PQC in Context
The 4th Crypto Crisis in a Century

Whitfield Diffie, ForMemRS

Gonville and Caius College
Cambridge University

Tuesday 17 March 2026

National

Cryptologic

Foundation

.

Copyleft

- If you are seeing or hearing this lecture you are entitled to record it.
- If you have a recording you are entitled to copy it.
- You are entitled to redsetribute any copy under the same terms.

"Modern" Cryptography Was Conceived Twice

- 200AH—Al Kindi in Baghdad
- 1500AD—Alberti et al. in Italy

The basic ideas are not new.

Basic Ideas

- Polyalphabetic Ciphers: substitution must change from character to character.
- Two techniques:

  table lookup

  some kind of arithmetic

Q: Why was cryptography so slow to develop?

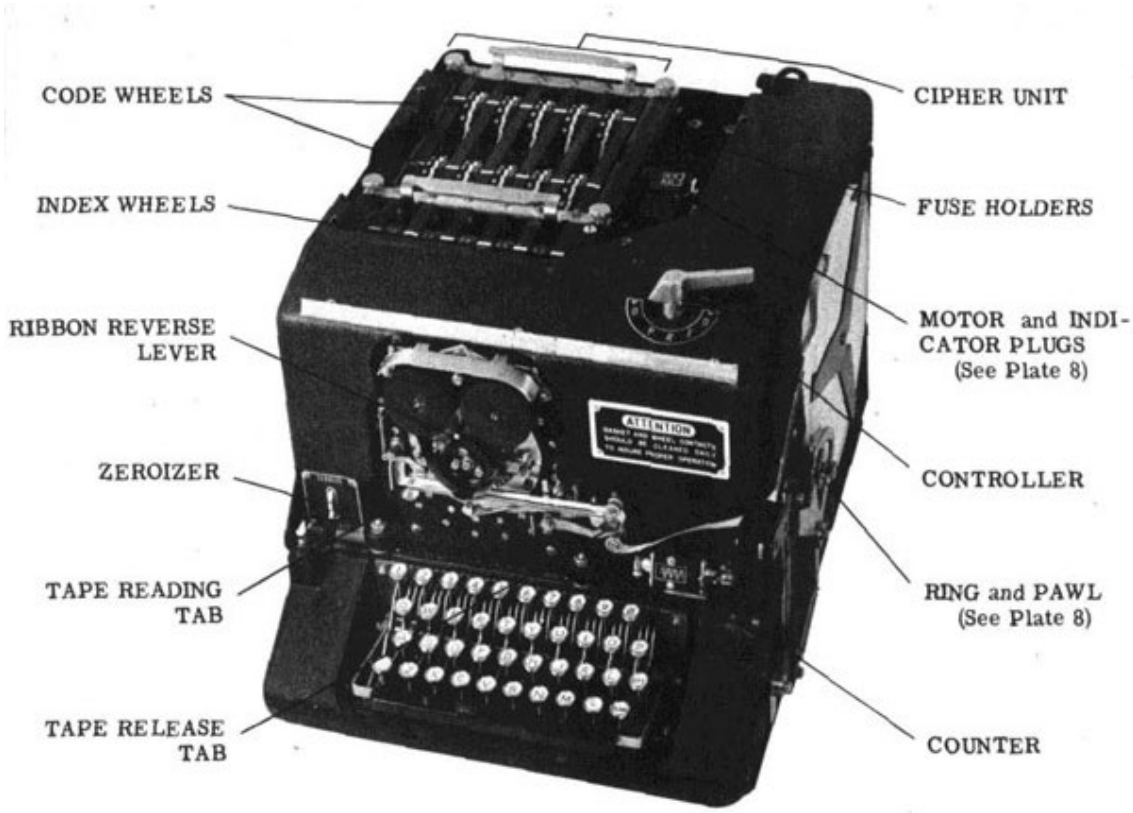
A: You can't really do it without machine computing.

Every generation or so, cryptography goes through a big transition caused by new requirements and new techniques. Quantum computing is the current one; there have been several; and there will surely be more.

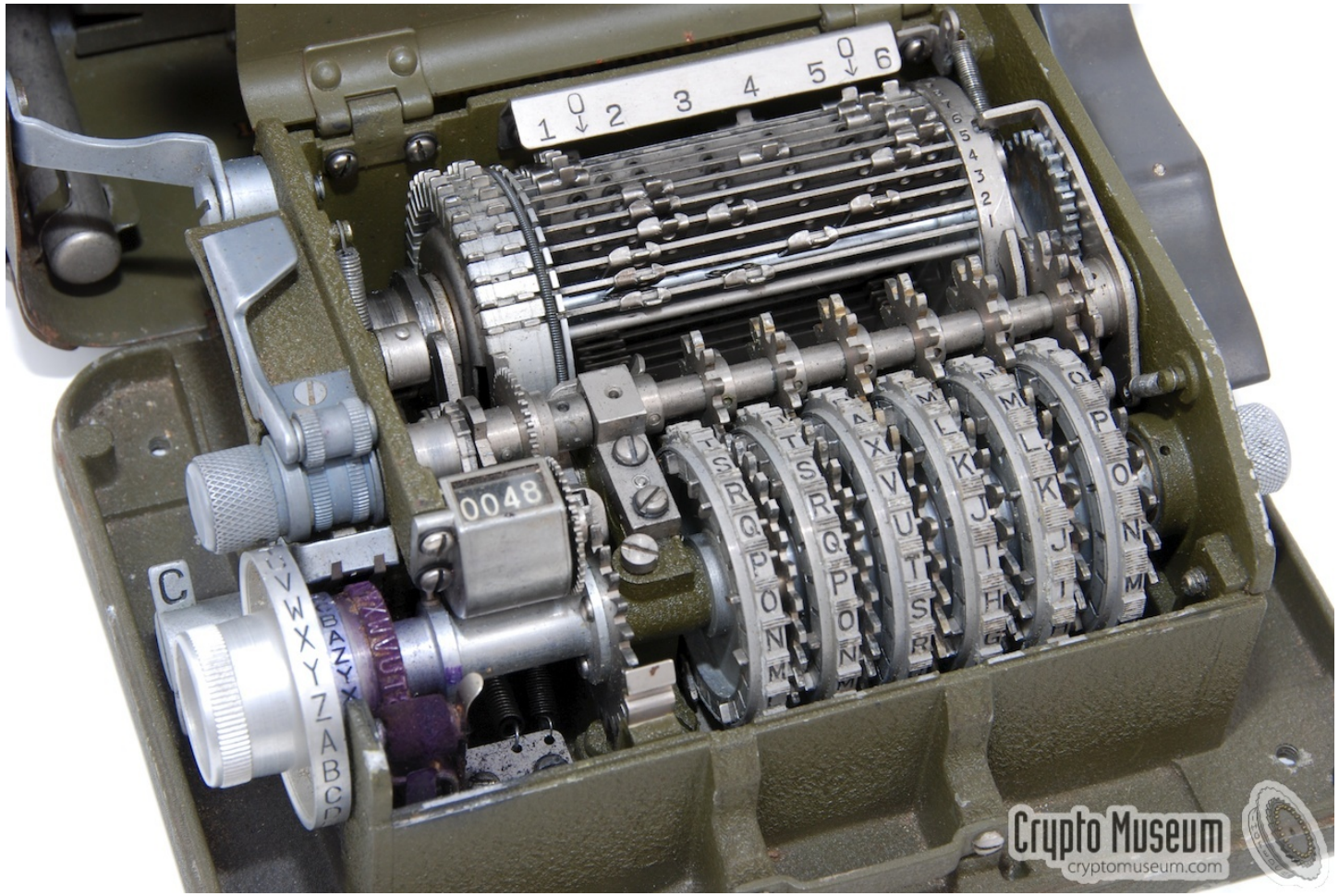
World War I
Birth of Modern Cryptography

- Challenge: Radio
- Techniques: Machining and Electricity

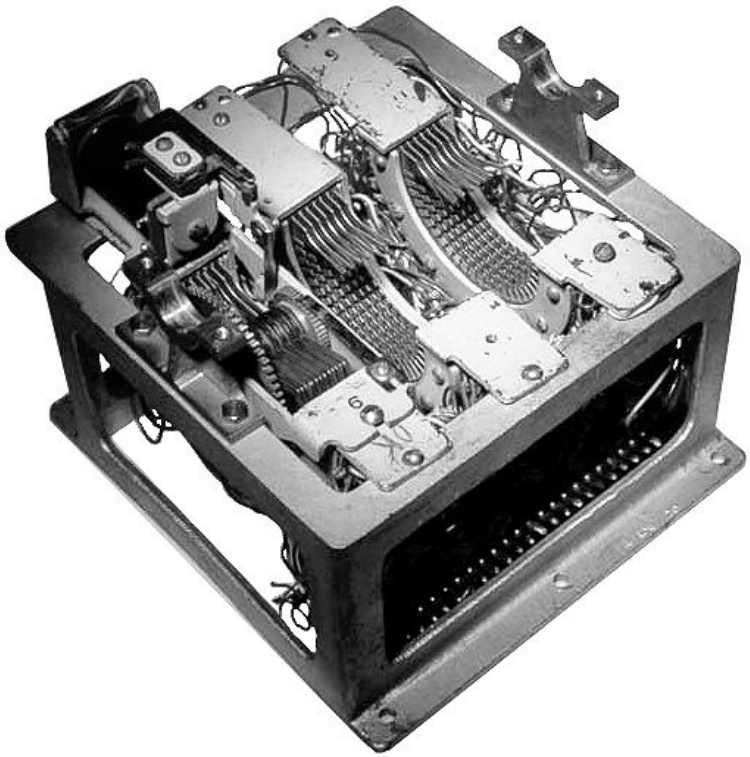
Rotor Machines



Pinwheel Machines



Stepping-switch Machines

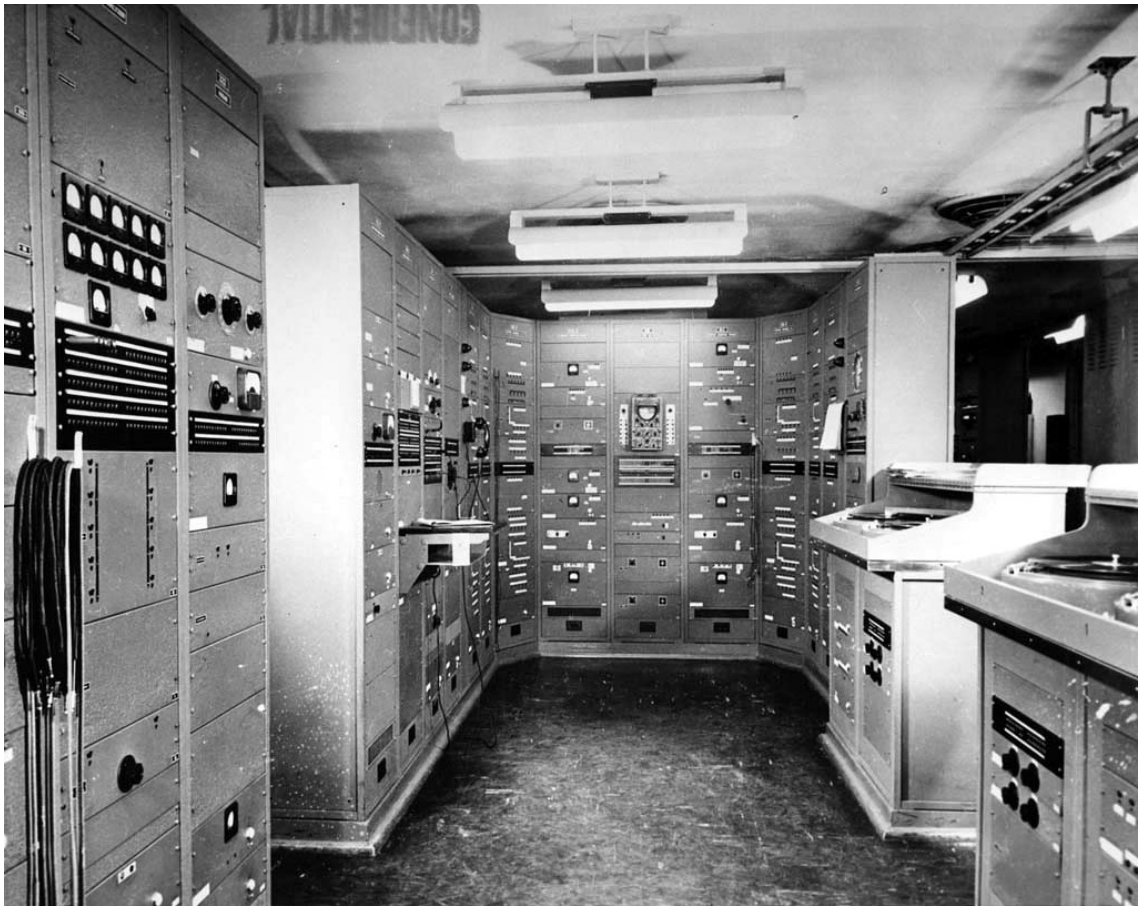


The Japanese machine that the U.S. called Purple, was made of stepping switches, available, non-custom, parts.

World War II
Rise of Electronics

- Challenge (hard to hide): traffic volume
- Challenge (secret): Computing
- New technique: Electronics

Sigsaly



World's first digital telephone

Many Elements Over a 30-Year Period

- Custom Electronics (shift registers)
- Computer-like machines
- Stream ciphers go to block ciphers

Late 20th Century Change of Scale

Challenge: Birth of the Internet

Techniques:

- Cryptography goes public
- Public-key cryptography
- Cryptography in software
- Cheap computing and storage

Early 21st Century Quantum Computing

- Challenge: Quantum Computing
- Techniques: New Cryptosystems

How Does Quantum Computing Break Public-Key Crypto?

- In a public-key system, anyone can do the forward operation.
- It is going back that is hard.

The step just before where you are is the decryption of what you started with.

Like a Race Track

You Can't Go Back

Like moving on a track, if you go forward long enough, you will get back where you started.

In systems like Diffie-Hellman and RSA, it is easy to move a long way forward very quickly.

The Secret in RSA

- Factors?

  Alternatively

- Length of a cycle $(p-1)(q-1)$

Shor's Algorithm Affects Public-Key Systems

Finds cycle length.

It will tell you how far to go.

Breaks the currently-used public key systems.

Grover's Algorithm Affects Everything But Not As Much

Square-roots sorting

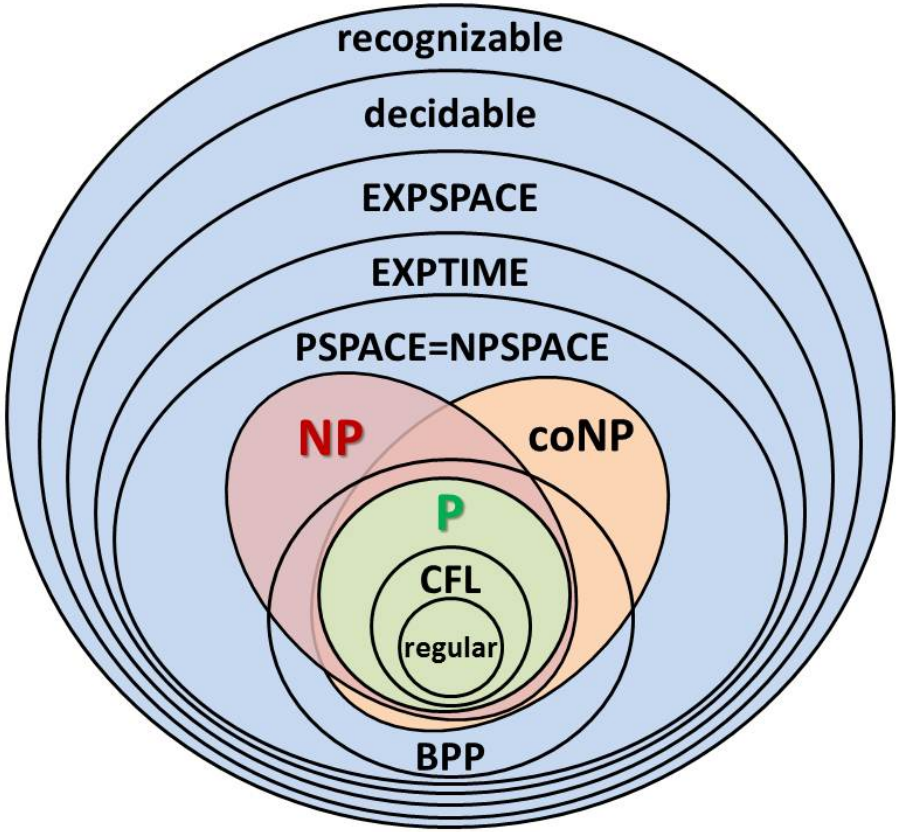
Not Much Affected

- Symmetric cryptography (AES)
- Message digests (secure-hash functions)
- Merkle trees (blockchains)

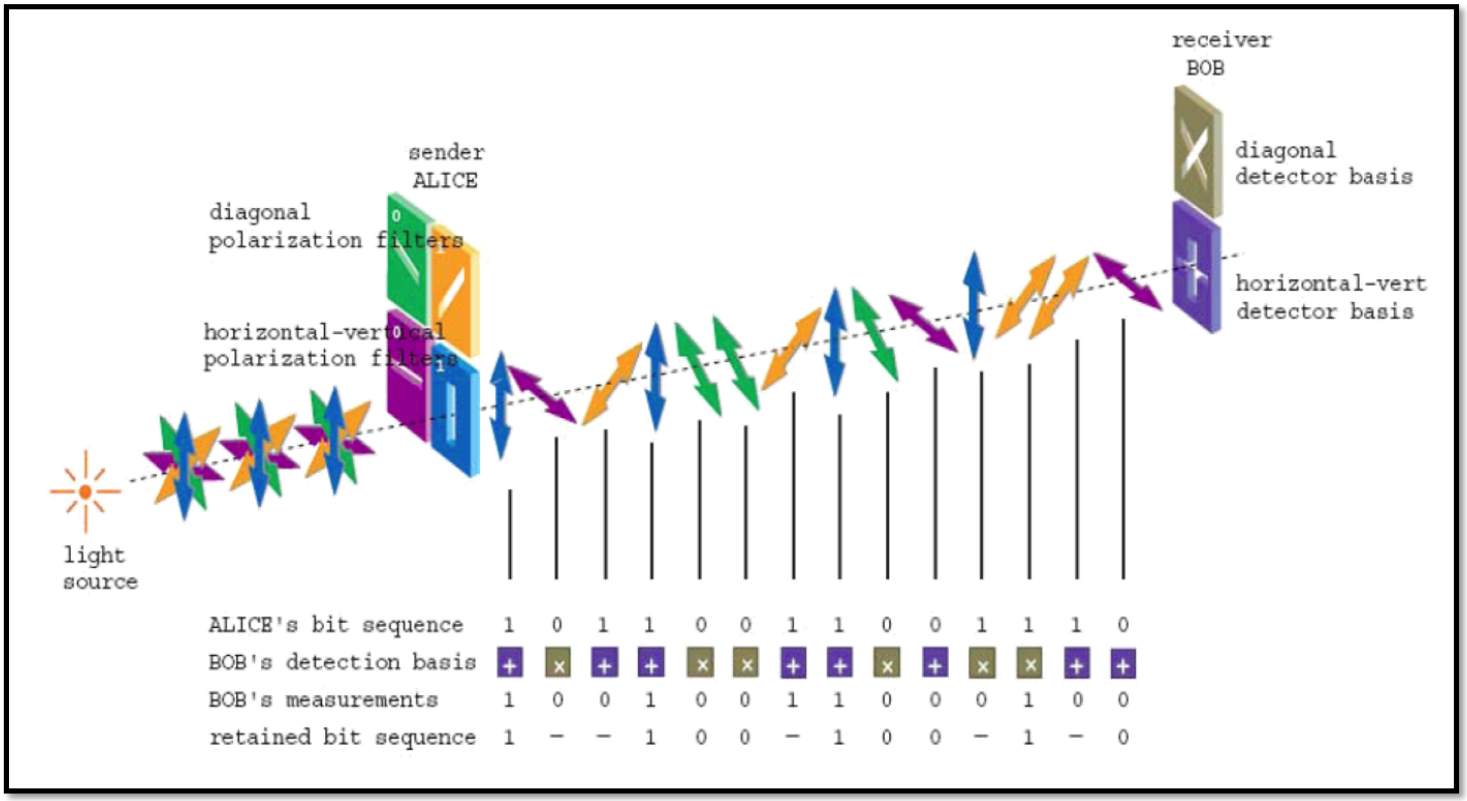
Very Much Affected

- Key negotiation
- Digital signatures

Looks Like and Isn't
$P = NP$?



Sounds Like and Isn't Quantum Key Distribution



The Coming Threat

- Quantum computing breaks authentication
- Allows hackers to trick their way in
- Requires having quantum computer

The Current Threat

- Quantum computing breaks confidentiality
- Collect (Harvest) now
- Exploit (Decrypt) later
- Hardly new: happening at least since WWI (E.g., 1945–1980: Venona project)

How Is This Crisis Different From the First Three

- More public (wider utility of QC)
- Widespread expert workforce
- International cooperation
- More warning

The Current Situation

- Quantum Computing may threaten current public-key cryptography within years.
- NSA and NIST have proposed new "quantun-safe" systems and set out a ten-year timeline.

Unknowns

- Is there a quantum-computing "Moore's Law"
- Should we change systems in all uses?
- Will new quantum algorithms increase the threat?
- Will new cryptosystems address the threat?