Секция «Математика и механика»

Эффективность различных реализаций модифицированного протокола Диффи-Хеллмана выработки общего ключа

Горбунов Евгений Сергеевич
Студент
Томский государственный университет, Механико-математический факультет, Томск, Россия
E-mail: ghostman23@mail.ru

Как известно, при создании более мощного квантового компьютера такие распространённые криптосистемы как RSA и Эль-Гамаля станут бесполезными[1]. Поэтому современная криптография нуждается в новых, устойчивых к атакам на квантовом компьютере криптосистемах. Как раз такой криптосистемой является BMMC[3]. По крайней мере, сейчас неизвестны квантовые алгоритмы которые могли бы дать преимущество над обычными алгоритмами для взлома BMMC.

Так же рассмотрим протокол Диффи-Хеллмана – это протокол обмена ключей, который позволяет двум сторонам достигнуть соглашения о секретном ключе по открытому каналу связи без предварительной личной встречи[2]. Однако протокол Диффи-Хеллмана не эффективен на практике, т.к. уязвим к атаке «человек посередине». Но можно применить криптосистему BMMC для построения некоммутативного протокола Диффи-Хеллмана, для устранения угрозы со стороны атаки «человек посередине»[4]. Модификация заключается в том, что идёт выработка общего ключа посредством некоторой криптосистемы с открытым ключом (в данном случае BMMC), затем проверка аутентичности общего ключа посредством некоторой симметричной криптосистемы(например AES) и хэш-функции.

По проведённым исследованиям(в том числе параллельным), шифрование BMMC занимает намного меньше времени, чем шифрование RSA или El-Gamal. Так же по ряду исследований, было получено, что 4 параллельных шифрования BMMC являются самым выигрышным вариантом, по сравнению с распараллеливанием степеней в шифровании или параллельным умножением матриц.

Получается, что использование BMMC в модификации Диффи-Хеллмана имеет ряд преимуществ. Во-первых, решается проблема уязвимости протокола к атаке «человек посередине». Во-вторых, шифрование RSA и Эль-Гамаля уступают в скорости шифрованию BMMC. В-третьих, устойчивость модифицированного варианта к атакам на квантоваом компьютере.

Литература

1. Садовничий В. А. Квантовый компьютер и квантовые вычисления. Том 2, Ижевск 1999, с. 200-248

2. Смарт Н., Крипторафия. Москва, Техносфера 2005, 257 - 261

3. Rososhek, S.K. New Practical Algebraic Public Key Cryptosystem and Some Related Algebraic and Computa-tional Aspects. Applied Math. 2013, 4, 1043–1049.

4. Rososhek, S.K., Gorbunov E. 2013. Noncommutative analogue of Diffie-Hellman protocol in matrix ring over the residue ring. International journal of computers & technology. 2013, vol. 11, no 10.

Слова благодарности

Выражаю благодарность своему научному руководителю Росошеку Семёну Константиновичу.