**Широкополосная рефлектометрия для анализа уязвимостей систем квантового распределения ключей в ближнем и среднем инфракрасном диапазоне**

***Бондарь К. Д.***

*Студент, 1 курс магистратуры*

*Московский государственный университет имени М. В. Ломоносова,*

*физический факультет, Москва, Россия*

*E–mail:* *bondar.kd19@physics.msu.ru*

**Введение**

Теоретически, системы квантового распределения ключей (КРК) обеспечивают безусловную секретность распределения ключей между легитимными пользователями, основанную на фундаментальных законах квантовой физики, таких как теорема о запрете клонирования, невозможности достоверно различать неортогональные квантовые состояния и т. д. Тем не менее, техническая реализация систем КРК далека от идеализированной модели, что приводит к появлению побочных каналов утечки информации.

Одним из таких побочных каналов, используемых при атаке троянского коня [1], является отражение от оптических компонентов, находящихся в оптических частях систем КРК. Наиболее распространенное решение этой проблемы – пассивные оптические компоненты, используемые в качестве защиты от таких атак – демонстрируют нестабильную эффективность в широком спектральном диапазоне [2]. Полноценное экспериментальное исследование этого побочного канала до сих пор остается незавершенным из-за определенных технических проблем, таких как отсутствие спектральных волоконных устройств, пригодных для измерений в широком спектральном диапазоне. В данной работе представлена установка, реализующая оптическую рефлектометрию во временной области (OTDR), и соответствующие результаты измерений над реальной системой КРК, которые позволяют сделать вывод об устойчивости таких систем к упомянутым атакам в ближнем и среднем инфракрасном диапазоне $λ$ = 1100–1800 нм.

**Экспериментальная установка**

Разработанный рефлектометр OTDR с однофотонным детектором в режиме счета фотонов ($ν$-OTDR) показан на Рис. 1. Алгоритм его работы следующий: световые импульсы от пикосекундного суперконтинуумного лазерного источника, выставленного на максимальную мощность, проходят через регулируемый аттенюатор и перестраиваемый акустооптический спектральный фильтр для установки требуемой мощности и длины волны. После прохождения циркулятора в направлении $1 \rightarrow 2$ излучение отражается от оптических компонентов, расположенных в тестируемом устройстве (DUT), и регистрируется однофотонным лавинным фотодиодом (SPAD) на основе на InGaAs после прохождения циркулятора в направлении $2 \rightarrow 3$. Дискретизация во временной области осуществляется соответствующей электроникой. Аналогичным образом можно измерить входную мощность лазерного излучения и коэффициенты пропускания оптического циркулятора $T\_{1\rightarrow 2}$ и $T\_{2\rightarrow 3}$. Величины фотоотсчётов, полученные SPAD, работающим в непрерывном режиме, могут быть преобразованы в величины отражений от оптических компонентов внутри тестируемого устройства по формуле $\left(1\right)$:

$$\begin{array}{c}R=10 log\_{10}\left(\frac{N\_{in}}{N\_{out}}\right)-T\_{1\rightarrow 2}-T\_{2\rightarrow 3};\#\left(1\right)\end{array}$$

где $N\_{in}$ и $N\_{out}$ - количество фотоотсчётов SPAD, соответственно вызванных отражением от DUT и входным лазерным излучением, $T\_{1\rightarrow 2}$ и $T\_{2\rightarrow 3}$ – коэффициенты пропускания в направлениях $1 \rightarrow 2$ и $2 \rightarrow 3$.



*Рис. 1:* Широкополосный OTDR-рефлектометр. $SCL$ – пикосекундный суперконтинуумный лазерный источник, $ATT$ – управляемый аттенюатор, $OF$ – перестраиваемый спектральный фильтр, $C$ – оптический циркулятор, SPAD – лавинный фотодиод на основе InGaAs, $DUT$ – тестируемое устройство, $P\_{in}$ – входная мощность излучения, $P\_{out}$ – мощность излучения, отраженного от DUT. Толстыми линиями обозначаются оптические волокна, тонкими – электрические провода.

Можно показать [3], что вероятность успешной атаки троянского коня зависит от среднего числа фотонов $μ\_{Eve}$, отраженных к злоумышленнику (Еве). В свою очередь, среднее число фотонов зависит от максимальной мощности нелегитимного излучения $P\_{Eve}^{max}$, которая соответствует порогу повреждения волокна или нижнему пределу мощности сторожевого детектора; от коэффициента пропускания пассивных компонентов защиты $T\_{def}$; от максимальных значений отражательной способности $R\_{max}$, полученных в эксперименте, через формулы $(2-3)$:

$$\begin{array}{c}μ\_{Eve}=\frac{P\_{ref}^{max}\left[W\right]λ}{hcf};\#\left(2\right)\end{array}$$

$$\begin{array}{c}P\_{ref}^{max}=P\_{Eve}^{max}\left[dBm\right]+R\_{max}\left[dB\right]+T\_{def}\left[dB\right];\#\left(3\right)\end{array}$$

где $λ$ – длина волны импульсов Евы, $h$ – постоянная Планка, $c$ – скорость света, $f$ – частота повторения лазерных импульсов.

Таким образом, разработанная в рамках данной работы установка может быть использована для оценки эффективности широкополосной атаки троянского коня на произвольную оптоволоконную систему КРК.

**Литература**

1. Jain, N. et al., *Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. IEEE J. Sel. Top. Quantum Electron. 21, 6600710 (2015).*

2. Sushchev, I. S. et al., *Practical security analysis against the Trojan-horse attacks on fiber-based phase-coding QKD system in the wide spectral range. Proc. SPIE 11868, 118680H (2021).*

3. Lucamarini, M. et al., *Practical security bounds against the trojan-horse attack in quantum key distribution. Phys. Rev. Lett. 5, 031030 (2015).*