конференция РусКрипто

СФБ ЛАБ

Исследование атаки ослепления однофотонных лавинных детекторов модулированным ярким светом

Булавкин Даниил Сергеевич, специалист, ООО «СФБ Лаб»

Зызыкин А.П., ведущий специалист, ООО «СФБ Лаб»

Сущев И.С, специалист, ООО «СФБ Лаб»

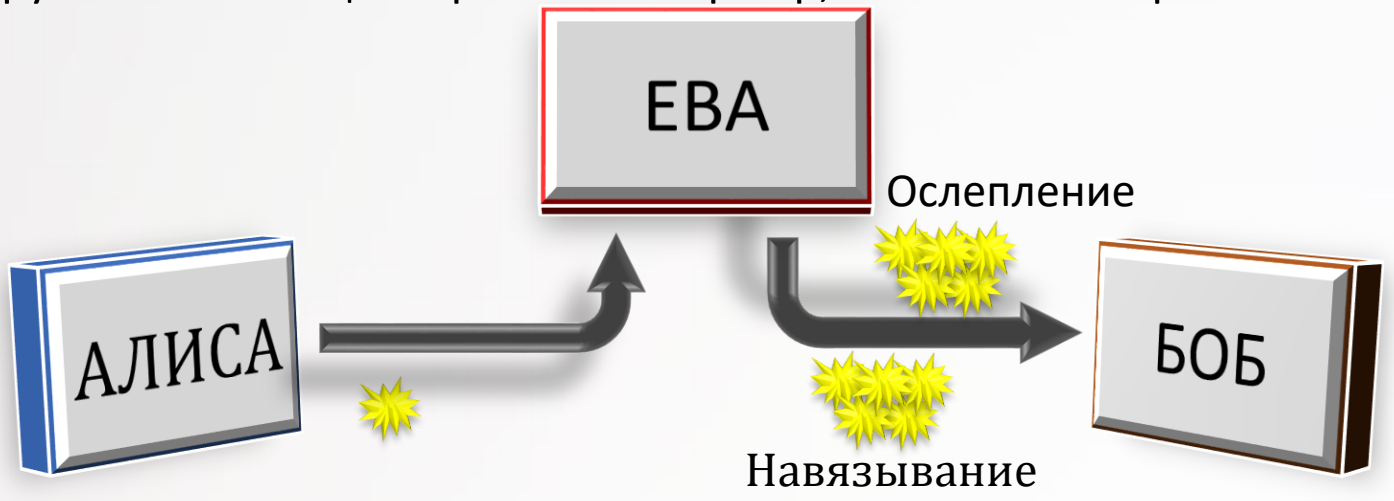
Бугай К.Е., специалист, ООО «СФБ Лаб»

Богданов С.А., специалист, ООО «СФБ Лаб»

Дворецкий Д.А., к.т.н., ведущий специалист, ООО «СФБ Лаб»

ВВЕДЕНИЕ

- Обычно на стороне Боба в системах распределения квантовых ключей используются однофотонные лавинные диоды InGaAs (SPAD) с высокоскоростным подсчетом фотонов.
- Эти детекторы можно переключать с режима счета фотонов (режима Гейгера) на линейный режим ярким светом.
- Этот эффект называется ослеплением SPAD.
- Детектор может быть ослеплен непрерывным (CW) оптическим освещением, но в таком случае эту атаку можно обнаружить с помощью простых контрмер, таких как контроль тока смещения SPAD.



Принцип атаки ослепления

ПРИНЦИП РАБОТЫ ОДНОФОТОННОГО ЛАВИННОГО ДЕТЕКТОРА

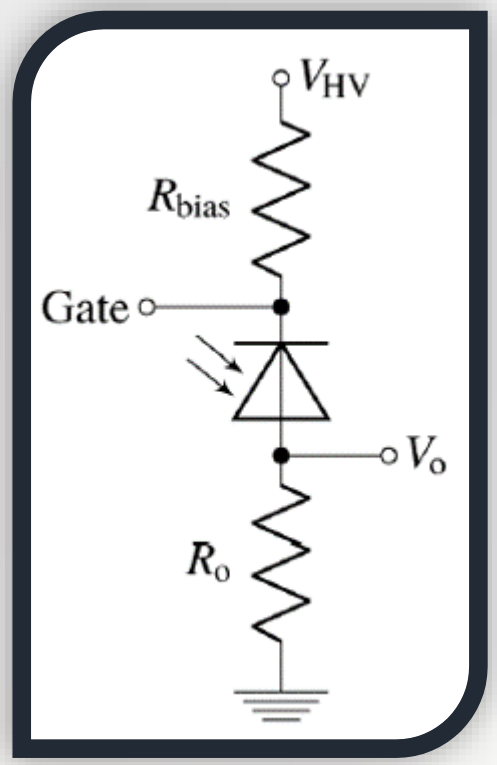
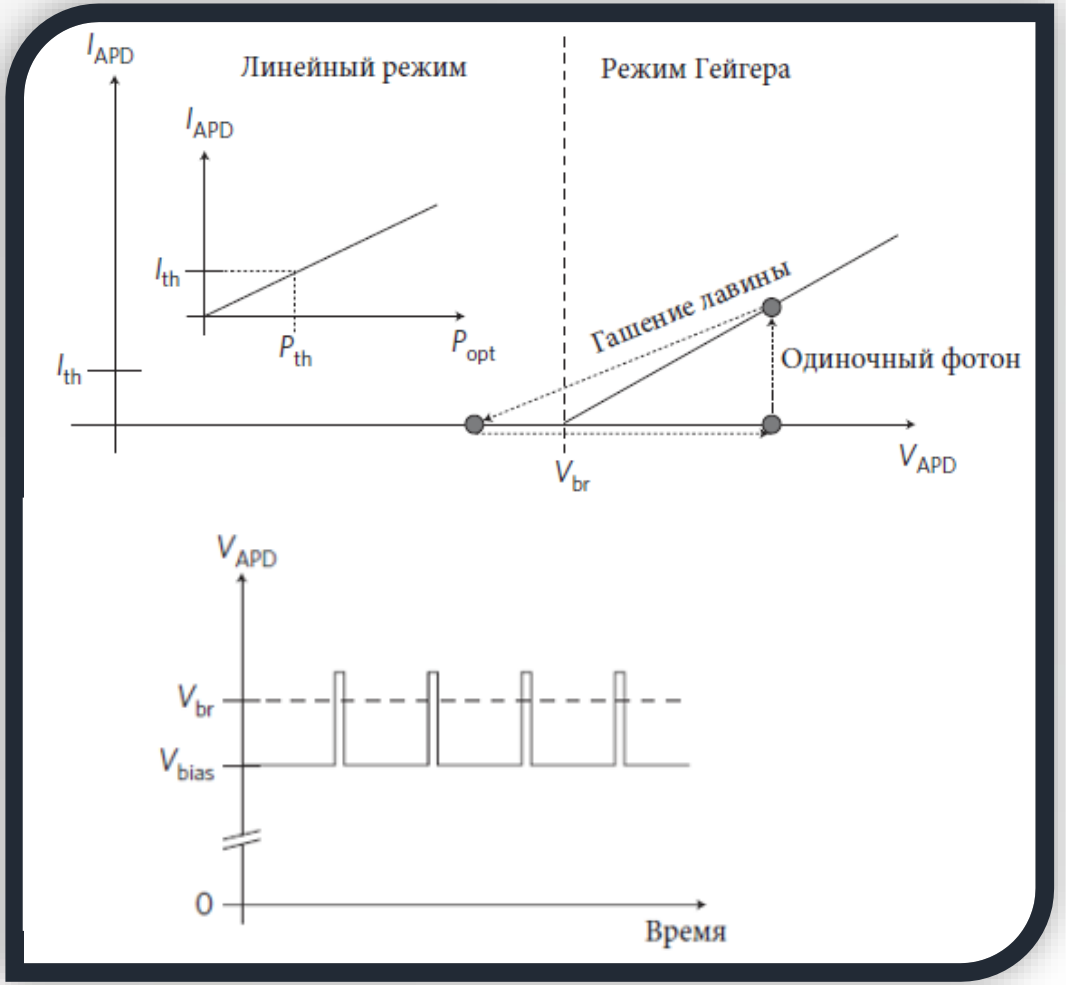


Схема включения ЛФД

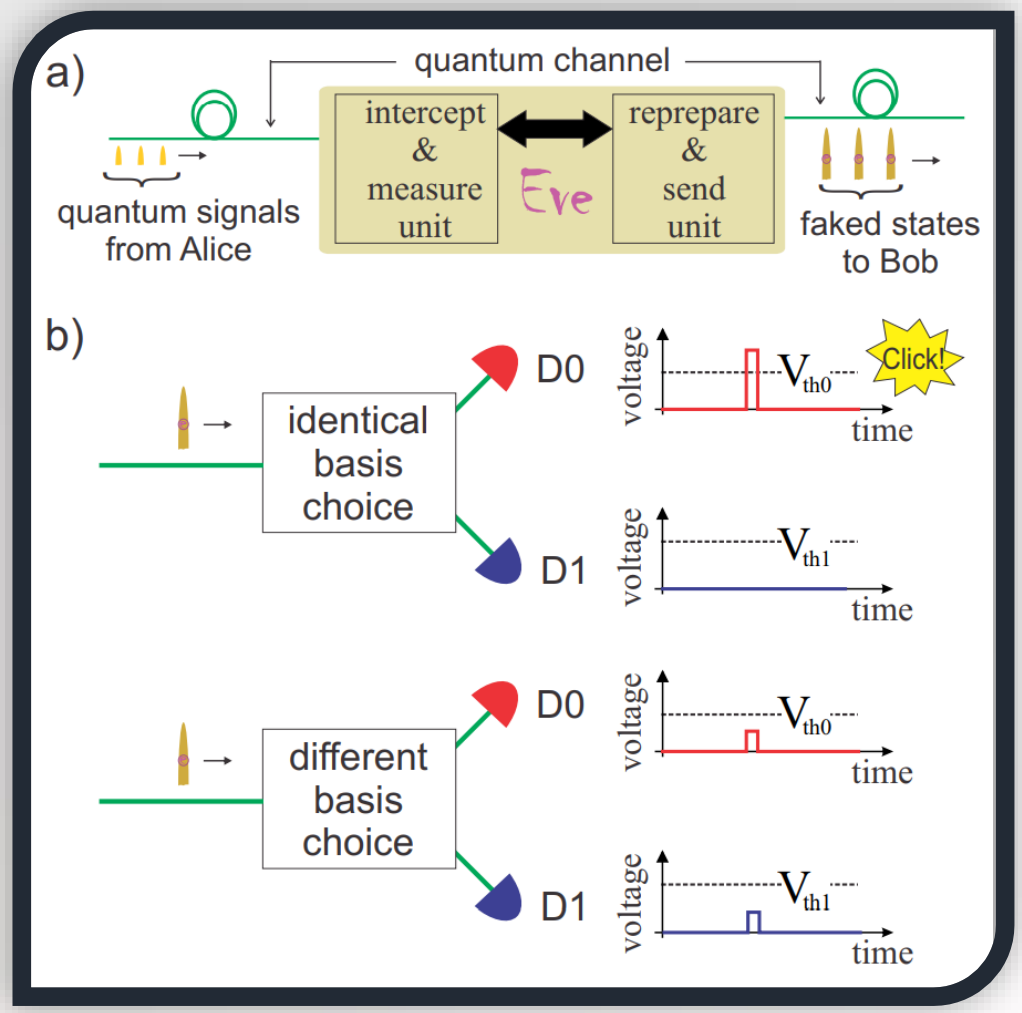
- R_{bias} – резистор для пассивного гашения лавины
- R_o – небольшой резистор для считывания. Напряжение на R_o равно V_o, которое является выходным сигналом
- V_{HV} – это источник постоянного тока в цепи однофотонного детектора
- V_{bias} – напряжение смещения на ЛФД



Режимы работы ЛФД

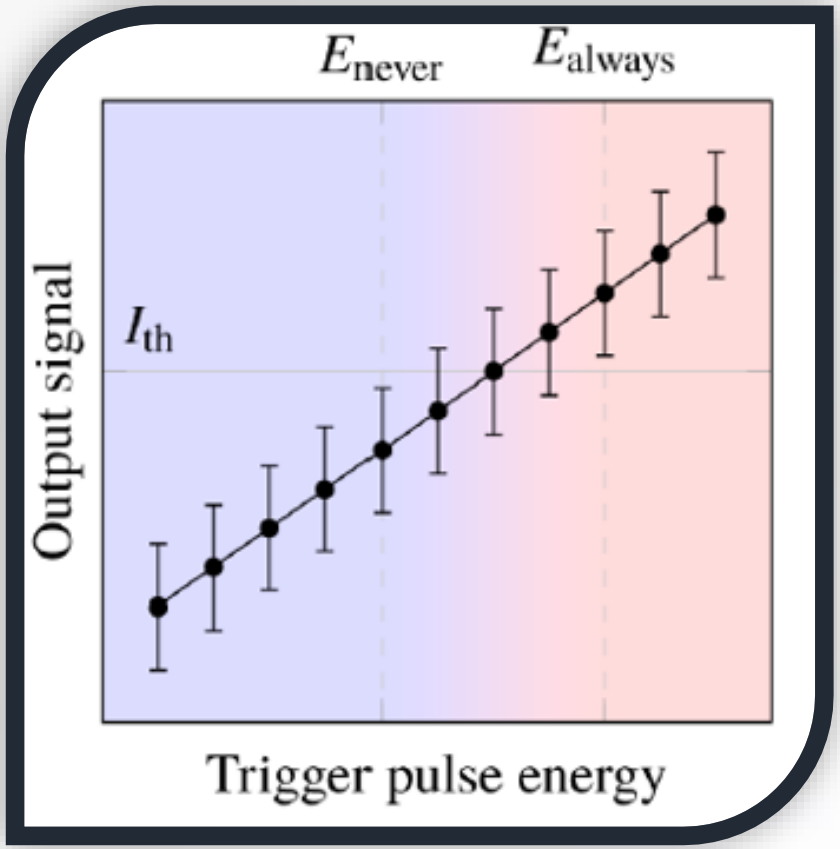
- V_{bias} – напряжение смещения на ЛФД
- V_{br} – напряжение пробоя ЛФД

ПРИНЦИП АТАКИ ОСЛЕПЛЕНИЯ



Механизм атаки ослепления

a) Прием-перепосыл ложных состояний при атаке ослепление
b) Принцип навязывания



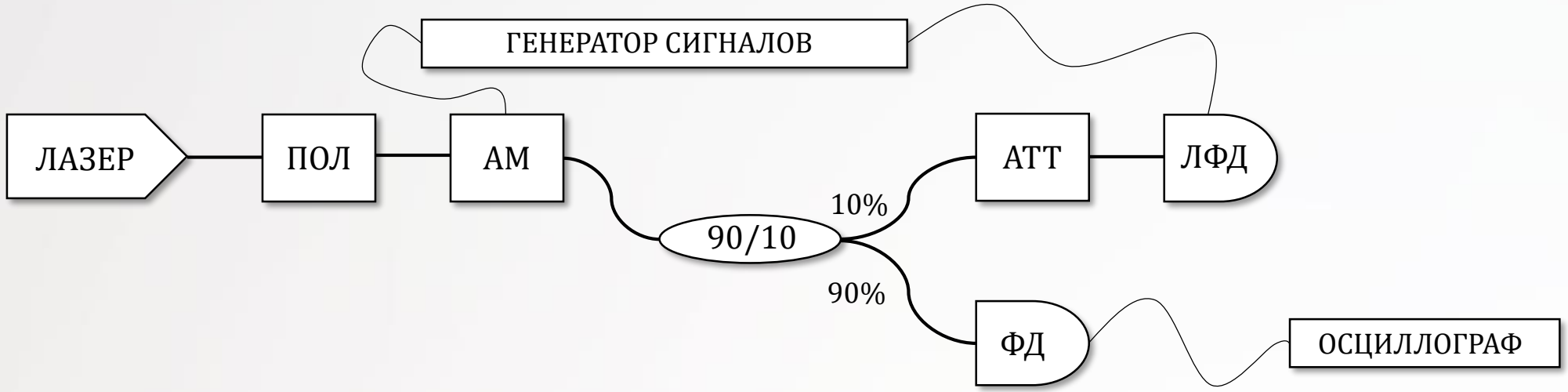
Энергии навязывания

- E_{always} – минимальная энергия, при которой детектор кликнет с вероятностью 100%
- E_{never} – максимальная энергия, при которой детектор НЕ кликнет с вероятностью 100%

$$E_{always} < 2 \times E_{never}$$

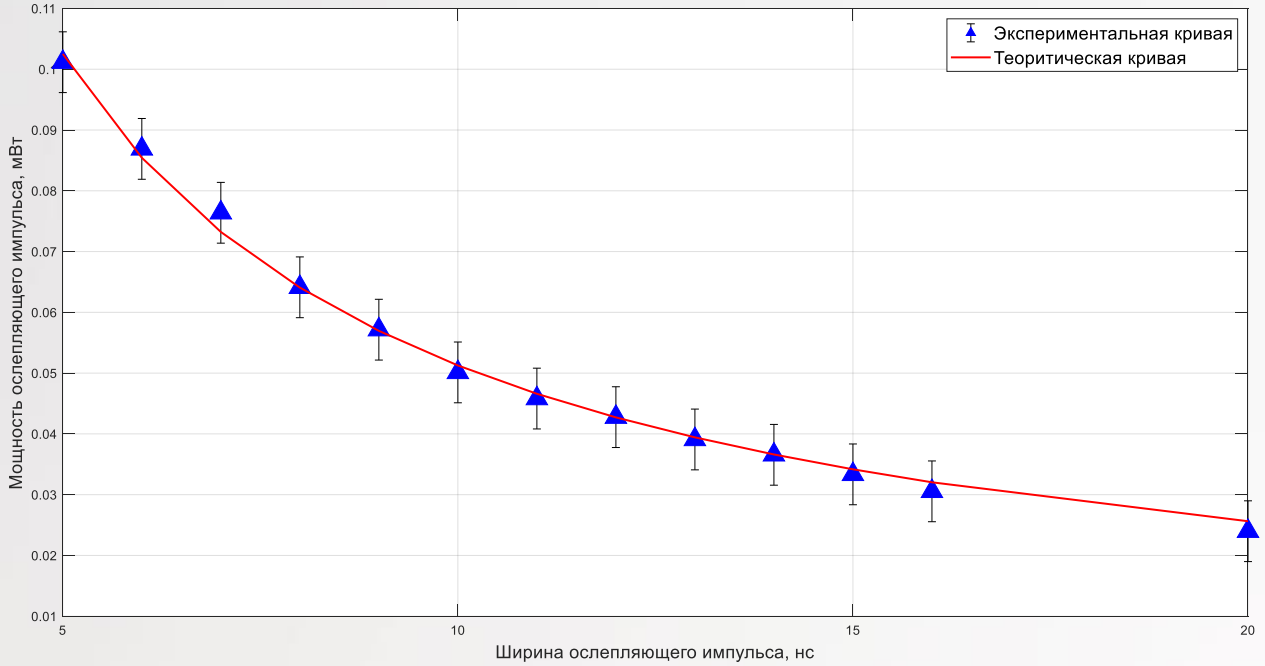
Ослепление модулированным ярким светом

- В отличие от классического импульсного ослепления мы используем модулированное непрерывное лазерное излучение.
- Одной из особенностей этого варианта ослепляющей атаки является наличие контраста в излучении с глубиной модуляции 50дБ. Этот вариант имеет интересное преимущество: между двумя импульсами имеется промежуток со слабым лазерным излучением, что не вызывает значительного увеличения тока смещения детектора, но приводит к ситуации, когда детектор легче переключить на линейный режим



Экспериментальная установка для ослепляющей атаки модулированным ярким светом (ПОЛ – волоконно-оптический поляризатор, АМ – амплитудный модулятор, 90/10 – волоконно-оптический ответвитель с соотношением 90/10, АТТ – перестраиваемый оптический аттенюатор, ФД – сверхбыстрый фотодиод, ЛФД – тестируемый однофотонный лавинный фотодиод)

Ослепление модулированным ярким светом

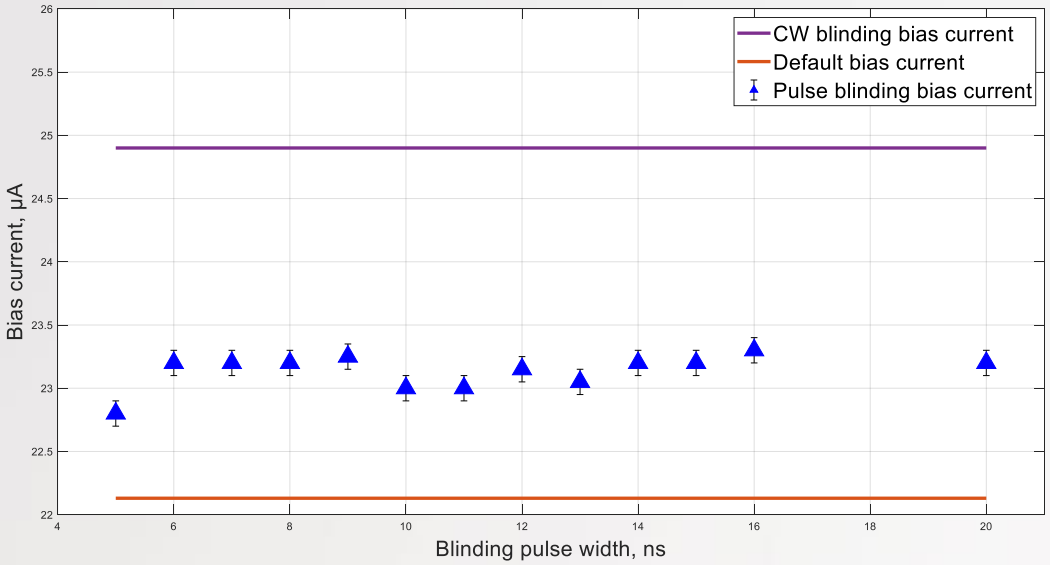


Результат аппроксимации зависимости мощности ослепляющих импульсов от их ширины функцией гиперболы

- Был экспериментально подтвержден факт, что мощность ослепления обратно пропорциональна ширине оптического импульса;
- На рисунке представлена аппроксимация полученной зависимости мощности ослепления от ширины импульса функцией гиперболы, константой которой является энергия ослепления

Эффект ослепления зависит именно от энергии импульса

Ослепление прямоугольными импульсами различной ширины

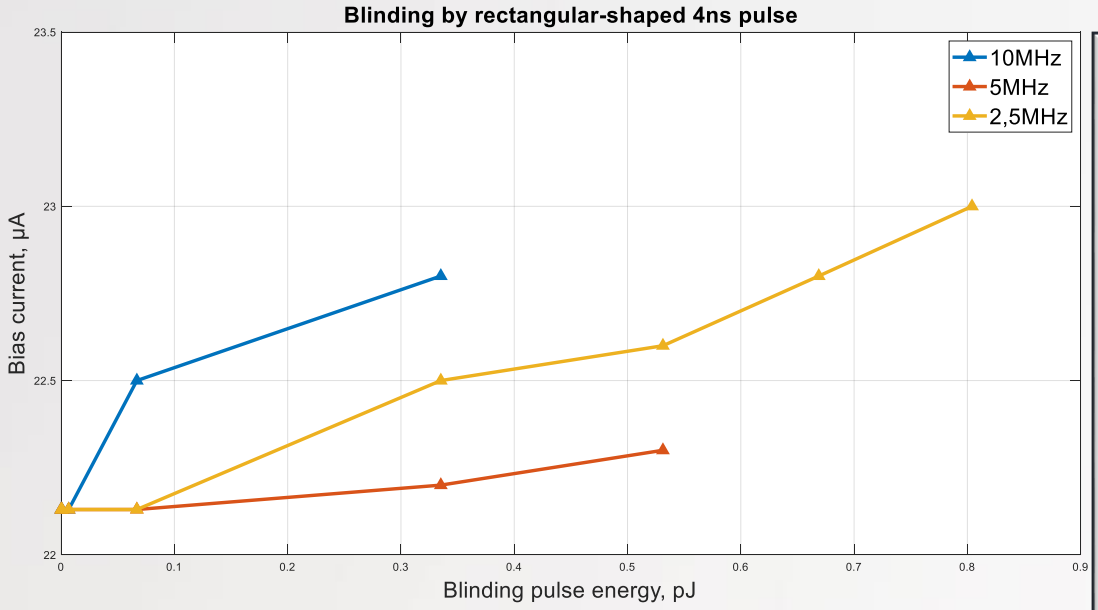


Зависимости тока смещения детектора при ослеплении от длительности ослепляющего импульса.

- Ширина ослепляющего импульса изменялась в диапазоне 4 – 20 нс.
- Энергия в каждом импульсе разной ширины одинакова.
- Ток смещения детектора при непрерывном ослеплении значительно выше, чем ток при импульсном ослеплении, что свидетельствует о большей эффективности импульсного ослепления.
- Наименьшее изменение тока смещения происходило при ослеплении импульсом прямоугольной формы длительностью 4 нс

Импульсное ослепление детектируется хуже, чем непрерывное

Ослепление прямоугольным импульсом длительностью 4 нс с разной частотой следования



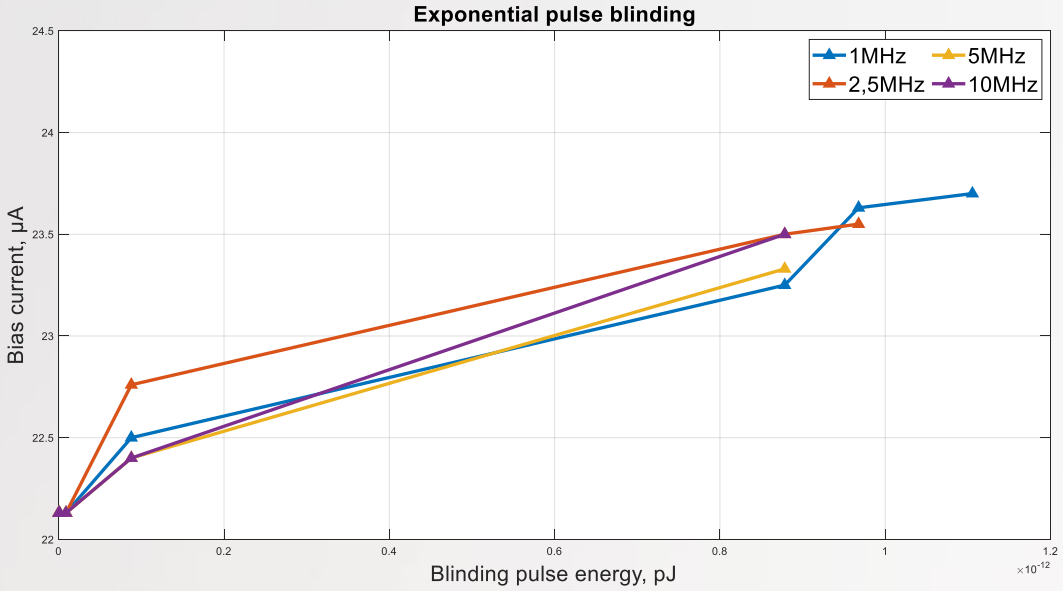
Зависимости тока смещения при ослеплении прямоугольным импульсом длительностью 4 нс при различных частотах следования

(Самые правые точки каждой кривой соответствуют ослеплению детектора)

- Как видно из графиков, частоты повторения 10 МГц и 2,5 МГц по-прежнему дают значительное увеличение тока, которое можно легко обнаружить.
- При частоте импульса 5 МГц рост тока смещения незначителен, несмотря на более высокую энергию ослепляющего импульса. Таким образом, значение тока смещения при ослеплении составило 22,27 мкА, в то время как в нормальном режиме работы тестируемого ЛФД значение тока смещения – 22,13 мкА.
- Это приращение настолько незначительно, что может быть воспринято как шум.

Ослепление при частоте следования импульсов вдвое меньшей частоты стробирования детектора почти не детектируется

Ослепление импульсом с экспоненциальным спадом на различных частотах следования



Зависимости тока при ослеплении экспоненциальным импульсом при различных частотах следования

(Самые правые точки каждой кривой соответствуют ослеплению детектора)

- Для импульсов с экспоненциальным спадом значение энергии, при которой происходит ослепление, изменяется от 0,8 пДж до 1,1 пДж, что выше, чем для импульсов прямоугольной формы.
- Ток детектора также выше по сравнению с ослеплением импульсами прямоугольной формы: 22,8 мкА для прямоугольной волны длительностью 4 нс на частоте 10 МГц против 23,5 мкА для экспоненциальной на той же частоте

Ослепление импульсами с экспоненциальным спадом детектируются намного лучше, чем ослепление импульсами прямоугольной формы

Заключение

- Мы продемонстрировали еще один тип ослепляющей атаки на однофотонные лавинные диоды на основе структуры InGaAs, которые используются в системах квантового распределения ключей;
- Ослепление модулированным ярким светом с импульсами прямоугольной формы вызывает незначительное увеличение тока смещения детектора.
- Минимальный ток смещения среди длительностей импульсов в диапазоне 4-20 нс был при длительности 4 нс и имел значение 22,8 мкА (в нормальных условиях ток смещения составлял 22,13 мкА) при частоте следования 10 МГц;
- Варьируя частоту следования ослепляющих импульсов, мы получили следующий результат: на частоте следования ослепляющих импульсов 5 МГц при их длительности 4 нс (частота стробирования SPAD по-прежнему составляла 10 МГц) было зафиксировано наименьшее изменение тока смещения, при этом разница между токами в нормальном состоянии и в состоянии ослепления составила 0,14 мкА;
- Импульсы экспоненциальной формы из-за длинного спада не дают схеме гашения лавины достаточно быстрого уменьшить ток смещения, что приводит к его значительно высокому уровню. По сравнению с импульсами прямоугольной формы приращение тока смещения составило 1,2 мкА при частоте следования 5 МГц против 0,14 мкА. Таким образом, наилучшей стратегией является проведение ослепления импульсами прямоугольной формы длительностью 4 нс с частотой повторения 5 МГц.

СФБ ЛАБ

СПАСИБО ЗА ВНИМАНИЕ!