УДК 004.056

О ПРИМЕНИМОСТИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ, ОСНОВАННЫХ НА ИЗОГЕНИЯХ, В РАБОТЕ НА УСТРОЙСТВАХ С ОГРАНИЧЕННЫМИ РЕСУРСАМИ

Максимова А.Ю. (ИТМО)
Научный руководитель – кандидат технических наук, преподаватель ФБИТ Давыдов В.В. (ИТМО)

Введение. Для обеспечения безопасности устройств с ограниченными ресурсами, широко применяемых в концепции Интернета вещей, требуются облегченные криптографические протоколы и примитивы [1, 2]. Но квантовые компьютеры смогут взломать традиционные примитивы и протоколы. Постквантовые протоколы, основанные на изогениях, представляют собой одно из перспективных направлений в области криптографии. Актуальность применения постквантовых протоколов на основе изогений для устройств Интернета вещей заключается в том, что эти протоколы могут работать с небольшими ключами, что является одним из ключевых моментов для устройств с ограниченным количеством памяти.

Основная часть. Изогении — это отображения между эллиптическими кривыми, которые используются для построения криптографических протоколов, обеспечивающих безопасность передачи данных. Протоколы на основе изогений обычно используются для обмена ключами, аутентификации и обеспечения конфиденциальности данных. Были рассмотрены различные протоколы, основанные на изогениях. Была проанализирована возможность их применения для устройств с ограниченными ресурсами. Протоколы SIDH и SIKE не могут быть использованы из-за их взлома [3], но протокол M-SIDH [4] – протокол для обмена ключами, может быть использован для устройств с ограниченными ресурсами. Также были рассмотрены и другие протоколы, основанные на изогениях, например, OSIDH [5, 6] и CSIDH [7]. При излишнем уменьшении параметров у протоколов может упасть стойкость к атакам [7], соответственно необходимо подбирать размер параметров протокола исходя из соотношений безопасности и ограниченности ресурсов устройства.

Выводы. Была рассмотрена возможность применения криптографических протоколов, основанных на математическом аппарате изогений, для устройств с ограниченными ресурсами. Помимо устойчивости к атакам квантового компьютера данные протоколы обладают важной характеристикой – масштабируемостью, то есть они могут работать с небольшими ключами, что безусловно является одним из ключевых моментов в работе с данными устройствами.

Список использованных источников:

1. Kumar A., Ottaviani C., Gill S. S., Buyya R. Securing the future internet of things with post-quantum cryptography // SECURITY AND PRIVACY. - 2021. - №5. - P. 2475-6725.
2. Lara-Nino C. A., Diaz-Perez A., Morales-Sandoval M. Elliptic Curve Lightweight Cryptography: A Survey // IEEE Access. - 2018. - №6. - P. 72514-72550.
3. Castryck W., Decru T. An Efficient Key Recovery Attack on SIDH // Cryptology ePrint Archive, Paper 2022/975. – 2022
4. Lin K., Lin J., Cai S., Wang W., Zhao C.-A. Public-key Compression in M-SIDH // Cryptology ePrint Archive, Paper 2023/136. – 2023
5. Colò L., Kohel D. Orienting supersingular isogeny graphs // Journal of Mathematical Cryptology. - 2020. - №14. - P. 414-437.
6. Dartois P., De Feo L. On the Security of OSIDH // Public-Key Cryptography - PKC 2022.

- Springer International Publishing, 2022. - P. 52-81.
7. Chi-Domínguez J.-J., Esser A., Kunzweiler S., May A. Low Memory Attacks on Small Key CSIDH // Cryptology ePrint Archive, Paper 2023/507. - 2023