Cryptography and quantum computers: Where do we stand?

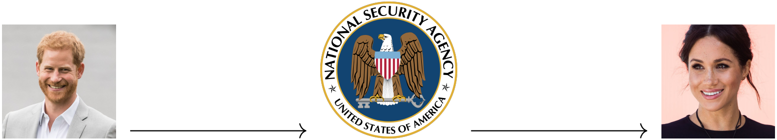
Dr Chloe Martindale

Lecturer in Cryptography,
University of Bristol

Engineering Faculty Research Showcase, 22nd April 2021

What is this all about?

Cryptography

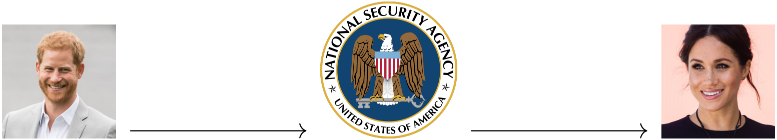


Sender

Channel with eavesdropper ‘Eve’

Receiver

Cryptography

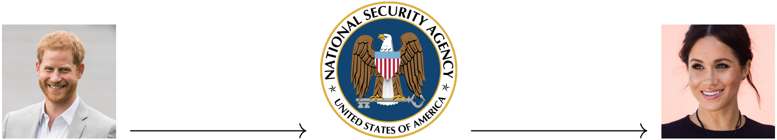


Sender Channel with eavesdropper ‘Eve’ Receiver

Problems:

- Communication channels store and spy on our data
- Communication channels are modifying our data

Cryptography



Sender | Channel with eavesdropper 'Eve' | Receiver

Problems:

- Communication channels store and spy on our data
- Communication channels are modifying our data

Goals:

- Confidentiality despite Eve's espionage.
- Integrity: recognising Eve's espionage.

(Slide mostly stolen from Tanja Lange)

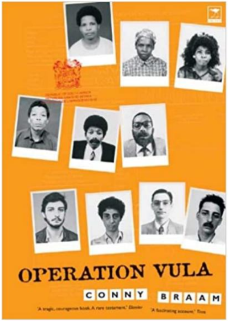
Example: encrypted messaging with one-time-pads

- Message: a bit string (e.g. $m = 1001100$)
- OTP: also a bit string (e.g. $k = 0111000$)
- Encrypted message: line up m and k, and flip the bit of m if the corresponding bit in k is 1:

$$\begin{array}{c} 1\,0\,0\,1\,1\,0\,0 \\ 0\,1\,1\,1\,0\,0\,0 \\ \downarrow \\ 1\,1\,1\,0\,1\,0\,0 \end{array}$$

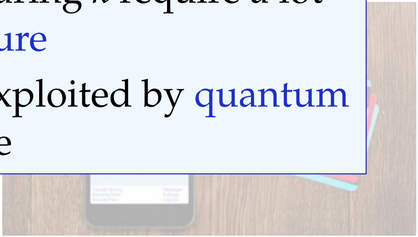
Anti-Apartheid
Movement

THE
VULA CONNECTION

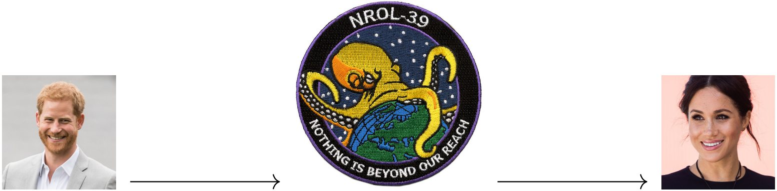

OPERATION VULA
CONNY BRAAM
'A tragic, courageous book. A rare testament.' Elsevier
'A fascinating account.' Trou

Online Banking
$ 304.02
Credit Card
1234 5678 9012 3456
CURRENT NAME

- All of these require sharing a key k securely
- Current methods of sharing k require a lot of mathematical structure
- This structure can be exploited by quantum computers in the future



My research: post-quantum cryptography

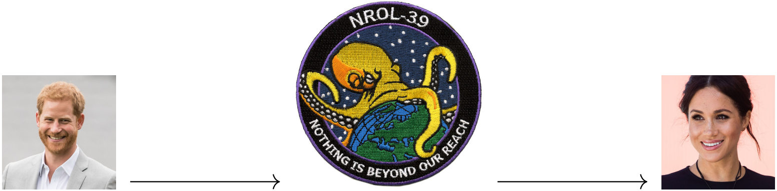


Sender

Channel with eavesdropper ‘Eve’

Receiver

My research: post-quantum cryptography



Sender

Channel with eavesdropper ‘Eve’

Receiver

- Eve has a quantum computer.
- Sender and receiver don’t have a quantum computer.

Where are we now?

- Post-quantum cryptography discussion dominated by NIST competition for standardization.

Where are we now?

- Post-quantum cryptography discussion dominated by NIST competition for standardization.
- This initiative comes after a US report with:

> **Key Finding 10:** Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster.

Where are we now (according to NIST)?

The NIST not-a-competition:

- Had 82 submissions in 2017.
- 69 were accepted.
- 15 submissions currently in 3rd round, aiming for a total of 4 rounds.
- Aiming for standardization in 2022.
- Only covers digital signatures and key encapsulation (c.f. “sharing k securely”).

Important open problems/research directions

Needed for many post-quantum candidates:

- Thorough cryptanalysis – classical and quantum.
- Secure and efficient implementation (especially considering hardware limitations).
- Meaningful comparison between candidates (must come from comparable implementations).
- More advanced protocols (e.g. for privacy, zero-knowledge etc).

Thank you! Questions?