МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АНГАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОЙ ГЕОФИЗИКИ СО РАН

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ИССЛЕДОВАНИИ СЛОЖНЫХ СТРУКТУР

МАТЕРИАЛЫ ЧЕТЫРНАДЦАТОЙ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ 19–24 сентября 2022 г.

Томск
Издательский Дом Томского государственного университета
2022

РЕАЛИЗАЦИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ НА БАЗЕ МЕТОДОВ КВАНТОВОЙ КРИПТОГРАФИИ*

С.Н. Торгаев[1], Д.Е. Каширский[1], М.Л. Громов[1], Л.Г. Евтушенко[2]

[1]Томский государственный университет, Томск, Россия
[2]Высшая школа экономики, Москва, Россия
torgaev@mail.tsu.ru

IMPLEMENTATION OF A TELECOMMUNICATION SYSTEM BASED ON QUANTUM CRYPTOGRAPHY METHODS

S.N. Torgaev[1], D.E. Kashirskii[1], M.L. Gromov[1], L.G. Yevtushenko[2]

[1]Tomsk State University, Tomsk, Russia
[2]Higher School of Economics, Moscow, Russia

Существующие на сегодняшний день системы квантовой коммуникации, как правило, имеют модульный принцип построения, т.е. существуют отдельные реализации систем квантового распределения ключей, шифрования и приемо-передачи данных. В данной работе представлены результаты разработки телекоммуникационной системы, построенной с использованием принципов квантового шифрования, в рамках единого устройства. Для реализации подобного устройства предлагается использовать систему на кристалле ПЛИС [1]. Преимуществом такой технологии является возможность реализации как аппаратных решений, так и программной обработки в рамках одного кристалла.

Для осуществления квантового распределения ключей предполагается использовать двухпроходную оптоволоконную схему “Plug & Play”, реализующую протокол BB84 [2]. Управление работой активных оптоволоконных компонентов схемы (лазер, фазовый модулятор, детектор одиночных фотонов) осуществляется с помощью ПЛИС, а управление установкой и обработка криптографических ключей производятся с помощью программного обеспечения для операционной системы семейства Linux, что становится возможным благодаря наличию процессора, размещенного на кристалле ПЛИС. Благодаря этому можно сделать систему более компактной и дешевой за счет, например, отсутствия в необходимости использования персональных компьютеров, дополнительного оборудования и платного программного обеспечения как в [3].

Распределенные криптографические ключи будут использоваться для аппаратного шифрования передаваемых по сети данных на том же ПЛИС. Алгоритм шифрования данных будет построен согласно ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

Литература

1. *Тарасов И.* Применение ПЛИС класса «система на кристалле» Xilinx Zynq и подходы к проектированию на основе языков описания аппаратуры высокого уровня // Электроника НТБ. – 2019. – № 4. – С. 62–66. – DOI: 10.22184/1992-4178.2019.185.4.62.66.
2. *Баумейстер Д., Экерт А., Цайлингер А.* Физика квантовой информации. – М.: Постмаркет, 2002. – 376 с.
3. *Rodimin V.E., Kiktenko E.O., Usova V.V. [et al.]*. Modular quantum key distribution setup for research and development applications // Journal of Russian Laser Research. – 2019. – Vol. 40, № 3. – P. 221–229.

* Работа выполнена в рамках программы развития Томского государственного университета (Приоритет 2030), проект № 2.4.6.22 ИГ.