Covert continuous-variable quantum key distribution

Raphaël Aymeric, David Fainsin, Romain Alléaume
Télécom Paris, LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

Context :

- QKD offers information-theoretical security on a distilled key between two users.
- However QKD does not guarantee the communication between both users is undetectable
- This can be an issue as this knowledge can sometimes pose a great threat to user privacy. For critical applications, secrecy is not sufficient

Objective : In this work we investigate the performance of CV-QKD when the signal is covert. We show it is impractical. However, using a block-coherent encoding technique over multiple modes we show quantum key establishment can be performed covertly.

The covertness of the protocol can be translated into this constraint on the signal power, or the modulation variance V_A

$$V_A \leq \frac{4\epsilon\sqrt{\xi/2(1+(1-T)\xi/2)}}{\sqrt{N(1-T)}}$$

Individual signal power scales as 1/√N.

Covert communications require some noise to hide the signal, more noise equals more allowed signal.

Unfeasibility of CV-QKD with the covert power constraint :

We upper-bound the number of bits generated by the covert CV-QKD protocol over what we call the set of experimentally achievable parameters.

To do this we set :

- T = 0.99
- ϵ = 0.1
- β = 0.99 (due to imperfect reconciliation)

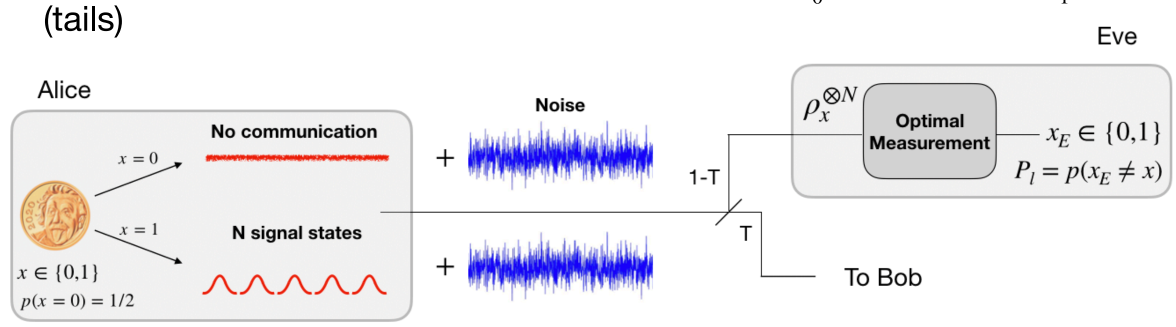
Then we optimise the number of bits obtained with the covert CV-QKD protocol over N and ξ.

Result : no more than 0.77 secret bits can be obtained covertly via covert CV-QKD, which we argue is impractical

Issue : Achieving covertness requires a V_A too small

Covert communication :

- Alice flips a coin and sends N signal states to Bob if the result is tails.
- Eve intercepts all signal which does not reach Bob and performs an optimal measurement to decide if the communication is taking place, which amounts to distinguishing between states $\rho_0^{\otimes N}$ (heads) and $\rho_1^{\otimes N}$ (tails)

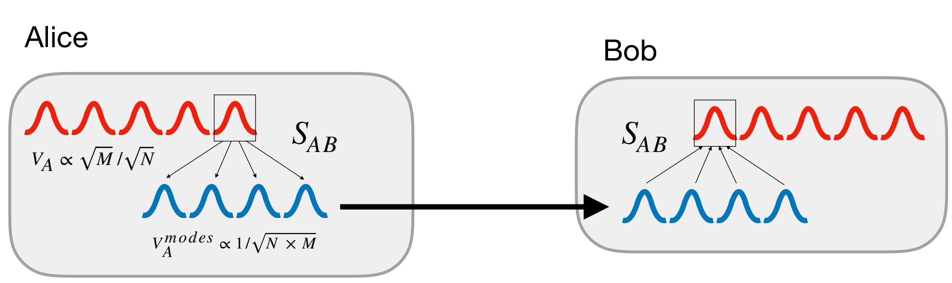


- The communication is covert if Eve's error probability can be brought arbitrarily close to a random guess, i.e. 1/2, up to a factor ϵ

Enabling covert CV-QKD with block-coherent encoding :

We propose an original idea to boost the SNR in the covert setting.

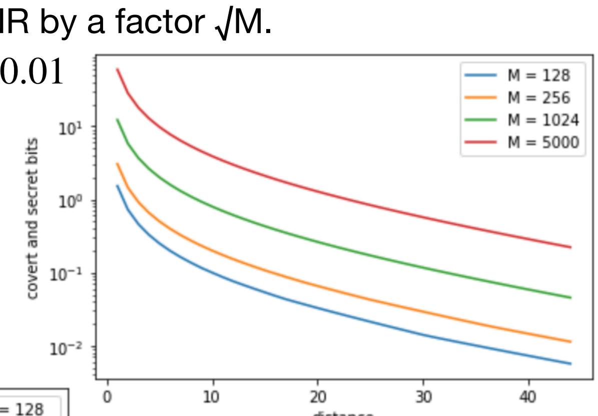
1. Alice generates N signal states sequentially
2. Each signal state is then equally split with a M-mode unitary indexed by a secret S_{AB} shared with Bob.
3. Individual modes are sent to Bob over the channel
4. With his knowledge of S_{AB} Bob recombines every set of M modes into the original signal states.
5. Bob performs his QKD measurement and goes on to the post-processing phase with Alice.



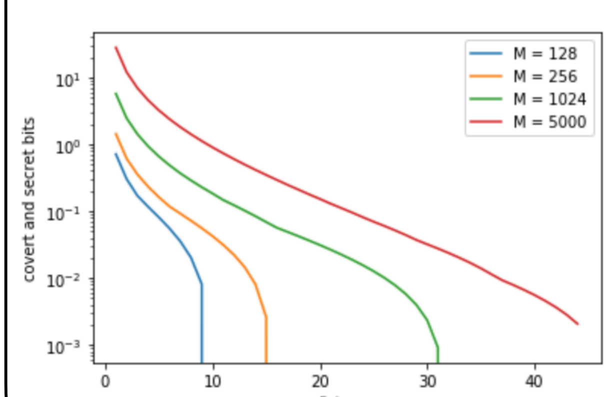
This increases the signal state SNR by a factor √M.

Impact :

$\xi = 0.01$



$\xi = 0.1$



Block-coherent encoding enables covert CV-QKD over metropolitan distances

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement CIVIQ No 820466.