Атаки на протокол квантовой криптографии COW

Квантовая криптография

- Криптография — наука о методах обеспечения конфиденциальности.
- Квантовая криптография, или квантовое распределение ключей, использует принципы квантовой механики, чтобы сделать безопасной передачу секретной информации.

Класическая, квантовая, постквантовая

	Достаточная изученность	Стойкость к QC	Время стойкости ключа
Класическая:	$+$	$-$	n лет
Квантовая:	$-$	$+$	∞
Постквантовая:	$-$	$+$	$m > n$ лет

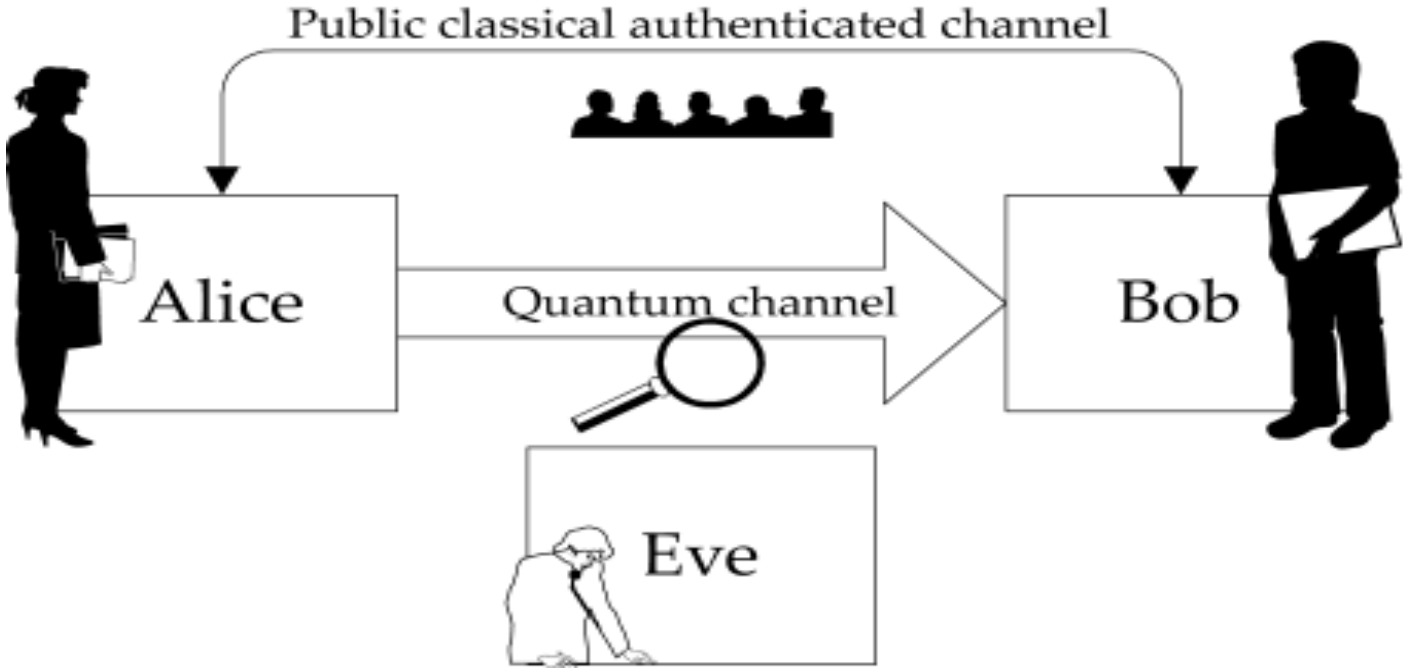
Одноразовый блокнот (шифр Вернама)

Квантовое распределение ключей

- КРК – протокол, который гарантированно надежен, и посредством которого биты закрытого ключа могут быть созданы в процессе коммуникации двух сторон по **открытому** каналу.
- Секретность получающегося в результате ключа гарантируется свойствами квантовой информации и обусловлена фундаментальными законами физики.

Квантовое распределение ключей

- **Теорема.** Невозможно точно копировать неизвестное квантовое состояние, используя унитарное преобразование.
- **Утв.** При любой попытке различить два неортогональных квантовых состояния извлечение информации сопровождается возмущением сигнала.



Протокол COW

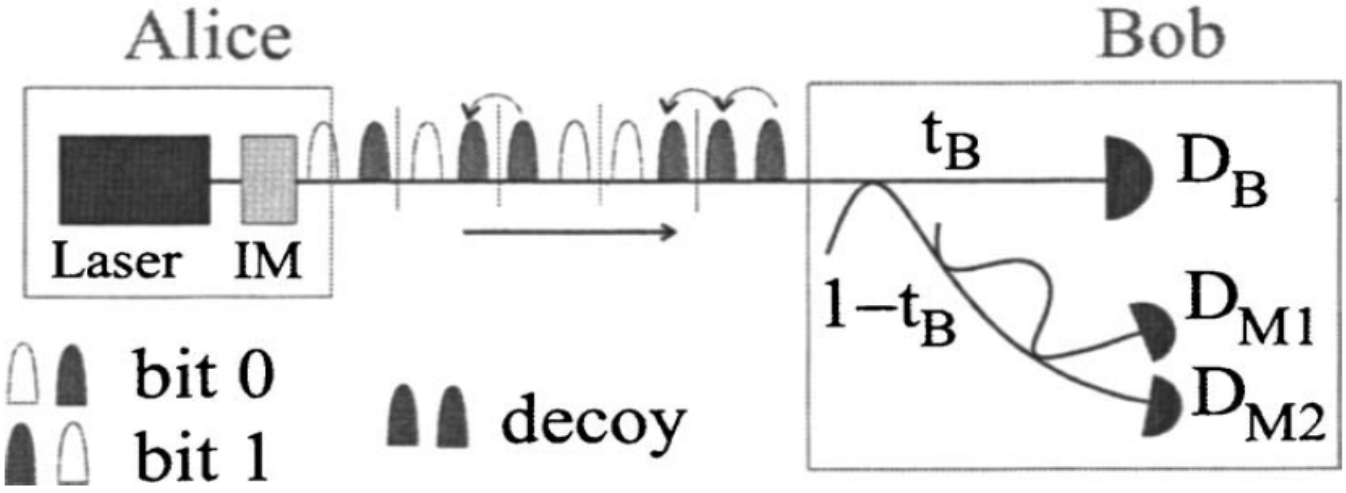
COW (Coherent One Way) – когерентный односторнний

- Clavis3, ID Quantique
- Европейская сеть КРК SECOQC

Когерентные состояния

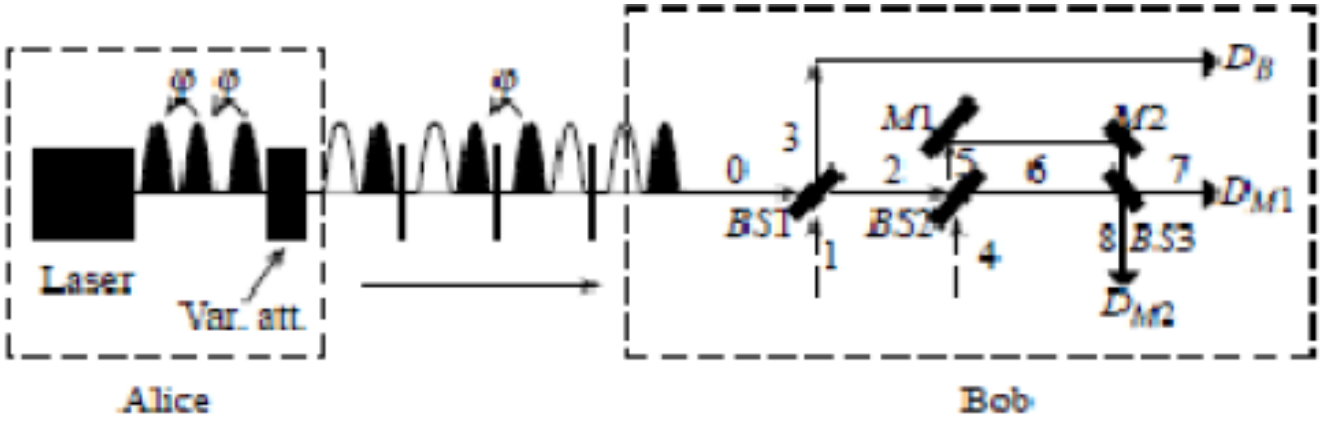
- $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$
- $\langle\beta|\alpha\rangle = e^{-(|\alpha|^2+|\beta|^2-2\beta^*\alpha)/2}$
- $\mu = |\alpha|^2$ – интенсивность
- На практике $\mu = 0,1;\ 0,2;\ 0.5$
- Могут быть получены, например, ослабленным излучением лазера

Протокол COW



- "0" $|\psi_0\rangle = |\alpha\rangle|0\rangle$
- "1" $|\psi_1\rangle = |0\rangle|\alpha\rangle$
- decoy state $|\psi_d\rangle = |\alpha\rangle|\alpha\rangle$
- Видность $V = \frac{p(D_{M1})-p(D_{M2})}{p(D_{M1})+p(D_{M2})}$

Протокол COW



$k=6$	$k=5$	$k=4$	$k=3$	$k=2$	$k=1$	
	1	0	0	0	1	$\leftarrow c$
$\|\mu\rangle_{12}\|\mu\rangle_{11}$	$\|0\rangle_{10}\|\mu\rangle_{9}$	$\|\mu\rangle_{8}\|0\rangle_{7}$	$\|\mu\rangle_{6}\|0\rangle_{5}$	$\|\mu\rangle_{4}\|0\rangle_{3}$	$\|0\rangle_{2}\|\mu\rangle_{1}$	$\leftarrow b$
decoy	1	0	0	0	1	$\leftarrow a$

Протокол COW

- Алиса отправляет ”0” с вероятностью $(1-f)/2$, ”1” с вероятностью $(1-f)/2$ и контрольные состояния (decoy) с вероятностью f.
- Боб объявляет для каких битов он провел измерения во временной линии и когда загорался детектор D_{M2}.
- ”Просеивание ключа” – Алиса говорит Бобу какие биты ему нужно исключить из его сырого ключа, т.к они обусловлены детектированием контрольных состояний.
- Анализируя срабатывания в D_{M2}, Алиса оценивает нарушения когерентности через видности V_{1-0} и V_d и вычисляет информацию Евы.
- Коррекция ошибок
- Усиление секретности просеянного ключа

Атаки на системы КРК

Предполагается, что ресурсы злоумышленика неограничены.

- Атаки на протоколы распределения ключа: общая схему приготовления и измерения квантовых состояний, процедуру полученния результатов измерений квантовых состояний ключа на стороне Алисы и Боба.
- Атаки на техническую реализацию квантово-криптографических систем (”квантовый хакинг”).

Атака светоделителем на протокол COW

- Затухание $\Rightarrow \mu_B = 10^{-\delta\ell/10}\mu$
- Светоделитель + идеальный канал связи
- $\mu_E^{max} = \mu - \mu_B = (1 - 10^{-\delta\ell/10})\mu$