ОТЗЫВ

на автореферат диссертации М.Л. Радюкевич
«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

Диссертационная работа посвящена протоколам формирования общего секрета с помощью синхронизируемых искусственных нейронных сетей (СИНС). СИНС – это сравнительно новая и все еще слабоизученная криптографическая платформа. Идея СИНС (в несколько другой, авторской форме) была в свое время сообщена рецензенту научным руководителем диссертации. Идея выглядит парадоксально: оказывается, стороны, начиная с любых собственных секретных состояний, могут добиться их совпадения, причем добиться так, что противнику будет трудно совпадающие состояния определить, даже если противник будет повторять синхронизацию.

Привлекательные черты платформы СИНС:

– гарантии стойкости протоколов СИНС не базируются на сложности трудных вычислительных задач (протоколы претендуют на звание постквантовых);
– низкая вычислительная сложность.

Недостатки платформы:

– высокая коммуникационная сложность (для синхронизации требуется большое число пересылок между сторонами);
– щадящая модель противника (противник только прослушивает канал связи, он не может изменять данные в канале);
– гарантии стойкости недостаточно весомы;
– недостаточно проработаны правила практического применения.

Первые два недостатка, по-видимому, являются неотъемлемыми чертами платформы. В диссертационной работе ведется работа по преодолению последних двух недостатков.

Во-первых, М.Л. Радюкевич предложила метод снижения корреляции ключей противника и легитимной стороны за счет r-кратного повтора сеансов синхронизации с последующим объединением результатов по определенным правилам.

В-вторых, в работе предложен способ повышения корреляции ключей легитимных сторон, вплоть до их полного совпадения, в рамках итерационной процедуры взаимоисключения несовпадений.

Замечания:

1. Символ l («эль маленькое») впервые встречается на стр. 8 без пояснений. Можно предположить, что $l = \log\_2 (2L + 1)$. Об этом следует сказать явно.
2. В абзаце 1 на стр. 9 допускается, что с вероятностью 0.045 пассивный противник синхронизируется с одной из сторон протокола, а, следовательно, и со второй стороной. Другими словами, противник найдет общий ключ с вероятностью 0.045 сторон за небольшое вычислительное время, располагая только данными перехвата. В криптографии криптосистема с k-битовым ключом счи-

тается надежной, если вероятность успеха атаки по определению ключа сравнима с $1/2^k$. В связи с этим вероятность успеха 0.045 представляется чрезмерно большой.

3. Таблица 2, последняя колонка. Странно, что вероятности не уменьшаются монотонно.

Отмеченные замечания не влияют на общую положительную оценку работы.

Считаю, что диссертационная работа отвечает требованиям, предъявляемым к кандидатским диссертациям по специальности 05.13.19 — методы и системы защиты информации, информационная безопасность, – а ее автор М.Л. Радюкевич заслуживает присуждения ученой степени кандидата технических наук.

Зав. лабораторией
Научно-исследовательского института
прикладных проблем математики и информатики
Белорусского государственного университета,
канд. физ.-мат. наук С.В. Агиевич

Я, Агиевич Сергей Валерьевич, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела М.Л.Радюкевич.

Агиевич Сергей Валерьевич

Личную подпись Агиевича С.В. удостоверяю
Ведущий специалист по кадрам НИИ прикладных проблем математики и информатики Ротина М.В.
«25» 10 2023 г.

Совет по защите диссертаций при БГУИР
«25» 10 2023 г.
Вх. № 05.02-11/246

Ознакомлена Радюкевич М.Л.
25.10.2023