Evolutionary Algorithms for the Design of Quantum Protocols

Walter O. Krawec[1] Stjepan Picek[2] Domagoj Jakobovic[3]

1: Department of Computer Science & Engineering, University of Connecticut, Storrs CT 06269, USA

2: Cyber Security Research Group, Delft University of Technology, Mekelweg 2, Delft, The Netherlands

3: Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Quantum Key Distribution (QKD)

- Allows two users – Alice (A) and Bob (B) – to establish a shared secret key
- Secure against an all powerful adversary
  - Does not require any computational assumptions
  - Attacker bounded only by the laws of physics
  - Something that is not possible using classical means only
- Very practical technology today...!
  - And in the future will play an even more important role.

QKD in Practice

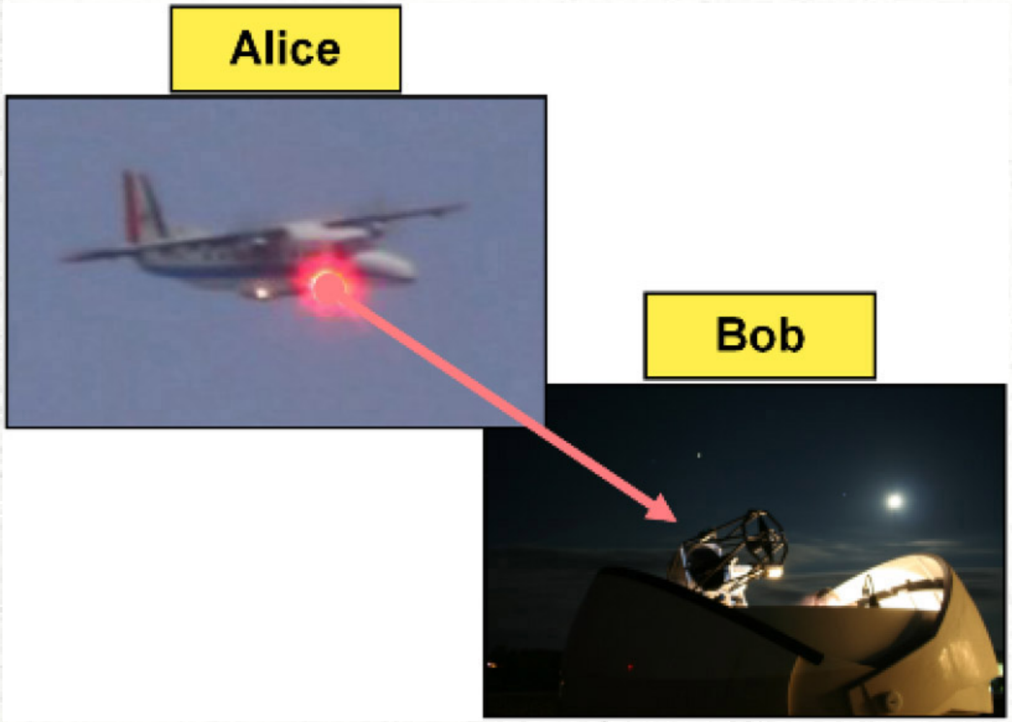
- Several companies produce commercial QKD equipment
    - Qubitekk, ID Quantique, Toshiba, Quintessence Labs

Qubitekk.com

idquantique.com

toshiba.eu

QKD in Practice: Freespace



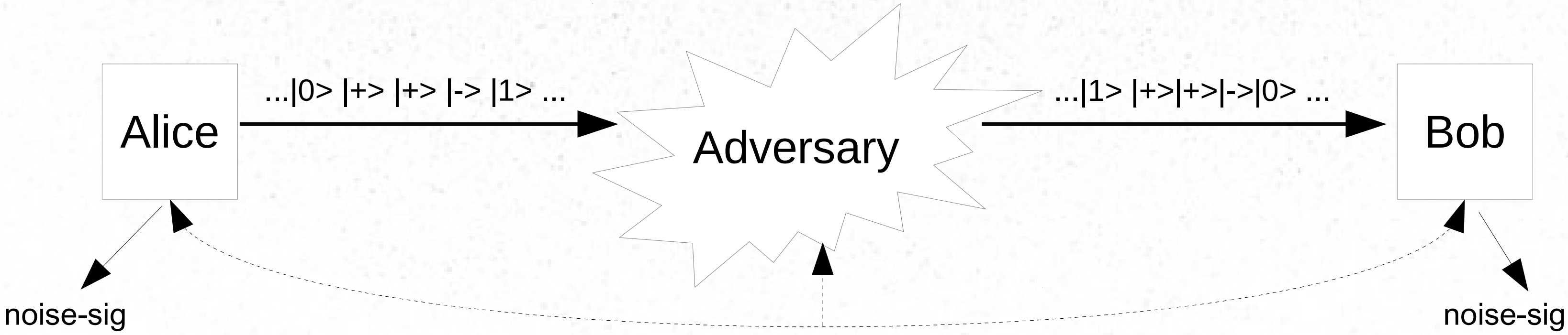
http://spie.org/newsroom/5189-free-space-laser-system-for-secure-air-to-ground-quantum-communications

Our Work

- Typically, QKD protocols are designed and then analyzed to determine which channels they are secure over
    - e.g., six-state BB84 can tolerate up to 12.6% error on a symmetric channel
- But none of these protocols are necessarily optimal for certain attacks
- What happens if you invest in this technology, and find the quantum channel is “too noisy” to support standard protocols?

Our Work

- We propose a system that creates optimized protocols for a given channel
- Start with a particular quantum channel
  - Measure its noise though standard **quantum tomography** to produce a **noise signature**
  - This noise signature helps identify the type of attack being launched – or just natural noise



Our Work

- We propose a system that creates optimized protocols for a given channel
- Start with a particular quantum channel
  - Measure its noise though standard **quantum tomography** to produce a **noise signature**
  - This noise signature helps identify the type of attack being launched – or just natural noise
- Then, use an evolutionary algorithm to design a secure QKD protocol **optimized** to run over this channel
- Users then configure their devices to implement the protocol

(B) *The result is equal to or better than a result that was accepted as a new scientific result at the time when it was published in a peer-reviewed scientific journal.*

We find different protocols **equaling** the human-made BB84 on symmetric channels.

(D) *The result is publishable in its own right as a new scientific result — independent of the fact that the result was mechanically created.*

We find new protocols with different elements **achieving** the **optimal result**.

(E) *The result is equal to or better than the most recent human-created solution to a long-standing problem for which there has been a succession of increasingly better human-created solutions.*

We find asymmetric noise protocols that **outperform** the human-made designs.

Noise signature	Our solutions	BB84 (Optimal human–made design)
1%	**.864**	.864
5%	**.497**	.497
10%	**.152**	.152
12%	**.035**	.035

Channel #	Our solutions	BB84
C1:	**.066**	0 (Abort)
C2:	**.018**	0 (Abort)

(F) *The result is equal to or better than a result that was considered an achievement in its field at the time it was first discovered.*

Our solutions are at least as good as state of the art protocols and **better** on certain asymmetric channels.

(G) *The result solves a problem of indisputable difficulty in its field.*

Designing efficient QKD protocols along with **constrained** gate sets is an **extremely difficult** problem.

Noise signature	Our solutions	BB84 (Optimal human–made design)
1%	**.864**	.864
5%	**.497**	.497
10%	**.152**	.152
12%	**.035**	.035

Channel #	Our solutions	BB84
C1:	**.066**	0 (Abort)
C2:	**.018**	0 (Abort)

Closing Remarks

- We showed how evolution strategies may be used to evolve QKD protocols as circuits
  - Our algorithm can take into account user-specified restrictions (e.g., gate set available and aux. wires)
- Our method finds protocols matching the optimal BB84 on symmetric channels
- We also find protocols that can operate over channels where ordinary, **human designed**, protocols simply fail