

## Влияние поляризации излучения на эффективность атаки оптической накачкой на источник систем квантового распределения ключа

А.К. Сотников<sup>1,2</sup>, М. А. Фадеев<sup>1,3</sup>, В.В. Макаров<sup>1,4,5</sup> и А.А. Поносова<sup>1,4</sup>

<sup>1</sup>Российский Квантовый Центр, Москва, Россия

<sup>2</sup>Московский Физико-Технический Институт (НИУ), Долгопрудный, Россия

<sup>3</sup>Университет ИТМО, Санкт-Петербург, Россия

<sup>4</sup>Центр НТИ Квантовые Коммуникации, Москва, Россия

<sup>5</sup>Университет Виго, Виго, Испания

[anatolijstnikov129@gmail.com](mailto:anatolijstnikov129@gmail.com)

Квантовое распределение ключей (КРК) позволяет безопасно сгенерировать секретный ключ у удаленных пользователей, Алисы и Боба. Его безопасность основана на квантовой физике [1], а не на вычислительной сложности [2], что обуславливает его перспективность с наступлением эры квантовых вычислений.

Безопасность протоколов КРК подтверждается строгими доказательствами. Однако реальные системы могут быть уязвимы к атакам на побочные каналы. Существуют протоколы с независимым измерительным устройством (measurement-device-independent), которые позволяют полностью устранить уязвимость приемника. Эти протоколы считаются практически защищенными от квантового взлома, когда они связаны с хорошо защищенными отправителями, которые готовят квантовые состояния. В недавней работе [3] продемонстрирована новая атака на Алису - атака оптической накачкой. Показано, что возможно увеличить энергию импульсов источника КРК на основе лазерного диода путем оптического накачивания его излучением на более короткой длине волны. В частности, под воздействием лазерного излучения на 1310 нм наблюдалось увеличение средней мощности и энергии импульсов. Это может позволить злоумышленнику украсть секретный ключ.

Целью настоящей работы является изучение влияния поляризации Евы на эффективность атаки оптической накачкой.

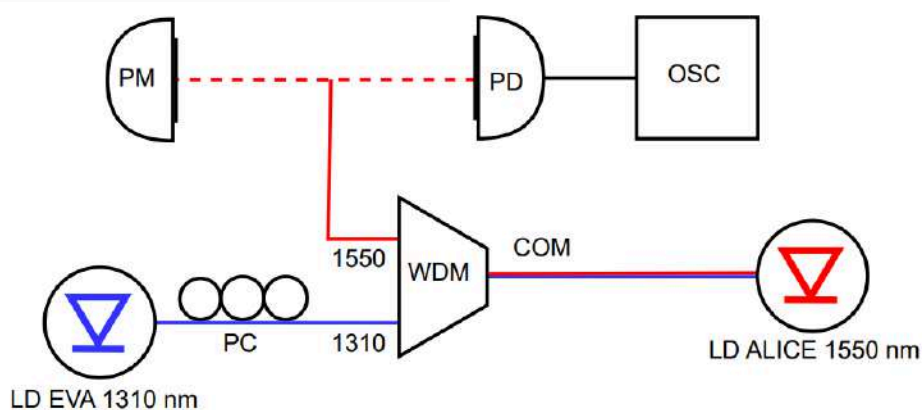


Рис. 1. Экспериментальная установка. LD, лазерный диод; PC, контроллер поляризации; WDM, спектрально-селективный ответвитель; PM, измеритель мощности; PD, фотодиод; OSC, осциллограф.

В рамках настоящей работы реализована установка, показанная на рис. 1. Атака производилась лазером на 1310 нм (LD EVE, Nolatech FPL-FBG-1310-14BF) на лазер на 1550 нм (LD ALICE, Nolatech FPL-FBG-1550-14BF) через 1310/1550 спектрально-селективный ответвитель (WDM, Gateray GW-FW1310SA). Лазерный диод Алисы работал в режиме переключения усиления. Мощность лазера Евы составляла

6.43 мВт. Для изменения состояния поляризации использовался механический контроллер поляризации (PC, Thorlabs FPC561). Он позволяет произвольно менять состояние поляризации, однако не измеряет его. В процессе изменения состояния поляризации контроллер изменял выходную мощность Евы на 0.65%. На выходе установки контролировалась средняя мощность и энергия импульсов. Амплитудно - временные характеристики импульсного излучения исследованы с помощью фотодетектора (PD, Laserscom PDI35-10G, полоса пропускания 10 ГГц) с осциллографом (OSC, LeCroy 816Zi, полоса пропускания 16 ГГц). Измерения проводились с разными поляризациями, а также без воздействия Евы.

Под воздействием Евы с постоянной мощностью накачки, но разной поляризацией выходная мощность Алисы увеличилась на 56.7 - 68.2% , а энергия импульса на 45.7-51.3% в сравнении с исходными характеристиками. Таким образом разница увеличения средней мощности в зависимости от поляризации составила 11.5%, а энергии импульса - 5.6 %. Согласно работе [3] вариация мощности накачки на 0.65%, имеющаяся в экспериментальной установке, вызовет изменение средней выходной мощности и энергии импульса излучения лазера Алисы на порядка 0.3-0.6%. Таким образом, продемонстрированное в настоящей работе изменение характеристик выходного излучения Алисы при воздействии излучением Евы постоянной мощности обусловлено различной эффективностью накачки в зависимости от поляризации излучения оптической накачки.

Наличие данного эффекта может представлять дополнительную угрозу безопасности для систем КРК с поляризационным кодированием. Поскольку при прохождении через фазовые модуляторы Алисы, излучение Евы будет поляризовано согласно выбранному базису и приготовленному состоянию. В результате различия эффективности от поляризации, по измерениям энергии выходного сигнала Ева будет также получать дополнительную информацию о базисе и состоянии, в котором приготовила Алиса. Малая зависимость от поляризации косвенно подтверждает, что механизм действия этого света - накачка. При засеве лазера наблюдалась бы сильная зависимость от поляризации, поскольку лазер излучает лишь в одной поляризационной моде. Данный эффект является предметом для будущих исследований.

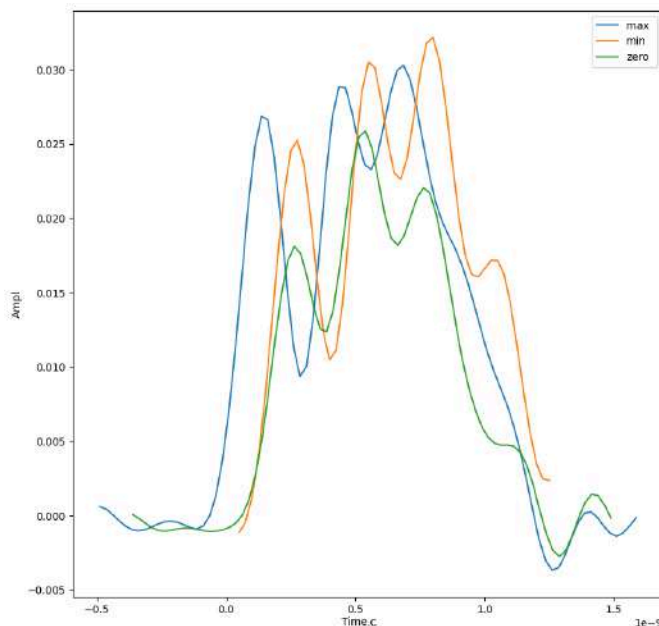


Рис. 2. Форма импульсов на выходе Алисы без атаки (зеленая линия) и при атаке излучением с разной поляризацией.

ЛИТЕРАТУРА

1. K.Weï et al. // Rev. Mod. Phys. **92**, 025002 (2020).
2. H.Tan et al. // Phys. Rev. Applied **15**, 064038 (2021).
3. M.Fadeev et al. // arXiv:2503.11239 [quant-ph]