучения (стр. 14)». В то же время делается необоснованный вывод о том, что «принципиальные усложнения технологии лишают ее простоты и прозрачности для практического применения». Это является неверным утверждением, так как в данный момент существует большое количество программных реализаций базовых блоков построения сложных нейронных сетей, как с закрытым, так и с открытым исходным кодом, что позволяет провести аудит безопасности используемого кода.
2. Ограничением практического применения разработанных методов формирования общего секрета является исходное предположение аутентифицированного канала связи.
3. Как уже отмечалось ранее, качество ключевой последовательности определяет криптостойкость системы. Отсутствие детального исследования статистических свойств (равновероятность, независимость) формируемых двоичных последовательностей ограничивает широкое внедрение разработанных автором методов ФОР.
4. В формуле 2.9 на стр.39 имеется неточность.
5. Не совсем понятно, зачем автор на стр.89-93 приводит рисунки графических интерфейсов, когда ниже в тех же параметрах приводятся результаты моделирования.

Заключение

Диссертация Радюкевич М.Л. на тему «Формирование общего секрета с помощью синхронизируемых искусственных нейронных сетей для

криптографических применений» является законченной научной работой. Приведенные выше замечания не оказывают существенного влияния на качество и значимость диссертационного исследования.

Автор диссертации Радюкевич М.Л. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность за новые методы формирования общего секрета повышенной конфиденциальности и быстродействия по сравнению с классической технологией Synchronization of Neural Networks, что позволяет использовать СИНС как инструмент формирования криптографических ключей в современных криптографических системах.

Доклад соискателя и отзыв эксперта были заслушаны и обсуждены 05.10.2023 на заседании научно-технического совета Научно-исследовательского учреждения «Институт прикладных физических проблем имени А.Н.Севченко» Белорусского государственного университета (протокол № 6 от 05.10.2023).

На заседании присутствовали 14 членов совета, из них 5 – с ученой степенью доктора наук и 9 – с ученой степенью кандидата наук: Беляев Б.И. д.ф.-м. н., Кучинский П.В. д.ф.-м.н., Комаров Ф.Ф. д.ф.-м.н., Дудчик Ю.И. к.ф.-м.н., Попков А.П. к.т.н., Катковский Л.В. д.ф.-м.н., Семененко Л.В., к. т.н., Самцов М.П. д.ф.-м.н., Цикман И.М.к.т.н.,Кныш В.П. к.т.н., Романов А.Ф. к.т.н., Мальцев М.В. к.ф.-м.н., Пузырев М.В., к.ф.-м.н., Беляев Ю.В. к. т.н.

Отзыв оппонирующей организации после обсуждения принят открытым голосованием членов научно-технического совета Научно-исследовательского учреждения «Институт прикладных физических проблем имени А.Н.Севченко» Белорусского государственного университета, имеющих ученые степени.

Результаты голосования членов научно-технического совета: за – 14, против – нет, воздержавшихся – нет.

Председатель
научно-технического совета, д.ф.-м.н. Беляев Б.И.

Эксперт, к.т.н Семененко Л.В.

Секретарь, к.т.н. Романов А.Ф.

Ознакомлена Радюкевич М.Л.
11.10.2023

Совет по защите диссертаций при БГУИР
«11» октября 2023 г.
Вх. № 05.02-11/184