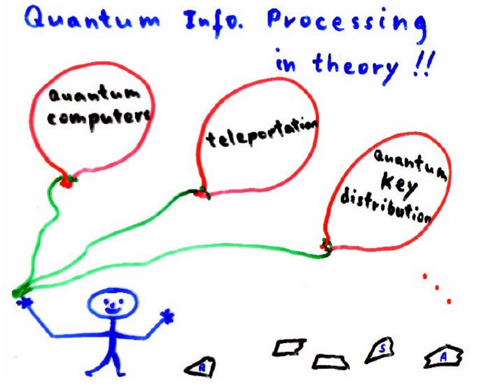
SHORT-TERM APPLICATIONS of QUANTUM INFORMATION PROCESSING

Tal Mor

Department of Computer Science
Technion- Israel Institute of Technology



Quantum Information Processing is very promising

Do we need to wait 20-30 years for an application?

Do we really need to wait 20-30 years for an application?

Quantum Cryptography

Unconditionally secure quantum key distribution (QKD)
Many experimental groups implementing QKD, and obtaining a "**secure**" key…
But is the key **truly secure also in practice**?

Quantum Computation

Algorithmic Cooling of Spins
Short-term application: improved NMR spectroscopy
[Long-term result: scalable NMR Quantum Computers]

Quantum Key Distribution

- Non-orthogonal quantum states
- No-cloning of such quantum states

→ **<u>Unconditionally</u> secure quantum key distribution**

(in theory)

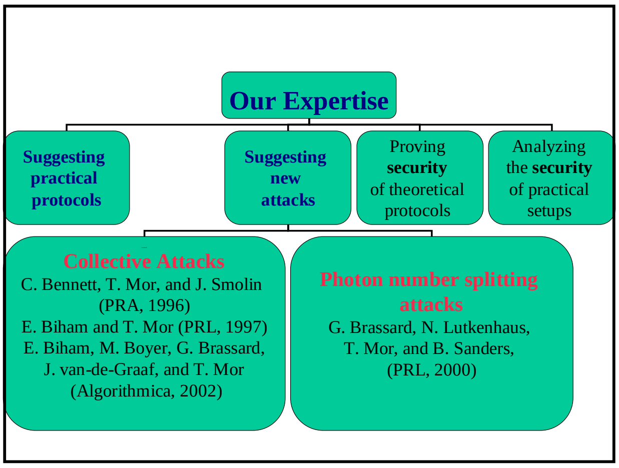
Practical QKD

But is the key **truly secure** also in practice???

Worldwide interest: various groups running practical QKD, performing **amazing** experiments

Experimental Groups: J. Franson; N. Gisin; R. Hughes; P. Kwiat; E.Polzik; J. Rarity; A. Sergienko; A. Zeilinger…

Companies: MAGIQ; BBN technologies; IBM; MITRE; NEC; MITSUBISHI; Idquantique; Qinetiq…



Our Expertise

Suggesting practical protocols

Suggesting new attacks

Proving **security** of theoretical protocols

Analyzing the **security** of practical setups

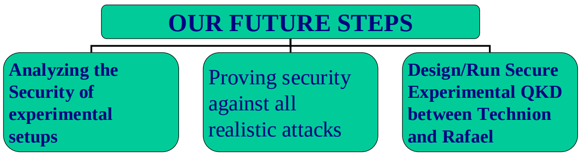
Collective Attacks
C. Bennett, T. Mor, and J. Smolin (PRA, 1996)
E. Biham and T. Mor (PRL, 1997)
E. Biham, M. Boyer, G. Brassard, J. van-de-Graaf, and T. Mor (Algorithmica, 2002)

Photon number splitting attacks
G. Brassard, N. Lutkenhaus, T. Mor, and B. Sanders, (PRL, 2000)

Worldwide Status of Security Analysis of Practical QKD

None of the practical protocols is proven secure. In particular, in September 2003:

- No practical scheme proven secure against **Collective Attacks!**
- No practical scheme proven secure against **Photon Number Splitting Attacks!**

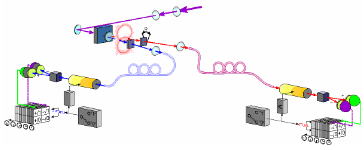


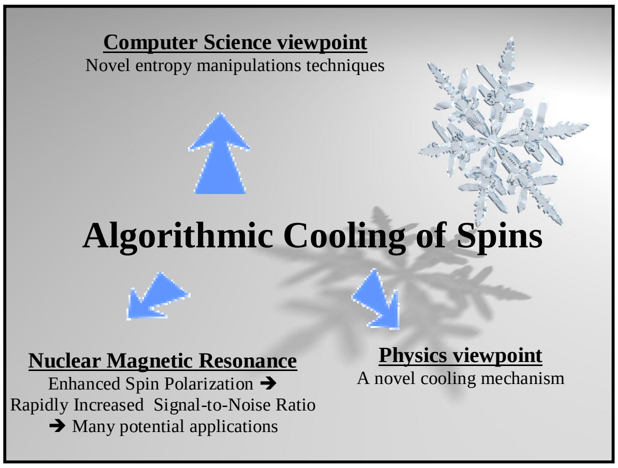
OUR FUTURE STEPS

Analyzing the Security of experimental setups

Proving security against all realistic attacks

Design/Run Secure Experimental QKD between Technion and Rafael





Computer Science viewpoint
Novel entropy manipulations techniques

Algorithmic Cooling of Spins

Nuclear Magnetic Resonance
Enhanced Spin Polarization ➔
Rapidly Increased Signal-to-Noise Ratio
➔ Many potential applications

Physics viewpoint
A novel cooling mechanism

Potential Future Applications

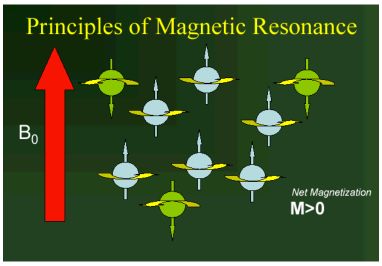
Enhanced Polarization

➔ Improved Signal-to-Noise ratio

Applications:

- Medical applications
- Monitoring brain activity (for instance, a lie detector)
- Identifying explosive materials
- Identifying narcotics
- Checking stability of materials exposed to severe conditions

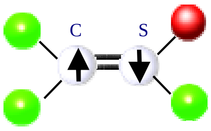
Nuclear Magnetic Resonance



Nuclei's spins in a magnetic field
Spin-half nucleus: a quantum bit

A Simple Logic Gate

$$\begin{array}{ccc} cs & & cs' \\ |00\rangle & \rightarrow & |00\rangle \\ |01\rangle & \rightarrow & |01\rangle \\ |10\rangle & \rightarrow & |11\rangle \\ |11\rangle & \rightarrow & |10\rangle \end{array} \qquad \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$



A molecule with two spins ➔ 2-bit computer
Manipulations of spins ➔ a gate operating on bits

Implementation of a gate: via a set of NMR pulses on a regular NMR machine

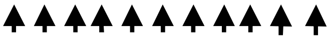
Magnetic Resonance: Polarization-Bias and Temperature

$$\Pr(\uparrow) = \frac{1+\varepsilon}{2} \qquad \Pr(\downarrow) = \frac{1-\varepsilon}{2}$$

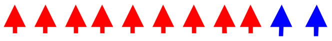
ε – *polarization* bias

$\varepsilon \rightarrow 0 \Leftrightarrow$ ↑ $\qquad \varepsilon \rightarrow 1 \Leftrightarrow$ ↑

Polarization Enhancement (Cooling)



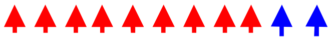
- **Data compression:** some spins can be cooled quite a lot (L. Schulman & U. Vazirani) using simple logical gates, while the rest of the spins get hotter
- The cold spins are pushed spatially to the edge of the molecule



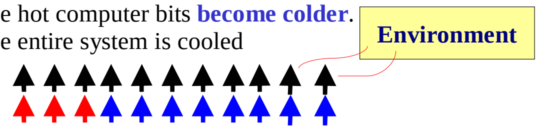
- Limited by Shannon's bound on data compression
- Therefore **impractical**

Algorithmic Cooling

1. Data compression steps:

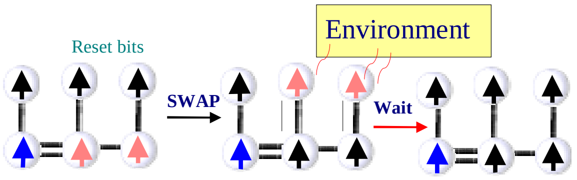


2. In addition to the computer bits, there are reset bits, namely spins that rapidly interact with the environment
3. Hot computer spins are "**thermalized**" via a SWAP with the reset spins (that can be re-used soon after)
4. The hot computer bits **become colder**.
5. The entire system is cooled



- This way Shannon's bound is bypassed!

Thermalization



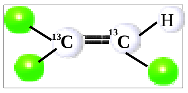
"Algorithmic Cooling and Scalable NMR Quantum Computers"
P. O. Boykin, T. Mor, V. Roychowdhury, F. Vatan, R. Vrijen
(Proceedings of the National Academy of Science, 2002);

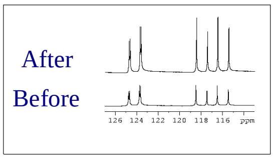
Algorithmic Cooling is patent pending

Cooling by Thermalization

We succeeded to **cool down 2 Carbons**
to a low temperature of ~ 150 K

TCE molecule





G. Brassard, J. Fernandez, R. Laflamme, T. Mor, & Y. Weinstein

Summary :
- Practical QKD is not yet proven secure
- Algorithmic Cooling is the first short-term application of quantum computing