Post-Quantum Cryptography
A Collective Challenge

Christophe Petit

University of Oxford
Mathematical Institute

Cryptography is very useful

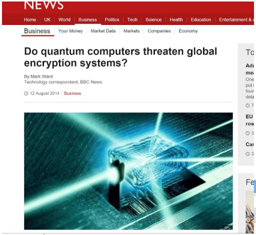
- Cryptography is the science and art of ensuring private and authenticated communications
- Used everyday in TLS, bank cards, mobile phones,. . .

How we build trust in cryptography protocols

- Precisely define what it means to break the protocol
  - Adversary's goal
  - Adversary's resources
  - Adversary's access to the system
- Choose your favorite hard problem
  - A computational problem that cannot be solved, even by clever people with the best computers available
- Build a protocol so that you can prove

  Breaking the protocol $\Rightarrow$ Solving the hard problem

The threat of quantum computers



NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Education | Entertainment & A

Business | Your Money | Market Data | Markets | Companies | Economy

Do quantum computers threaten global encryption systems?

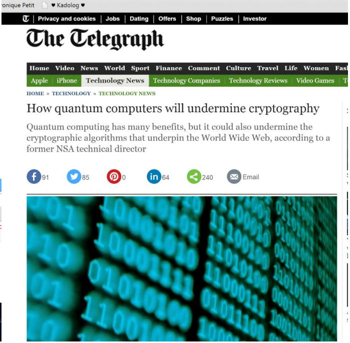
By Mark Ward
Technology correspondent, BBC News

12 August 2014 | Business

makeuseof

Quantum Computers: The End of Cryptography?

Written by Andre Infante
November 16, 2014



ronique Petit | ♥ Kadolog ♥

Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles | Investor

The Telegraph

Home | Video | News | World | Sport | Finance | Comment | Culture | Travel | Life | Women | Fas

Apple | iPhone | Technology News | Technology Companies | Technology Reviews | Video Games | T

HOME » TECHNOLOGY » TECHNOLOGY NEWS

How quantum computers will undermine cryptography

Quantum computing has many benefits, but it could also undermine the cryptographic algorithms that underpin the World Wide Web, according to a former NSA technical director

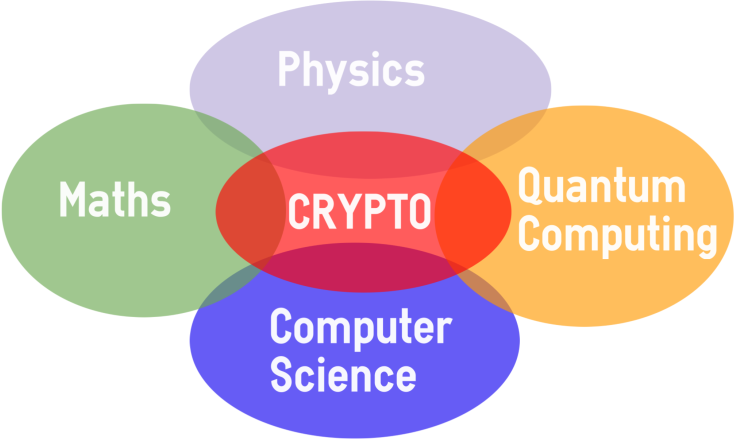
- Quantum computers change the boundaries between hard and easy problems

Post-Quantum Cryptography

- Abandon factoring and discrete logarithm problems
- Double your key sizes to resist Grover's search
- Find quantum-hard computational problems
- Build a protocol such that you can prove

  Breaking the protocol $\Rightarrow$ Solving the hard problem
- Evaluate how practical your protocol is, and improve it

Collaborations needed !



Cryptanalysis

- Not just factoring in polynomial time !

- Can allow larger time / memory
- May succeed only with some small probability
- May target special instances of the general problem
- May give unexpected power to the attacker (decryption oracle, side-channel, fault, cold boot attacks)
- May solve several instances on average faster than one
- Asymptotic and/or practical attack
- May combine several techniques

Quantum Cryptanalysis

- Solve search, factorization & discrete logarithm problems using Grover and Shor algorithms
- Find new cryptanalysis-relevant (sub)-problems which can be solved with Grover and Shor
- Modify Grover and Shor, or any quantum algorithm to target one of these subproblems
- Find new quantum attack scenarios, new physical threats
- Use the D-WAVE for what it can already do
- Design new quantum algorithms

Classical Cryptanalysis

- Confidence that discrete logs and factorization problems are (classically) hard comes from decades of attempts
- Are post-quantum candidates classically secure ?
    - **Special instances of NP-hard problems**
    - **Short factorizations in non-Abelian groups** : given a non Abelian finite group G, a generator set S, and a group element h, compute a *short* factorization $h = \prod_{s_i \in S} s_i$
    - **Isogeny problems** : given two isogenous supersingular elliptic curves, compute an isogeny between them

Building cryptography : Theory

- **Wanted : one-way functions**
  - A function that is easy to compute, but hard to invert
  - Enough for authentication purposes (signatures)
- **Wanted : trapdoor one-way functions**
  - A one-way function that can be inverted given some additional information (the trapdoor)
  - Enough for public key encryption
- **Wanted : hard problems**
  - Current (trapdoor) one-way functions from discrete logs, factorization, lattice, polynomial system problems, . . .
  - Do you know any other hard problems ?

Building cryptography : Practice

- Theoretical constructions from (trapdoor) OW functions can be too inefficient, may need ad hoc constructions
- Much more than just signature and encryption
- Find best parameters for efficiency and security
- Make sure to resist physical attacks
- Write new cryptographic standards
- Ensure backward-compatibility (or not)
- Enforce post-quantum migration in applications

Conclusion

- Post-quantum cryptography is a huge challenge
- The cryptography community is currently addressing it, but we definitely welcome and need your help
- There is a lot of relevant expertise in Oxford, we would love to get more interactions
- Lots of fun problems to tackle for everyone !