УДК 003.26:004.056.55:621.39

СОВРЕМЕННЫЕ КВАНТОВЫЕ МЕТОДЫ РАЗДЕЛЕНИЯ СЕКРЕТА

И. В. Лимарь, д. т. н. Е. В. Василиу

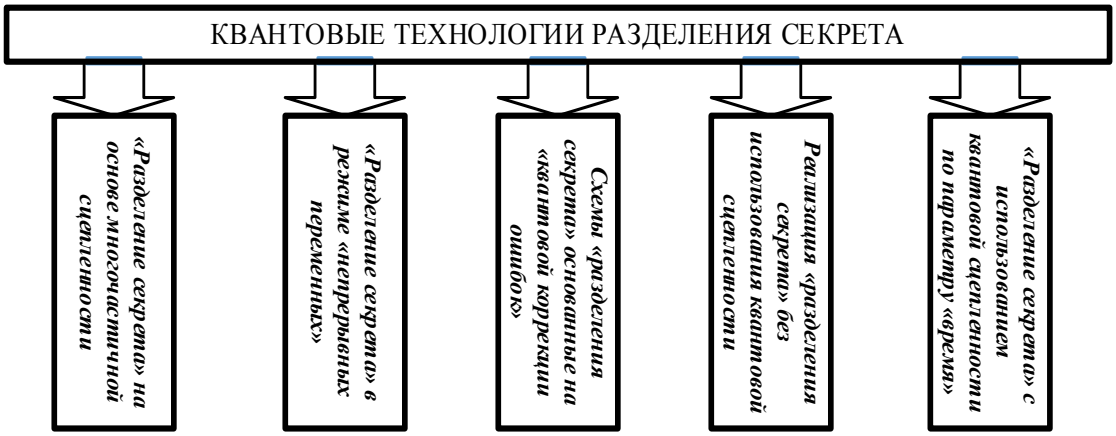
Одесская национальная академия связи им. А. С. Попова
Украина, г. Одесса
iv.limar@onu.edu.ua

Приводится выполненная с учетом наукометрических показателей классификация наиболее известных схем разделения секрета на основе квантовых технологий. При этом в качестве критериев, по которым выполнена классификация, выбраны как физические принципы, на которых основаны соответствующие методы разделения секрета, так и виды задач защиты информации, которые решаются этими методами.

Ключевые слова: квантовая криптография, разделение секрета, классификация.

Для решения задачи взаимного контроля субъектами управления той или иной системы, в криптографии используется принцип, который носит название «разделение секрета». С другой стороны, в связи с развитием в последние десятилетия такого направления в рамках криптологической науки, как квантовая криптография, были предложены схемы разделения секрета на основе квантовых технологий. При проведении исследований, целью которых является повышение стойкости квантовых схем разделения секрета, существенную помощь может оказать использование сформированной классификации таких схем и протоколов. В той или иной степени, определенную классификацию предлагали другие авторы и ранее [1]. Однако, как правило, классификация выполнялась на основе других оригинальных исследований, и это сказывалось на полноте выполняемого обзора. Кроме того, на наш взгляд, до сих пор при систематизации схем квантового разделения секрета методологически не использовался подход, учитывающий показатели цитируемости соответствующих публикаций. Очевидно, что такая ситуация не является приемлемой в условиях лавинообразного роста количества публикуемых материалов. Проведенная нами работа призвана восполнить этот пробел.

Если осуществлять классификацию по такому признаку, как принцип физической реализации (см. рисунок), то изначально следует выделить исторически первыми появившиеся схемы на основе многочастичной сцепленности [2]. Данные схемы, в свою очередь, делятся на собственно схемы и протоколы семейства HBB99 – производные от базовой схемы, описанной в [2], а также схемы с использованием так называемого «product measurement», схемы с использованием «свопинга», схемы и протоколы на основе гейтов «управляемое «НЕ» и «преобразование Адамара», схемы на основе алгоритма Гровера, схемы с «перегруппировкой порядка» и схемы с использованием перепутанных состояний *W*-типа. Следует отметить, что схемы класса HBB также представлены различными протоколами: это, например, протокол, основанный на использовании лишь двух связанных квантовой сцепленностью фотонов, протоколы без использования так называемой «максимальной запутанности», «5-ти кубитные» протоколы, а также расширение базового протокола HBB99 на произвольное количество связанных квантовой сцепленностью частиц. К другому важнейшему классу схем квантового разделения секрета относятся решения на основе так называемых «непрерывных переменных», т. е. квантовых систем с бесконечной размерностью гильбертова пространства [3]. Следующим весьма известным методом разделения секрета в рамках квантовой криптографии является класс схем, основанный на квантовой коррекции ошибок [4]. Еще один «канонический» способ квантового разделения секрета представлен в рамках схемы, реализующей такую задачу без использования квантовой сцепленности [5]. И, наконец, последним из выделенных нами основных видов физической реализации схем квантового разделения секрета является решение на основе квантовой сцепленности по параметру время.



Основные физические реализации квантовой технологии разделения секрета

При выборе же в качестве классификационного критерия типа решаемой задачи, согласно данным наукометрических баз мы выделили три наиболее распространенных вида схем, использующих принцип квантового разделения секрета: совместный контроль телепортации квантового состояния, взаимный контроль при совместном осуществлении зашифрования-расшифрования и разделение секрета при реализации квантовой прямой безопасной связи. В свою очередь, эти три основных типа задач по защите информации решаются с использованием уже перечисленных нами физических принципов построения криптосистем. В частности, используются схемы на основе многочастичной сцепленности – главным образом для реализации телепортации, и схемы на основе единичных фотонов для взаимоконтроля при процедуре зашифрования-расшифрования.

Таким образом, в работе выделены наиболее известные в настоящее время схемы разделения секрета, основанные на квантовых технологиях. Такая классификация может оказать методологическую помощи при проведении научных исследований в данной предметной области, и, в частности, может являться справочным материалом для отечественных специалистов по криптографии. Многообразие же предложенных различными авторами квантовых схем разделения секрета определяется стремлением усовершенствовать изначально предложенные решения с целью сделать их более практичными для конкретных инженерных реализаций, повысить эффективность создаваемых криптосистем, информационную емкость протоколов и т. д.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Li Q. Semiquantum secret sharing using entangled states / Q. Li, W.H. Chan, D.Y. Long // Physical Review A.— 2010.— Vol. 82, issue 2.— 022303.

2. Hillery M. Quantum Secret Sharing / M. Hillery, V. Buzek, A. Berthiaume // Physical Review A.— 1999.— Vol. 59, issue 3.— P. 1829—1834.

3. Lance A.M. Tripartite Quantum State Sharing / A.M. Lance, T. Symul, W.P. Bowen, B.C. Sanders, P.K. Lam // Physical Review Letters.— 2004.— Vol. 92, issue 17.— 177903.

4. Cleve R. How to Share a Quantum Secret / R. Cleve, D. Gottesman, H. Lo // Physical Review Letters.— 1999.— Vol. 83, issue 3.— P. 648—651.

5. Zhang Z. Multiparty quantum secret sharing / Z. Zhang, Y. Li, Z. Man // Physical Review A.— 2005.— Vol. 71, issue 4.— 044301.

I. V. Limar, E. V. Vasiliu

State-of-the-art quantum methods for secret sharing.

The paper presents a classification of the most prominent secret sharing schemes based on quantum technology and performed by taking scientometric indicators into account. The classification criteria include both the physical principles, on which the relevant secret sharing methods are based, and the types of information security problems, which can be solved using such methods.

Keywords: *quantum cryptography, secret sharing, classification.*