Software Defined Quantum Stream-Cipher

Michel Barbeau, VE3EMB

School of Computer Science, Carleton University, CANADA

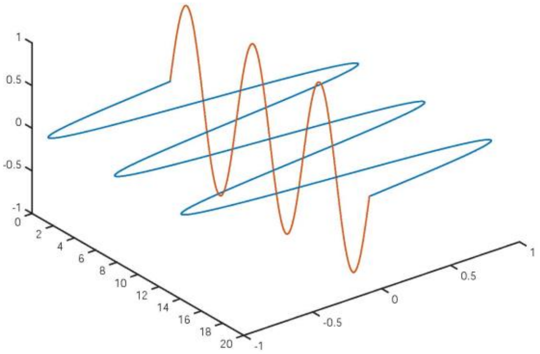
Introduction/Background

What are quantum communications?

- Use microscopic properties of light
  - Photon (quanta of light): carrier of data
- Medium is optical fibe or free space: UV or infrared
- Applications: quantum networking, distributed quantum computing and secret communications (photon detection changes its state)

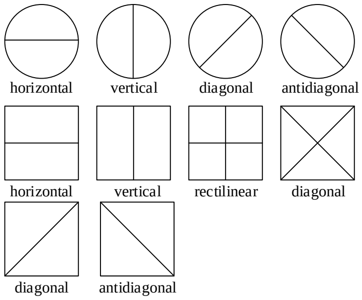
Polarization of photons

Horizontal (blue) and vertical (red)

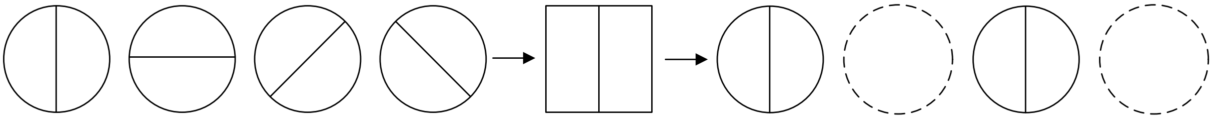


Bases, encoding and filters

Binary value	Rectilinear basis	Diagonal basis
0	horizontal (0°)	diagonal (45°)
1	vertical (90°)	antidiagonal (135°)



Photon filtering example



SD Quantum Stream-Cipher

Why software-defined quantum communications?

- Extension of the software-defined radio paradigm to quantum communications
  - implement in software, communication functions traditionally realized with complex hardware
  - more versatile, more control abilities and more advanced features
- GNU Radio Conference, 2011
  - GNU Radio for Quantum Optical Communications - Dr. Travis Humble

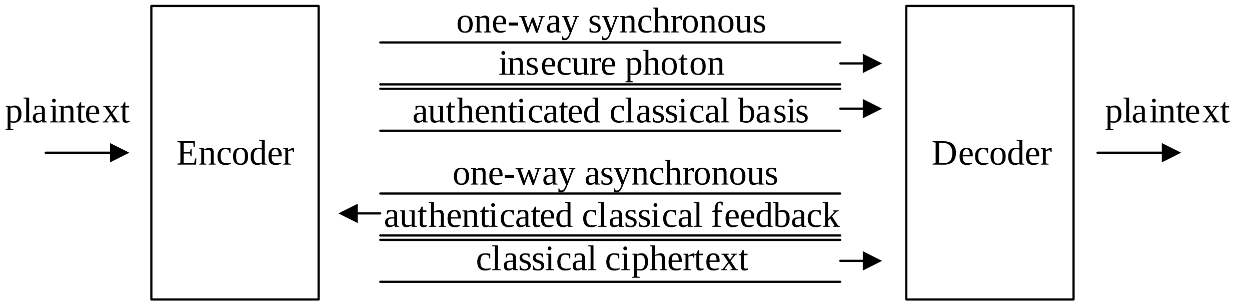
Why may this design be interesting?

- Solve a quantum communication problem with the software-defined approach
- Combine QKD with classical stream-cipher encryption
- Simulate a communication problem with GNU radio and
- Implement in GNU radio a system with feedback

Stream-cipher logic

- Secret bit-string key
  - same length as the message to be encrypted and communicated
  - single use
  - source and destination use the same
- Ciphertext
  - exclusive or of plaintext message and secret bit-string key
- Plaintext recovery
  - a second exclusive on the ciphertext and secret bit-string key

Architecture of the software-defined quantum stream-cipher



plaintext

Encoder

one-way synchronous

insecure photon

authenticated classical basis

one-way asynchronous

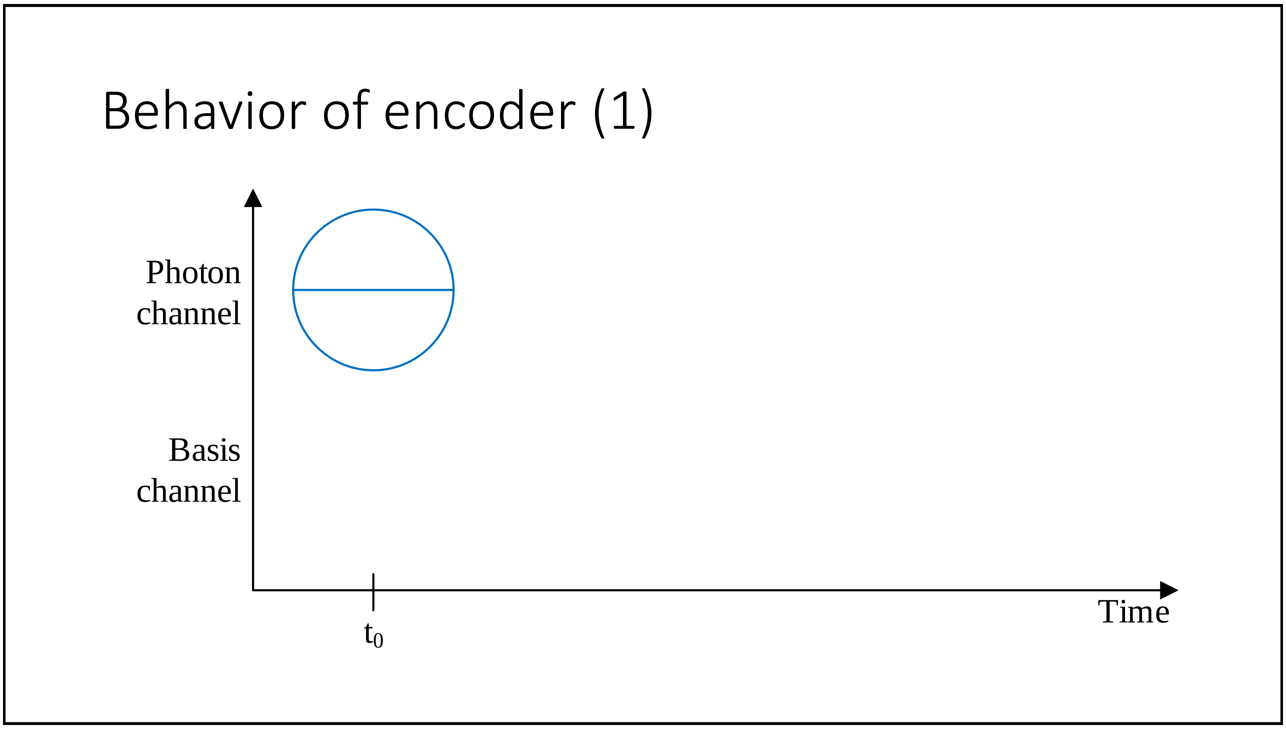
authenticated classical feedback

classical ciphertext

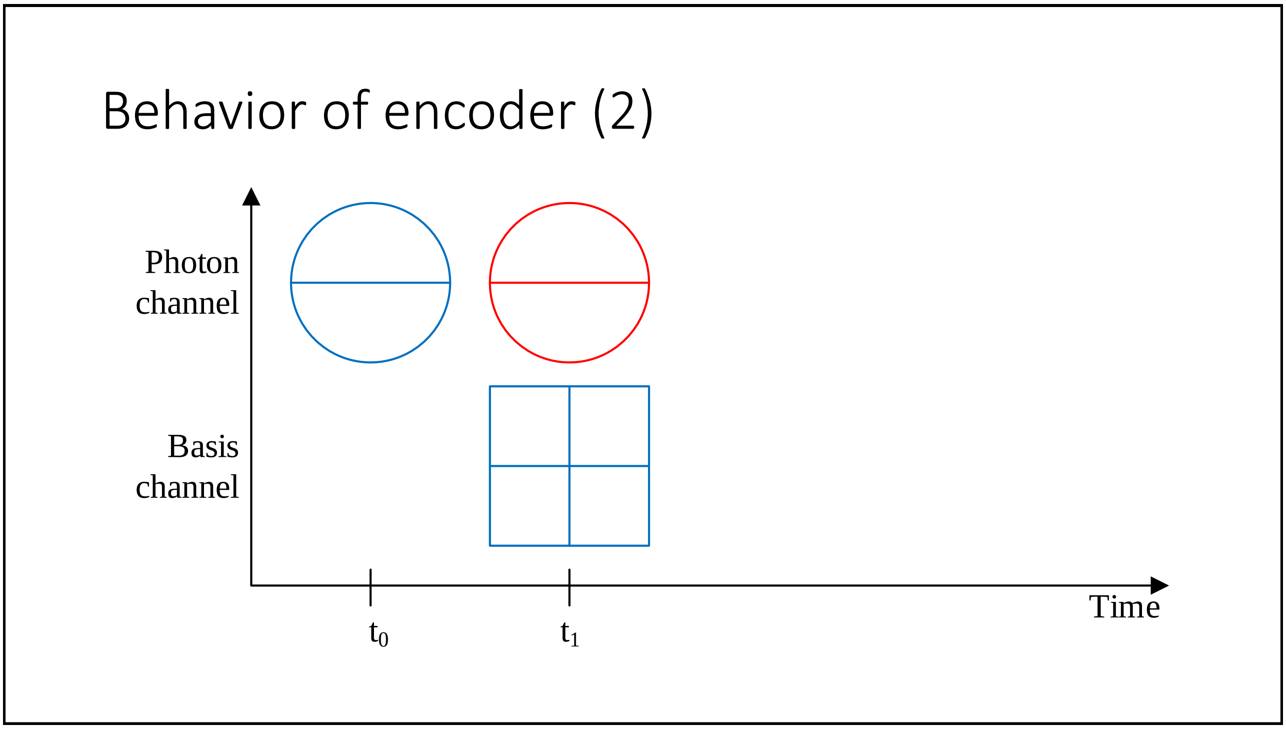
Decoder

plaintext

Quantum communications and cryptography used to distribute secret bit-string key, in accordance with the principles of the BB84 QKD protocol.

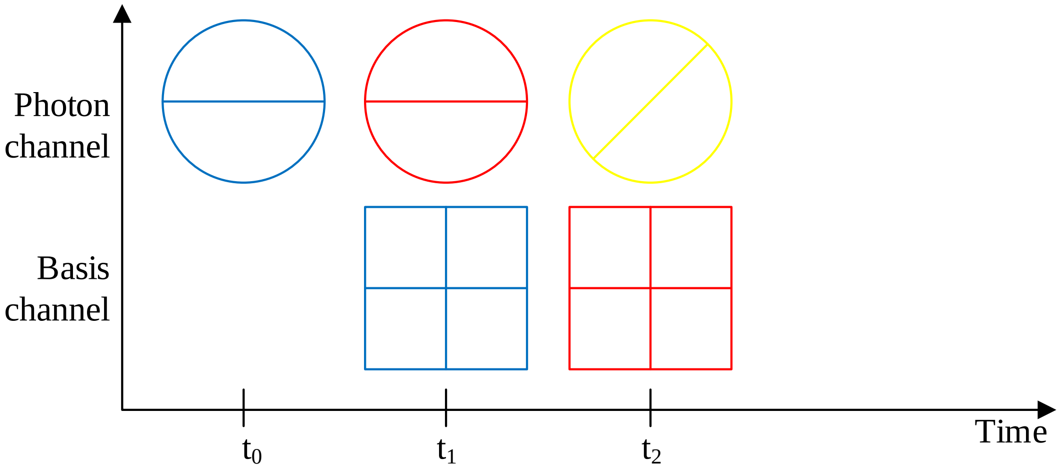


Behavior of encoder (1)

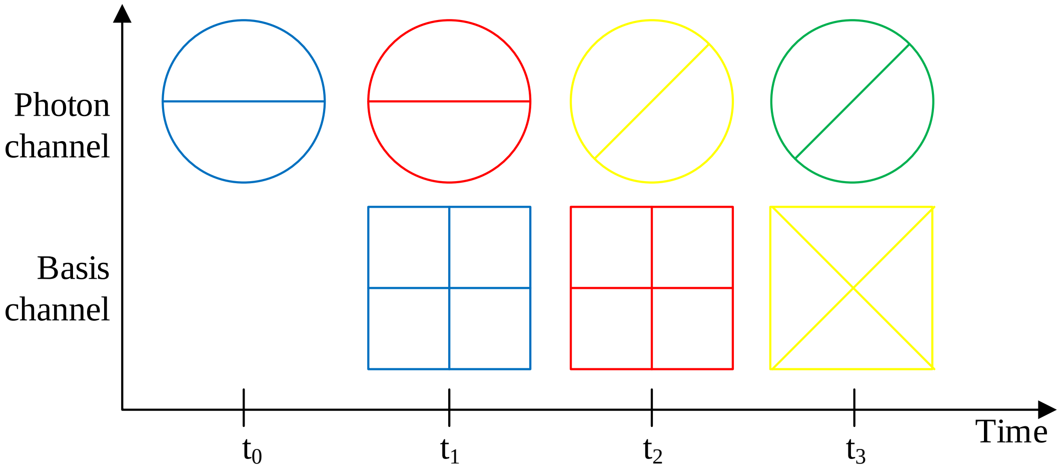


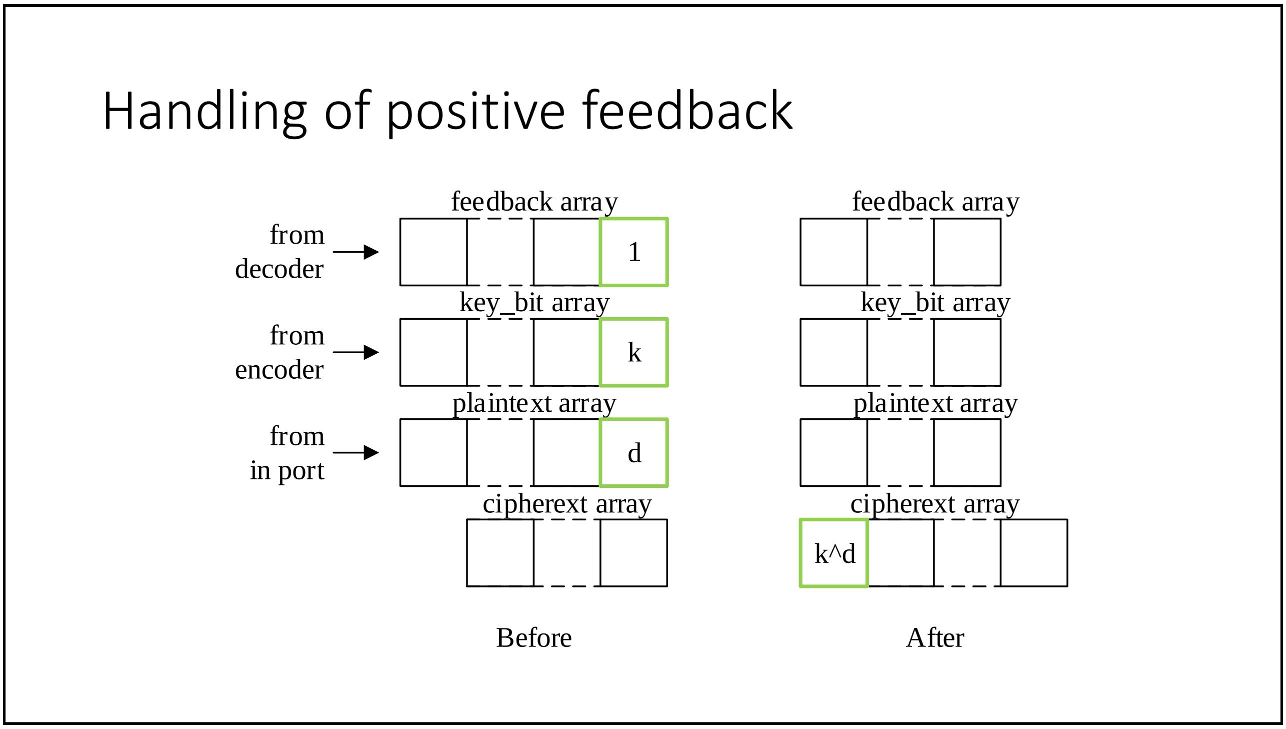
Behavior of encoder (2)

Behavior of encoder (3)

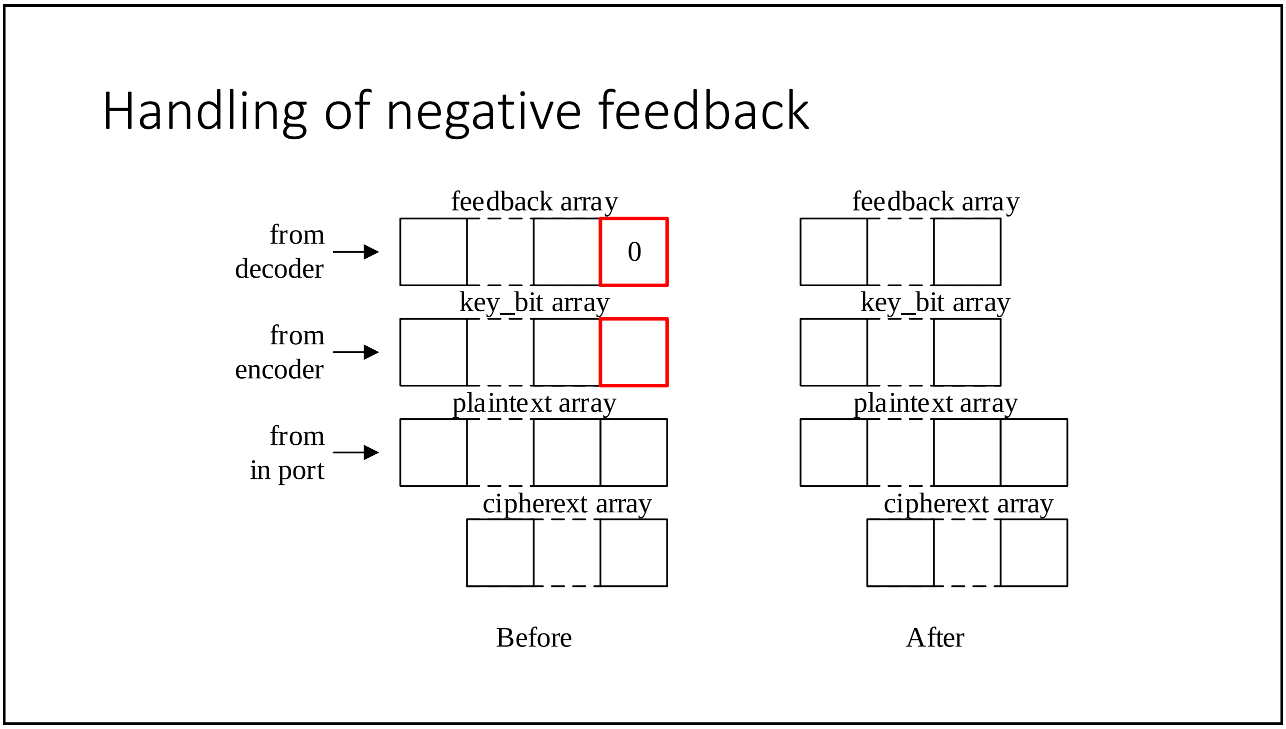


Behavior of encoder (4)





Handling of positive feedback



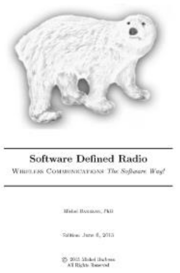
Handling of negative feedback

Links

Software

scs.carleton.ca/~barbeau/Publications/2015/gr-quantomm.tar.gz

scs.carleton.ca/~barbeau/SDRCRBook/



Software Defined Radio

Wireless Communications *The Software Way!*

Michel Barbeau, PhD

Edition: June 8, 2015

© 2015 Michel Barbeau
All Rights Reserved