

АНАЛИЗ ТЕОРЕТИЧЕСКОЙ РЕАЛИЗАЦИИ КВАНТОВОГО ПРОТОКОЛА E91 (EPR) ПРИ ПОМОЩИ ПАТЕНТНОГО ПОИСКА

Вингурская Д.В., Гареева В.С., Курышева А.А.

Научный руководитель: профессор, Ткалич В.Л.

Университет ИТМО, Санкт-Петербург

Одним из перспективных направлений в квантовой криптографии является использование так называемых перепутанных состояний для создания секретного ключа. Соответствующий протокол - E91, предложенный Экертом в 1991 году.

Цель работы: анализ текущего состояния реализации квантового протокола E91 (EPR), а также исследование направлений развития объектов изобретений, использующих данный протокол.

Другое название протокола E91 – EPR, так как он основан на парадоксе Эйнштейна-Подольски-Розенберга. Протокол реализуется следующим образом: атом излучает два фотона в противоположных направлениях в сторону двух наблюдателей – Алисы и Боба. Фотоны излучаются с неопределенной поляризацией, но в силу симметрии их поляризации всегда противоположны. Однако особенность эффекта EPR состоит в том, что поляризацию фотонов можно узнать только после измерения. Данный эффект гарантирует безопасность пересылки и хранения ключа шифрования.

В ходе патентного поиска, был составлен перечень патентов, которые зарегистрированы в США, Китае, Англии и России. Проведенный анализ позволил выделить группы проблем реализации протокола, на решение которых направлены данные объекты изобретения, а также перспективы развития объектов исследования. Наше исследование было ориентировано на американские и отечественные патенты, а именно:

- 1) Bovino F. Method and system for estimating the noise of a two-photon entangled state // United States Patent № 9490909;
- 2) Trojek P., Weinfurter H. Generation of Quantum-Correlated and/or Polarization Entangled Photon Pairs with Unequal Wavelengths // United States Patent № 8222623;
- 3) Мордовин А.А., Дмитриев С.В. Способ передачи информации на основе нелокальной квантовой корреляции между частицами в перепутанном квантово-механическом состоянии// Патент России № 2235434;
- 4) Бородакий Ю.В., Антонов Ю.П., Добродеев А.Ю. [и др.]. Способ генерации секретных ключей с помощью перепутанных по времени фотонных пар// Патент России № 2360367;
- 5) Фроловцев Д.Н., Магницкий С.А. Способ и устройство источника поляризационно-перепутанных фотонов с максимально возможной степенью перепутанности// Патент России № 2636808;
- 6) Бородакий Ю.В., Антонов Ю.П., Добродеев А.Ю. [и др.]. Поляризационная квантовая криптосистема// Патент России № 2360367;
- 7) Кулиш О. А., Хисамов Ф. Г., Чернуха Ю В. [и др.]. Способ передачи ключа шифрования/расшифрования по волоконно-оптической линии неограниченной длины // Патент России № 22661287.

Была произведена систематизация патентов по нескольким признакам объектов изобретения, направленных на: повышение эффективности передачи данных и устранение недостатков известного уровня техники.

В результате проведенного патентного поиска был проведена оценка технической реализации квантового протокола E91 (EPR) и выделены направления развития объектов изобретений, реализующих данный протокол.

Авторы: Гареева В.С., Курышева А.А., Вингурская Д.В.

Научный руководитель: Ткалич В.Л.

Руководитель подразделения: Заколдаев Д.А.