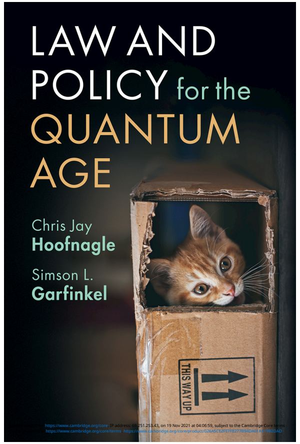
The likely impact of quantum computing on the *extraction and* authentication of digital evidence

Simson L. Garfinkel
Chief Scientist, BasisTech, LLC

Kyushu University
October 24, 2025
Fukuoka, Japan



Abstract

Today most digital evidence is authenticated using cryptographic algorithms and procedures developed in the 1990s. Digital evidence is typically processed with a cryptographic "hash function" and then, occasionally, digitally signed. The security of these algorithms has steadily eroded over time as a result of advances in computing power and cryptographic understanding. It might suddenly crumble with the development of a practical cryptographically relevant quantum computer (CRQC).

In this talk, Dr. Garfinkel will present the mathematical underpinnings of digital evidence certification and validation with numerous examples.

He will then present an introduction to quantum computing, discuss the likely impact on digital evidence, and introduce work on so-called "post-quantum cryptography.”

Outline for today's talk

Digital Evidence:

What is it?

How do we get it?

How do we authenticate it?

A Cryptographically Relevant Quantum Computer (CRQC)

What is it?

Will we get it?

What will its impact be on digital evidence?

What should we do? A strategy for innovation and deployment.

Digital Evidence

Digital information is all around us today.

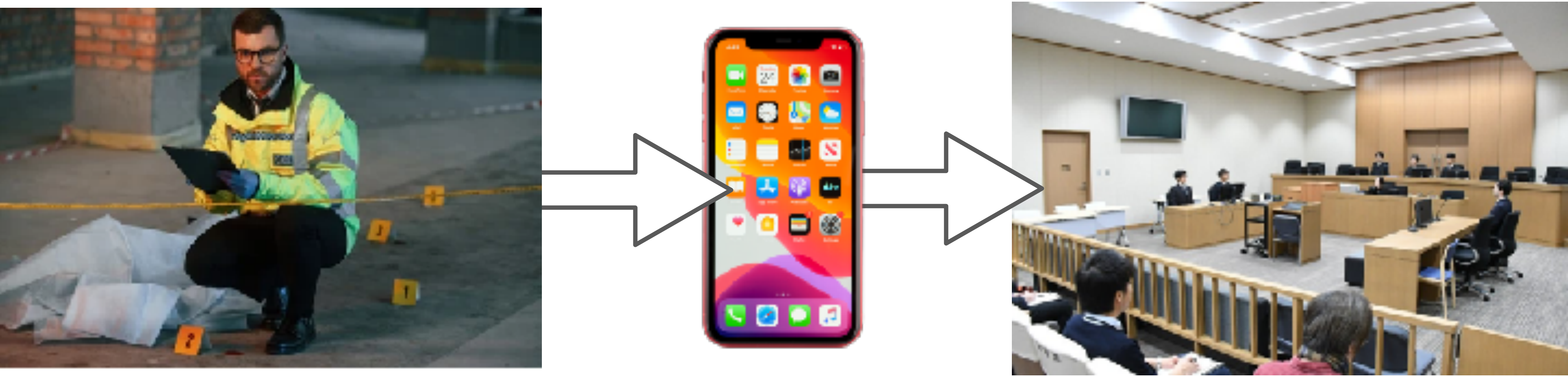
“Digital evidence is information stored or transmitted in binary form that may be relied on in court.” — US National Institute of Justice

NIJ | NATIONAL INSTITUTE OF JUSTICE
ADVANCING JUSTICE THROUGH SCIENCE
About | Contact Us | Subscribe | Topics A-Z
Search

Digital & Multimedia Evidence

Computers are used for committing crime, and, thanks to the burgeoning science of digital evidence forensics, law enforcement now uses computers to fight crime.

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime.

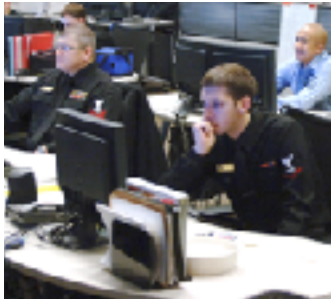


The digital forensics *process* involves many steps.

Preparation: policy, training & tools

Collect & preserve evidence

Extract preserved data



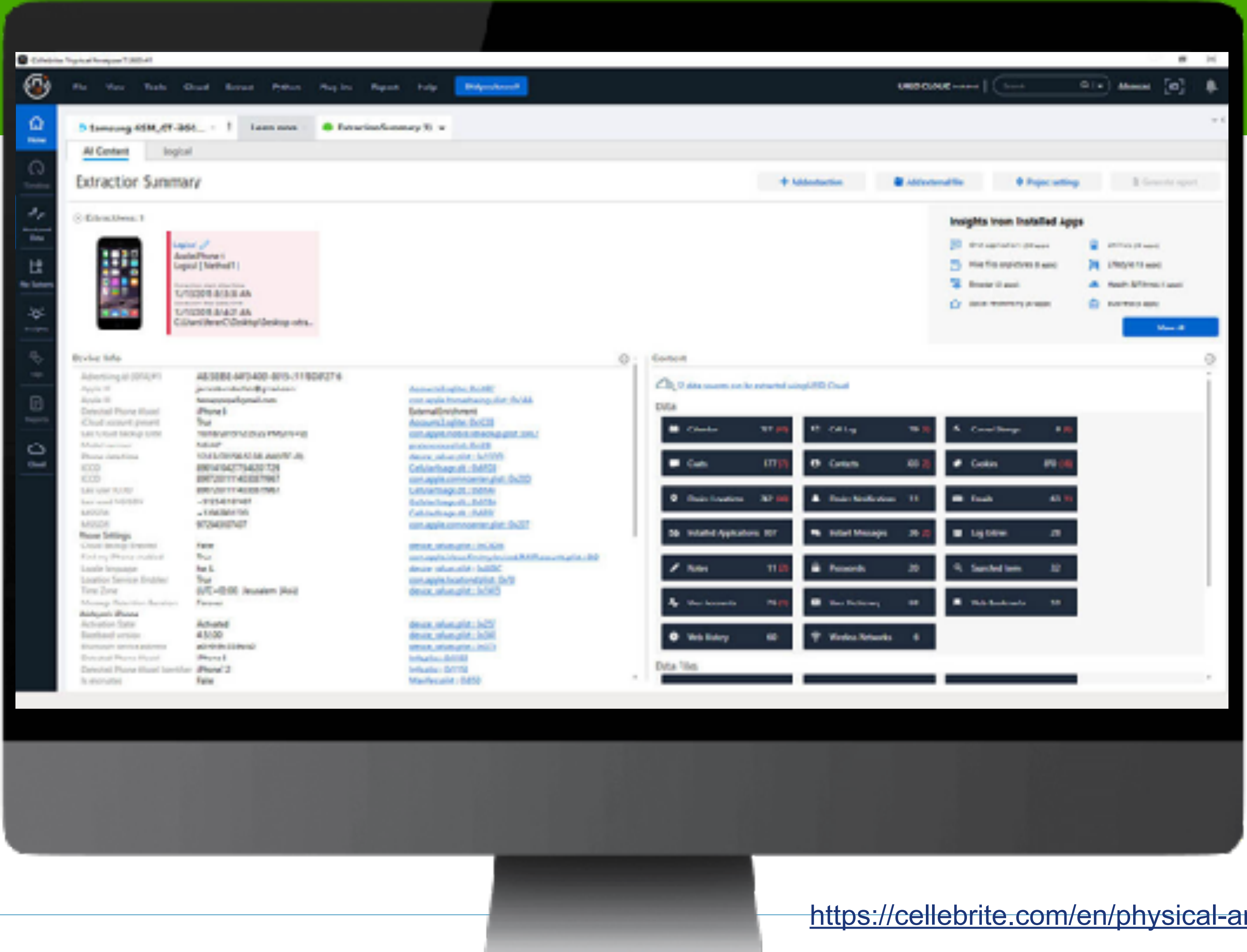
Analysis

Reporting & Testimony

Digital Evidence Extraction

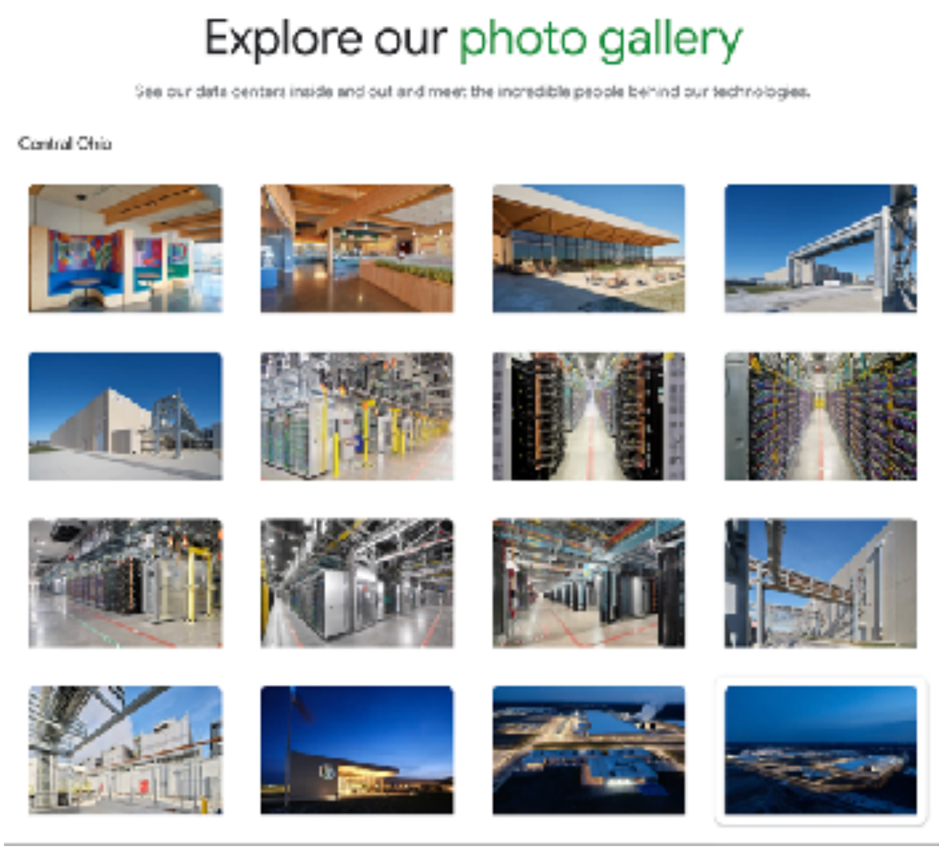
Data can be extracted from mobile devices

Evidence file



https://cellebrite.com/en/physical-analyzer/

Data can be downloaded from the cloud



Explore our photo gallery

See our data centers inside and out and meet the incredible people behind our technologies.

Central Ohio

https://datacenters.google/discover-more/photo-gallery/

Data can be downloaded from the cloud

email messages
location data
page views
cloud storage files

https://datacenters.google/discover-more/photo-gallery/

Cryptography plays an important role in digital forensics

(Evidence file)$_{\text{hash}}$

1. Cryptographic hash functions assure that evidence is *unaltered after acquisition*

2. Occasionally, encrypted data are forcibly extracted and decrypted.

$(\text{Evidence file})_{\text{hash}}$

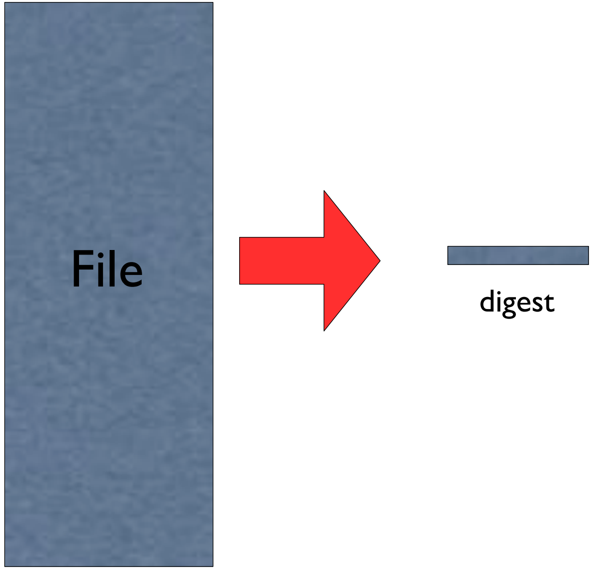
1. Cryptographic hash functions assure that evidence is *unaltered after acquisition*

Cryptographic Hash Functions (a.k.a. message digests)

Input: 1-2^{64} bytes

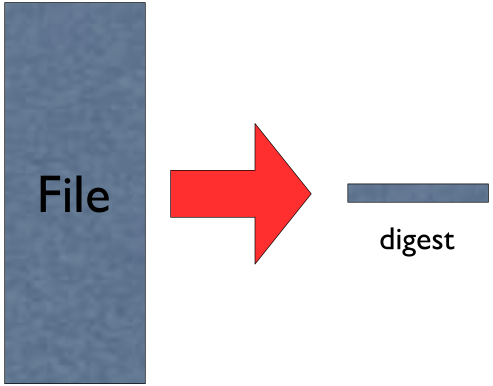
Output: 128, 160, 256 or 512 bits — each bit with ~50% of being 1 or 0

Common hash functions: MD5, BLAKE, RIPEM, SHA1, SHA2, SHA3, …



The same input always produces the same hash value.

"All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood."



```
$ echo -n "All human beings are born free and equal in dignity and rights. They
are endowed with reason and conscience and should act towards one another in a
spirit of brotherhood." | openssl sha256

SHA2-256(stdin)= a2ccb5fb55a20f5d5db80ecf01a1e24803441a328040261fd07466369b09a345
```

Change one bit, and half the output bits change.

```
$ echo –n 'All human beings are born free and equal in dignity and rights. They
are endowed with reason and conscience and should act towards one another in a
spirit of brotherhood.' | openssl sha256

SHA2–256(stdin)= a2ccb5fb55a20f5d5db80ecf01a1e24803441a328040261fd07466369b09a345
```

```
$ echo –n 'All human beings are born free and equal in dignity and rights. They
are endowed with reason and conscience and should act towards one another in a
spirit of brotherhood!' | openssl sha256

SHA2–256(stdin)= 949e90c8ddfd91f167c8dee7b88bb8893ce38a447941c3e23c817922a003093c
```

64 Hexadecimal numbers (0-9a-f) = 256 bits

Sometimes called a file “fingerprint”

a2ccb5fb55a20f5d5db80ecf01a1e24803441a328040261fd07466369b09a345

Good analogy:

- No two files should have the same hash value.
- You can identify a file given a database of hash values.
  - —*Similar to identifying a person from a database of fingerprints.*

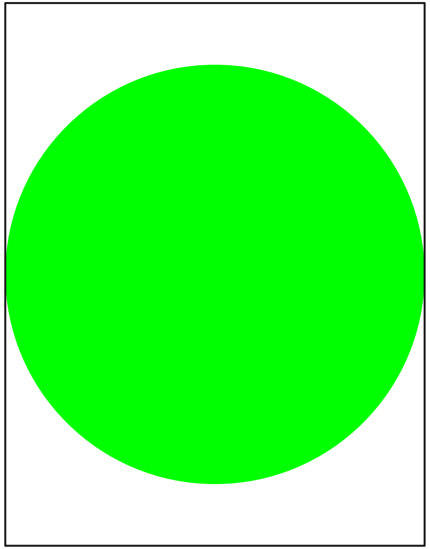
But…

- How do we know that no two people have the same fingerprint?

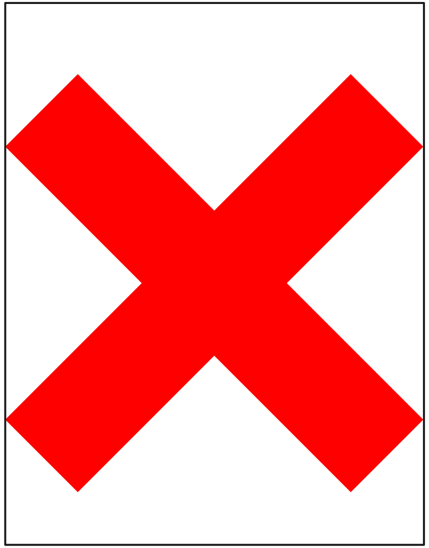
Some hash functions have been "broken" — two documents have the same hash.

MD5 is "broken"

Both of these files have the same MD5 hash value.



md5-1.pdf



md5-2.pdf

MD5(md5-1.pdf)= 150df5a6596a8c06a879c4b84e331c8a
MD5(md5-2.pdf)= 150df5a6596a8c06a879c4b84e331c8a

https://github.com/corkami/collisions/tree/master

Hash functions today

Rivest Functions (don’t use these)

~~MD2 (RFC 1319), MD4 (RFC 1320), MD5 (RFC 1321)~~

NIST Functions (FIPS 180-4)

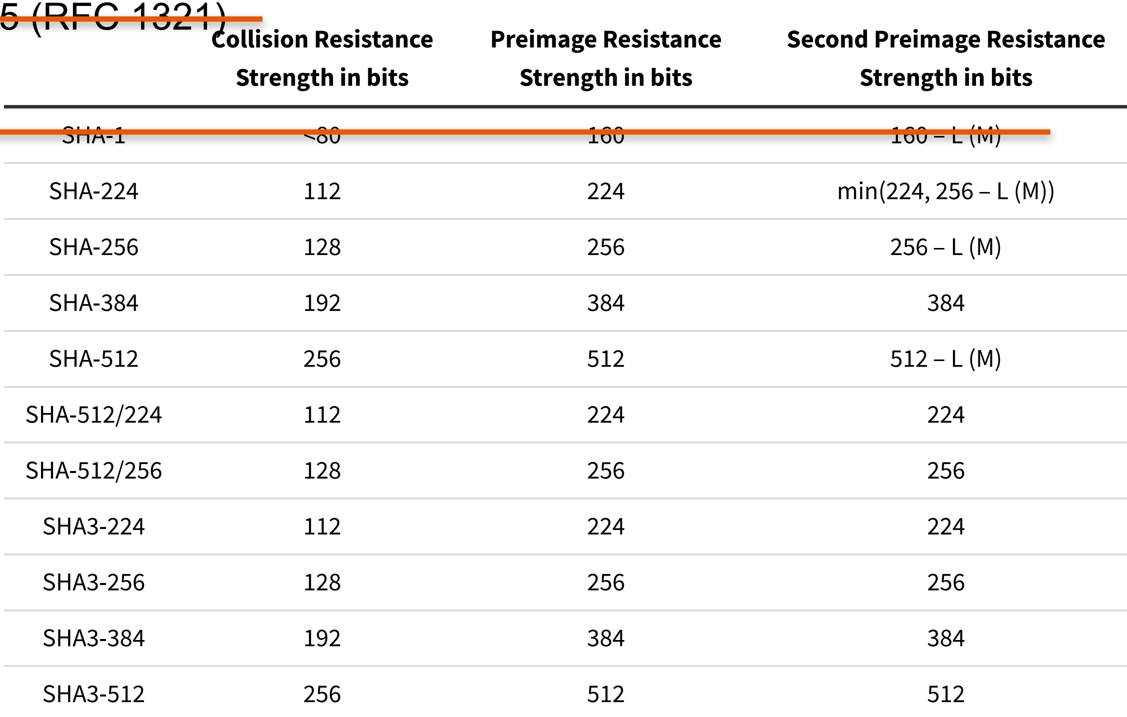
~~SHA-1~~

SHA-2 family of hash algorithms:

—SHA-224, SHA-256, SHA-384, SHA-512 SHA-512/224, and SHA-512/256

NIST Functions (FIPS 202)

SHA3-224, SHA3-256,
SHA3-384, SHA3-512



	Collision Resistance Strength in bits	Preimage Resistance Strength in bits	Second Preimage Resistance Strength in bits
~~SHA-1~~	~~<80~~	~~160~~	~~160 – L (M)~~
SHA-224	112	224	min(224, 256 – L (M))
SHA-256	128	256	256 – L (M)
SHA-384	192	384	384
SHA-512	256	512	512 – L (M)
SHA-512/224	112	224	224
SHA-512/256	128	256	256
SHA3-224	112	224	224
SHA3-256	128	256	256
SHA3-384	192	384	384
SHA3-512	256	512	512

https://csrc.nist.gov/projects/hash-functions

$L(M) \approx \log_2(n)$.

Integrity is the primary use of hash functions in digital forensics

$(\text{Evidence file})_{\text{hash}}$

1. Cryptographic hash functions assure that evidence is *unaltered after acquisition*

Hashing in digital forensics — we hash evidence files

`2GB-xfs-raw.E01`

Evidence & Metadata
MD5 & SHA1 hashes
No digital signature

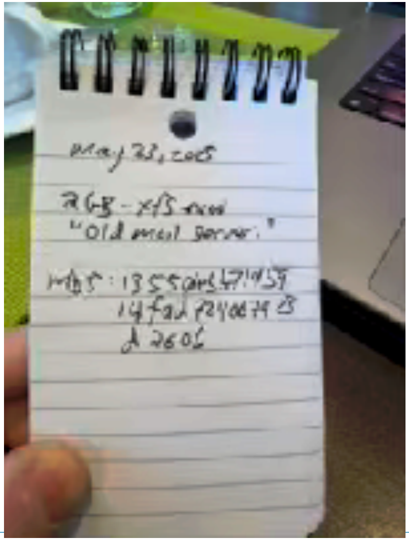
`2GB-xfs-raw.EX01`

AES encryption for data & metadata
SHA1 & SHA256 hashes
No digital signatures

Investigators record the MD5 hash value of the evidence in a notebook.

```
Media information
            Media type:                     fixed disk
            Is physical:                    yes
            Bytes per sector:               512
            Number of sectors:              4194304
            Media size:                     2.0 GiB (2147483648 bytes)

Digest hash information
            MD5:                            13350ebb7145914fad724007923d260b
```



May 23, 2005

2GB - XFS [illegible]
"Old mail server."

MD5: 13350ebb7145
914fad724007923
d260b

Disk imagers *could* digitally sign the disk image with a per-device key…

In practice, they don't.

Wait, digital forensics practitioners are still using MD5?

Yes — MD5 is used for authenticating forensic data

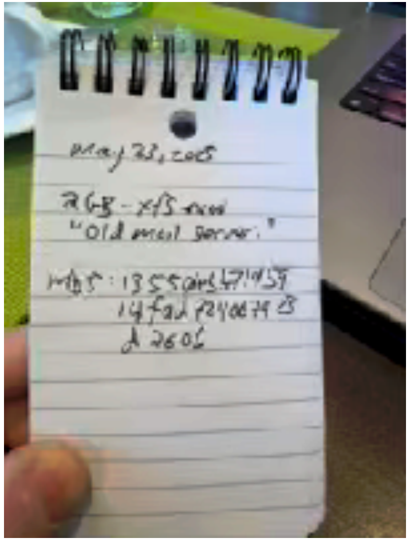
collision resistance — ❌

preimage resistance —~ ✓ (weakened)

It’s hard to find an input that produces a specific digest H1.

It’s hard to modify a disk image and get the same MD5.

If the hash value was recorded and the hash value hasn’t changed, it’s unlikely that the data have changed.



Digital Evidence Decryption

Encryption typically encountered by digital forensics examiners

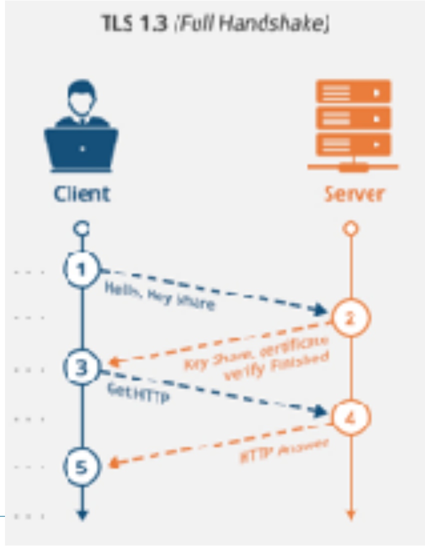
Device encryption (laptops, cell phones, servers)

End-to-end encrypted Cloud data

HTTPS encryption — TLS

Most of these are using *hybrid cryptographic protocols*.

- AES for data encryption
- RSA2048 or Elliptic curve with for Key Exchange Mechanism.
- Modern protocols like TLS 1.3 and WhatsApp use *perfect forward secrecy.*



In 2020, Apple transitioned from AES-128 to AES-256

AES-128 has a 128-bit key

340282366920938463463374607431768211456
possible keys

AES-256 has 256-bit key

1157920892373161954235709850086879078532699
84665640564039457584007913129639936
possible keys

Apple did this transition to protect from future quantum computers.

Devices like the “GrayKey” can

2. Occasionally, encrypted data are forcibly decrypted.

These devices try every password and PIN

A
a
aa
aal
aalii
aam
Aani
aardvark
aardwolf
Aaron
Aaronic
Aaronical
Aaronite
Aaronitic
Aaru
Ab
aba
Ababdeh
Ababua
abac
abaca
abacate

abacay
abacinate
abacination
abaciscus
abacist
aback
abactinal
abactinally
abaction
abactor
abaculus
abacus
Abadite
abaff
abaft
abaisance
abaiser
abaissed
abalienate
abalienation
abalone
Abama

abampere
abandon
abandonable
abandoned
abandonedly
abandonee
abandoner
abandonment
Abanic
Abantes
abaptiston
Abarambo
Abaris
abarthrosis
abarticular
abarticulation
abas
abase
abased
abasedly
abasedness
abasement

abaser
Abasgi
abash
abashed
abashedly
abashedness
abashless
abashlessly
abashment
abasia
abasic
abask
Abassin
abastardize
abatable
abate
abatement
abater
abatis
abatised
abaton
abator

abattoir
Abatua
abature
abave
abaxial
abaxile
abaze
abb
Abba
abbacomes
abbacy
Abbadide

abbot
abbotcy
abbotnullius
abbotship
abbreviate
abbreviately
abbreviation
abbreviator
abbreviatory
abbreviature
Abby
abcoulomb

They do not try to “crack” AES-128

2^{128} = 340282366920938463463374607431768211456 ~ 3.4E38

2^{128} ÷ 1 billion ÷ 1 billion = 340282366920938487808

A billion computers, each trying a billion keys every second

2^{128} ÷ 1 billion ÷ 1 billion ÷ (60*60*24*365) = 10,790,283,070,806 years!

That’s ~ 11 trillion years.

The earth is 4.5 billion years old. The universe is 13.8 billion years old.

AES-256 → 2^{256} possible keys = 1.1E77

With a trillion (1E12) computers trying a trillion keys!

We have transitioned to AES-256
But we are still using public key algorithms that are vulnerable

Public key cryptography uses today:

- Code Signing — Most Windows, MacOS, Android and iOS apps are now signed
- User and Machine Authentication — PKI, Server Certificates
- Network Security Protocols — TLS, VPN, SSH

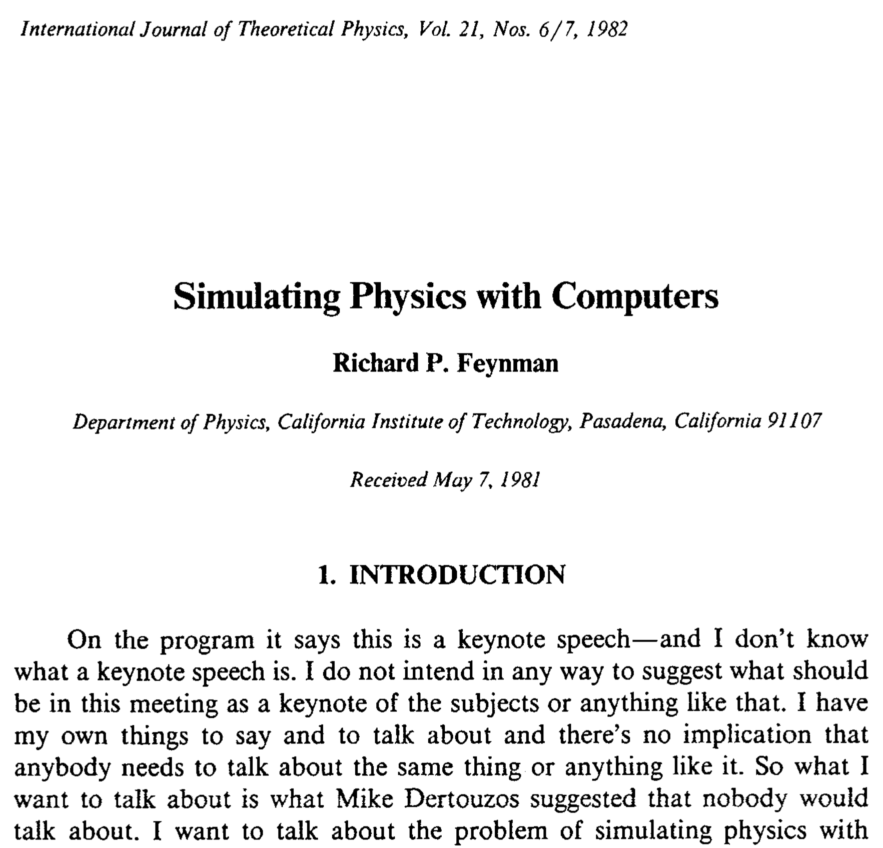
Widespread algorithms: RSA2048 and ED25519

A Cryptographically Relevant Quantum Computer

Not a CRQC →

IBM Quantum

1981 Richard Feynman proposed building a “quantum computer”



International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

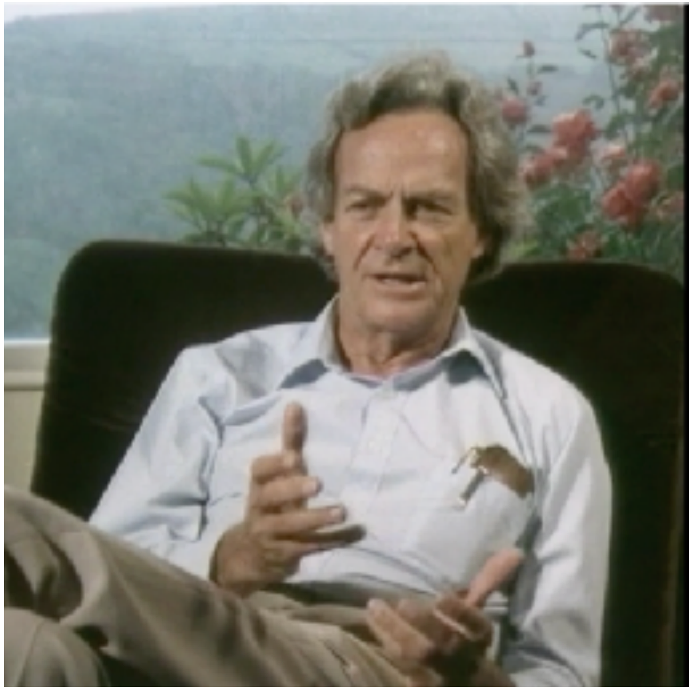
Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don’t know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there’s no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with



[FEYNMAN: THE PLEASURE OF FINDING THINGS OUT (1981)](https://vimeo.com/340695809)
https://vimeo.com/340695809

Feynman imaged using physical systems to simulate physical systems

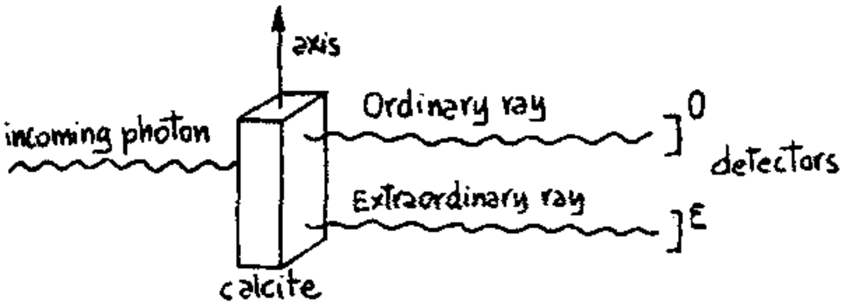


Fig. 2.

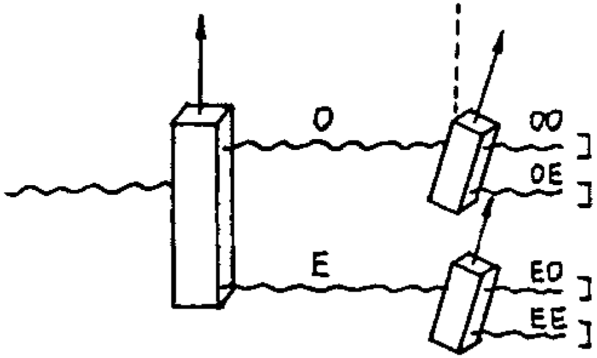


Fig. 3.

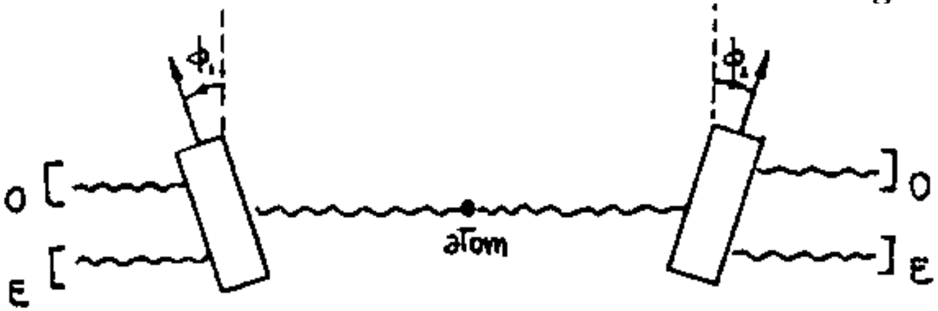


Fig. 4.

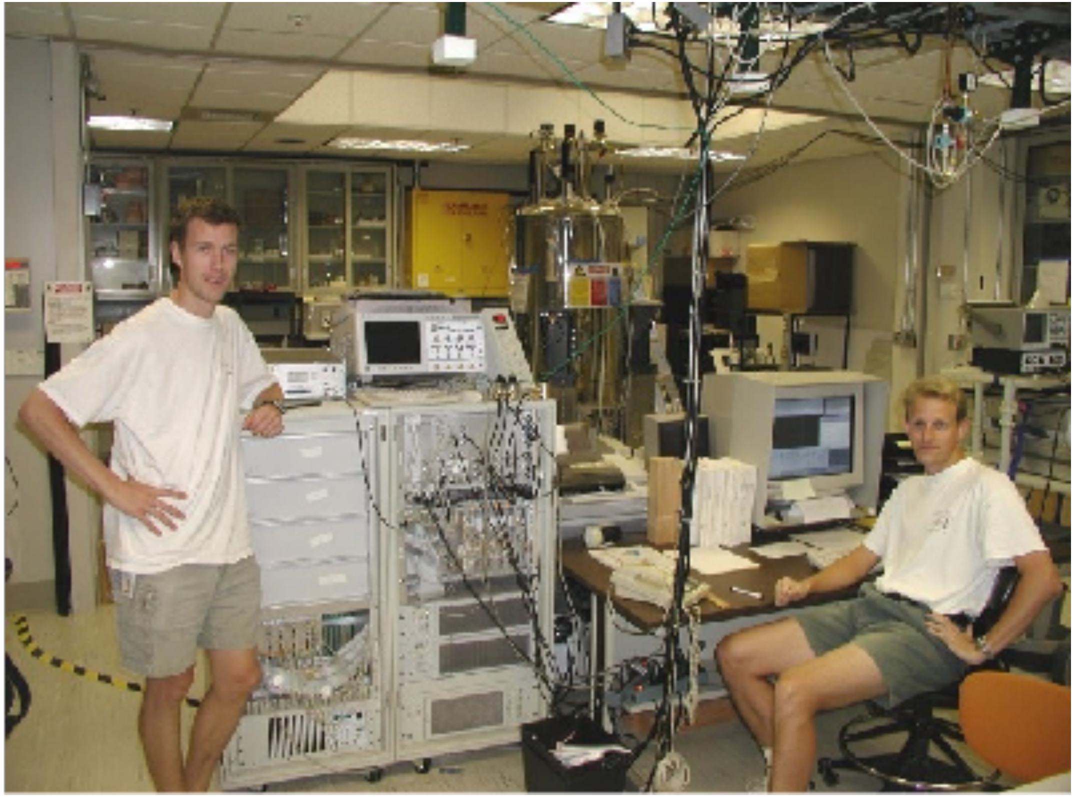
Growth of quantum computing

1994 - Peter Shor shows that quantum computers would be able to **factor integers and compute discrete logarithms in polynomial time**.

1996 - Lov Grover shows that a quantum computer can find an answer to a “black box” **search of n bits in** $O(\sqrt{2^n})$ **operations instead of** $O(2^n)$**.**

Factoring a RSA2048 number requires approx. 7000 qubits.

2001 — IBM researchers factor the number 15 with a quantum computer

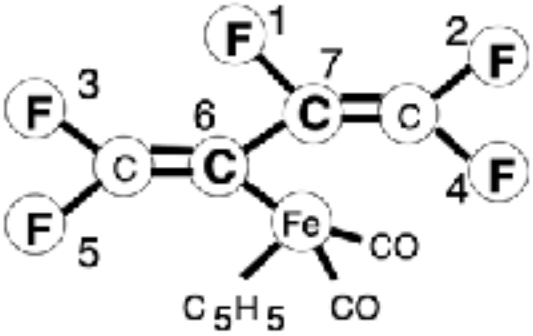


https://www.ibm.com/quantum/blog/factor-15-shors-algorithm

Great news!
IBM found that

$$15 = 3 \times 5$$

Quantum computers compute with qubits. IBM’s 2001 computer had 7 qubits.



IBM's "condor" computer claims 1,121 superconducting qubits

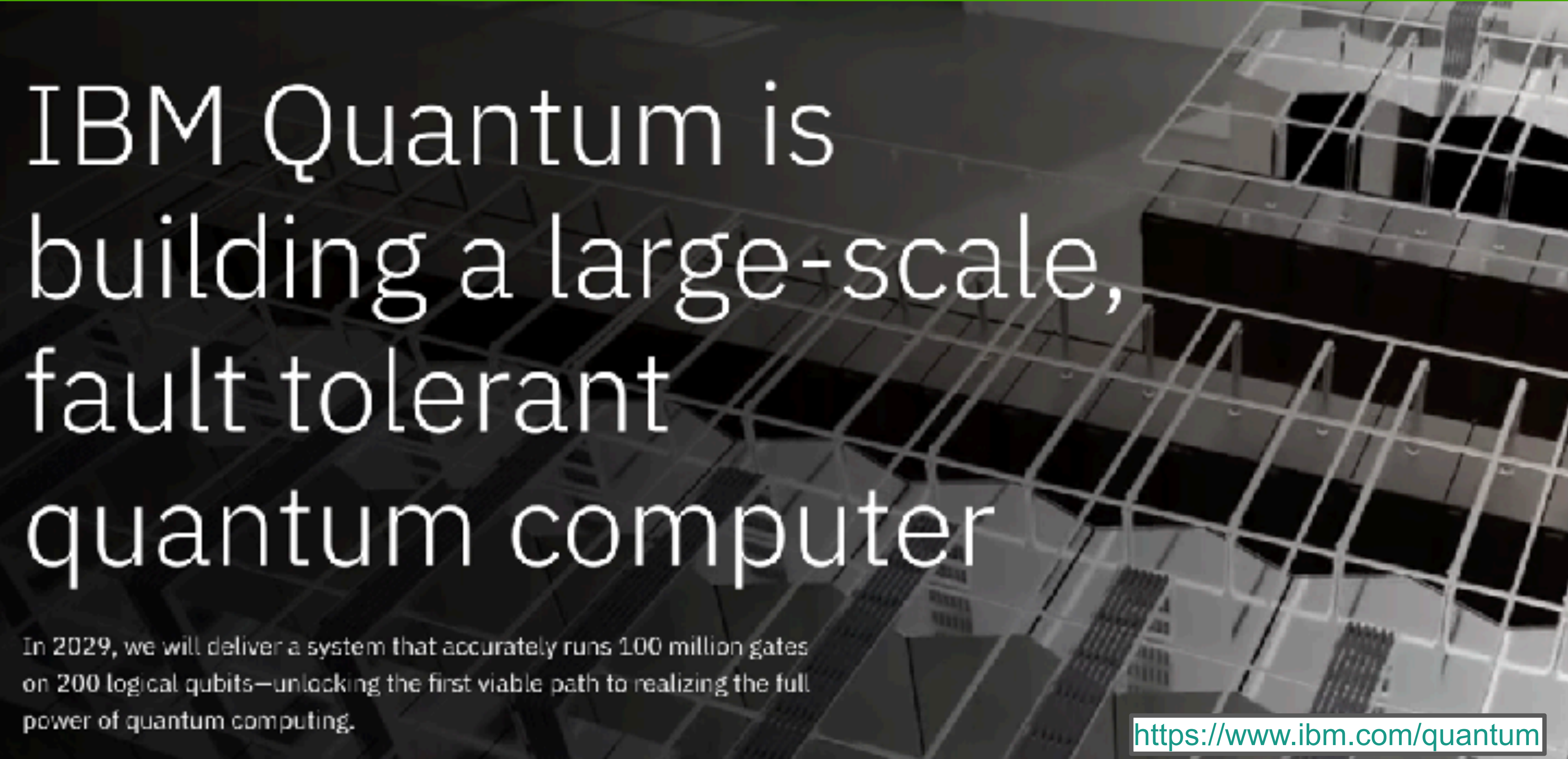
These are "noisy" qubits.

They need error correction.

~ 1-50 logical qubits

https://spectrum.ieee.org/ibm-condor

IBM promises 200 logical qubits to run 100 million "gates" by 2029.

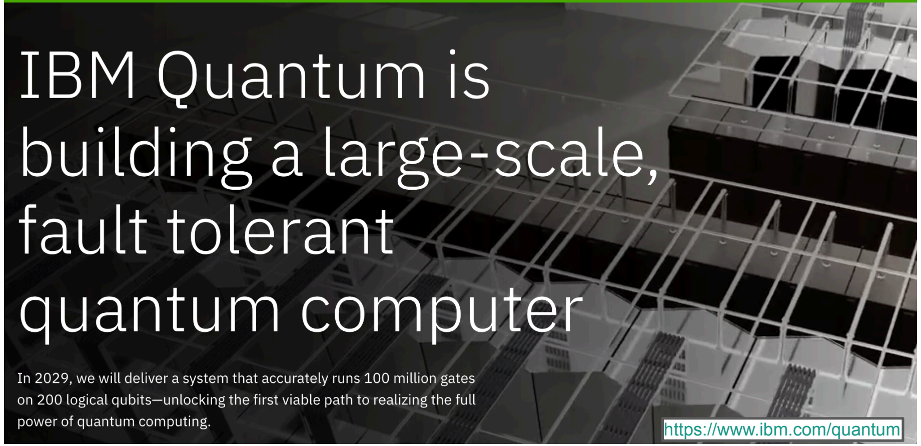


IBM Quantum is building a large-scale, fault tolerant quantum computer

In 2029, we will deliver a system that accurately runs 100 million gates on 200 logical qubits—unlocking the first viable path to realizing the full power of quantum computing.

https://www.ibm.com/quantum

IBM promises 200 logical qubits to run 100 million “gates” by 2029.



IBM Quantum is building a large-scale, fault tolerant quantum computer

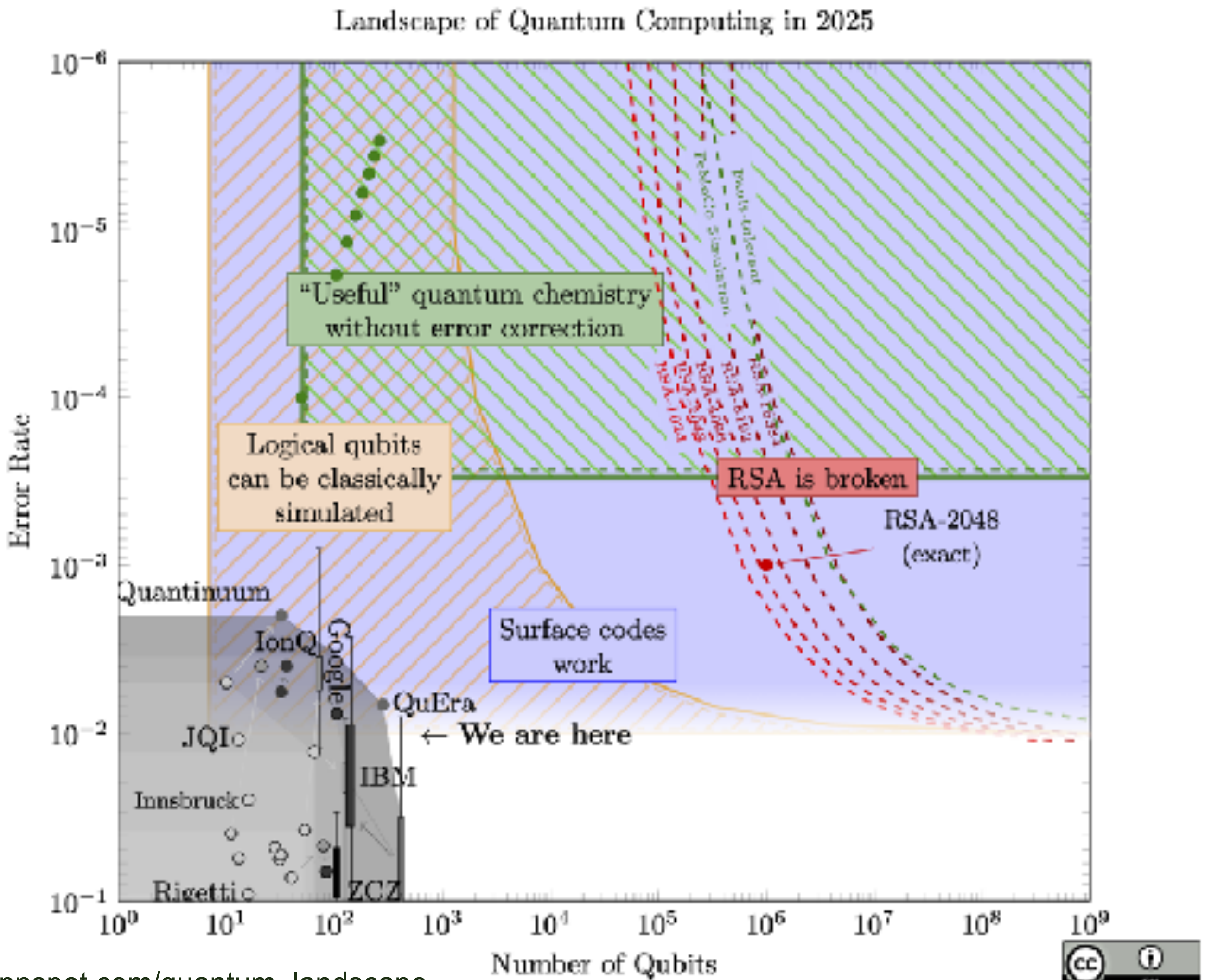
In 2029, we will deliver a system that accurately runs 100 million gates on 200 logical qubits—unlocking the first viable path to realizing the full power of quantum computing.

https://www.ibm.com/quantum

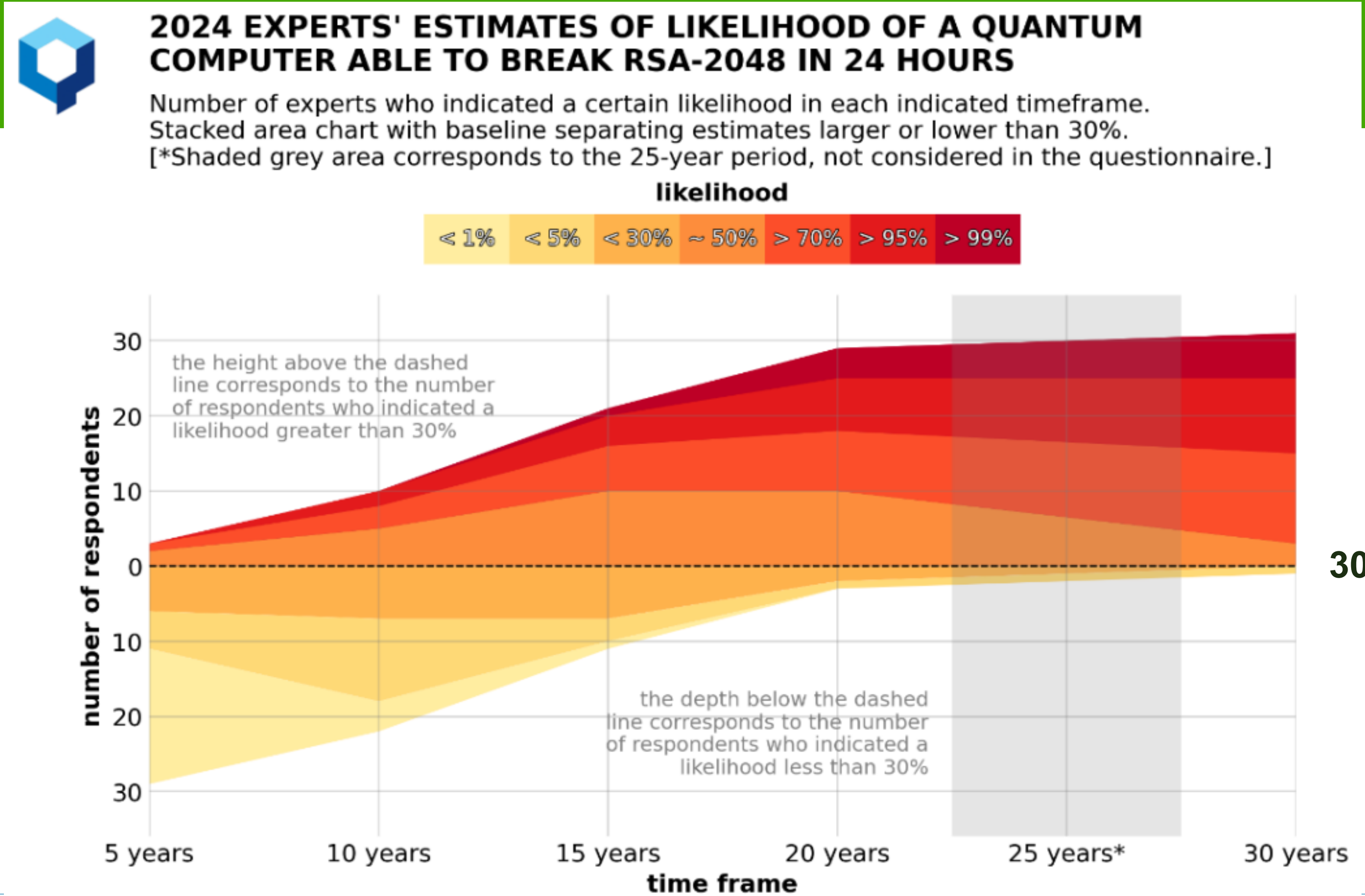
Not cryptographically relevant

(Need ~ 7000!)

2025



https://sam-jaques.appspot.com/quantum_landscape



2024 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

Number of experts who indicated a certain likelihood in each indicated timeframe.
Stacked area chart with baseline separating estimates larger or lower than 30%.
[*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]

30% likelihood

https://www.quintessencelabs.com/hubfs/PDFs/Global-Risk-Institute-Quantum-Threat-Timeline-Report-2024.pdf

Moving public key cryptography to quantum resistant algorithms (NIST IR 8747 ipd)

2016 — NIST starts post-quantum encryption project.

2016 - 2020 — NIST evaluated 23 signature and 59 KEM schemes.

2024 — NIST published three FIPS (Federal Information Processing Standards):

FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*	CRYSTALS-KYBER
FIPS 204, *Module-Lattice-Based Digital Signature Standard*	CRYSTALS-DILITHIUM
FIPS 205, *Stateless Hash-Based Digital Signature Standard*	eXtended Merkle Signature Scheme (XMSS)

2025 — NIST selected HQC as a fifth PQ algorithm

- https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline
- https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms

2030 — RSA, ECC and Diffie-Hellman deprecated
2031 — High-Priority Systems Migrated (US / Canada / EU)
2035 — Full transition completed

What would be in the impact on digital forensics?

Impact of a CRQC on Digital Forensics

Extraction — Could we get access to data that are currently denied?

- Could a CRQC decrypt evidence on seized devices?
- Could a CRQC forcibly access data in the cloud?

Authentication — Would a CRQC challenge the veracity of digital evidence?

- Impact of a CRQC on MD5, SHA1, SHA-256

Could a CRQC forcibly decrypt data on a seized device?

No.

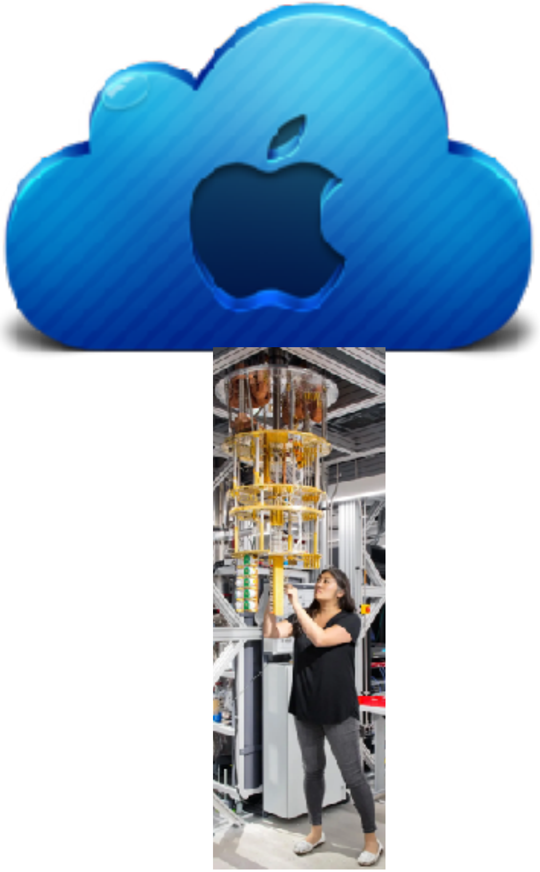
1) Today's devices are encrypted with AES-256.

2) A quantum computer won't brute-force PINs faster.

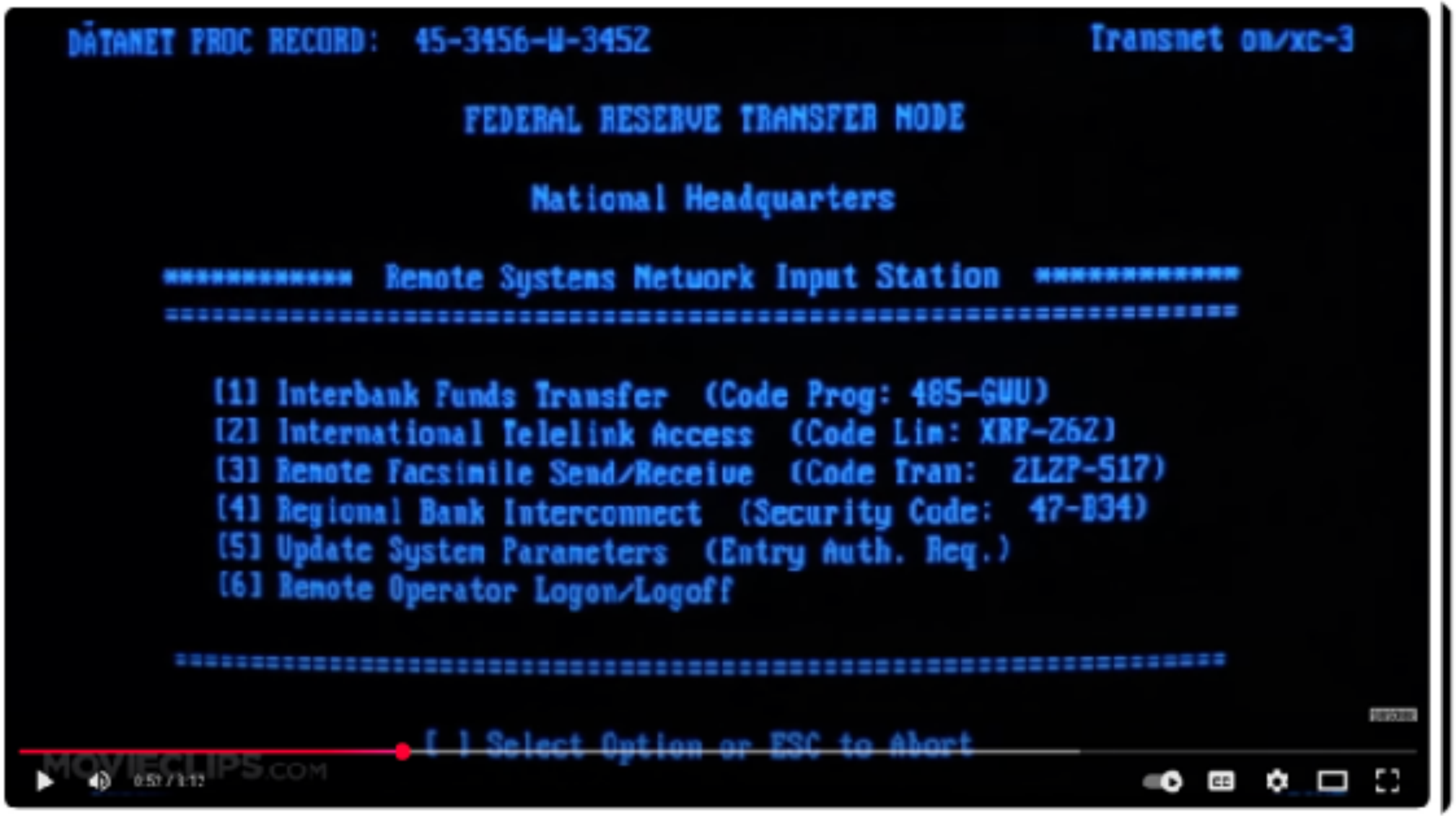
Some people who don't understand why we moved to AES-256 now argue that we should move to AES-512.

This is nonsense.

Could a CRQC forcibly access data in the cloud?



This is the plot of the movie Sneakers (1992)



```
DĂTANET PROC RECORD:  45-3456-W-3452                    Transnet on/xc-3

                   FEDERAL RESERVE TRANSFER NODE

                       National Headquarters

    *************  Remote Systems Network Input Station  *************
    ===================================================================

      [1] Interbank Funds Transfer  (Code Prog: 485-GWU)
      [2] International Telelink Access  (Code Lim: XRP-262)
      [3] Remote Facsimile Send/Receive  (Code Tran:  2LZP-517)
      [4] Regional Bank Interconnect  (Security Code:  47-B34)
      [5] Update System Parameters  (Entry Auth. Req.)
      [6] Remote Operator Logon/Logoff

     ==================================================================

                   [ ] Select Option or ESC to Abort
```

Sneakers (4/9) Movie CLIP - No More Secrets (1992) HD

Sneakers (1992) is fiction, but CRQC might not be

Could you break into someone's cloud account?

Not today…

Usernames & passwords protect most accounts.

Perhaps tomorrow…

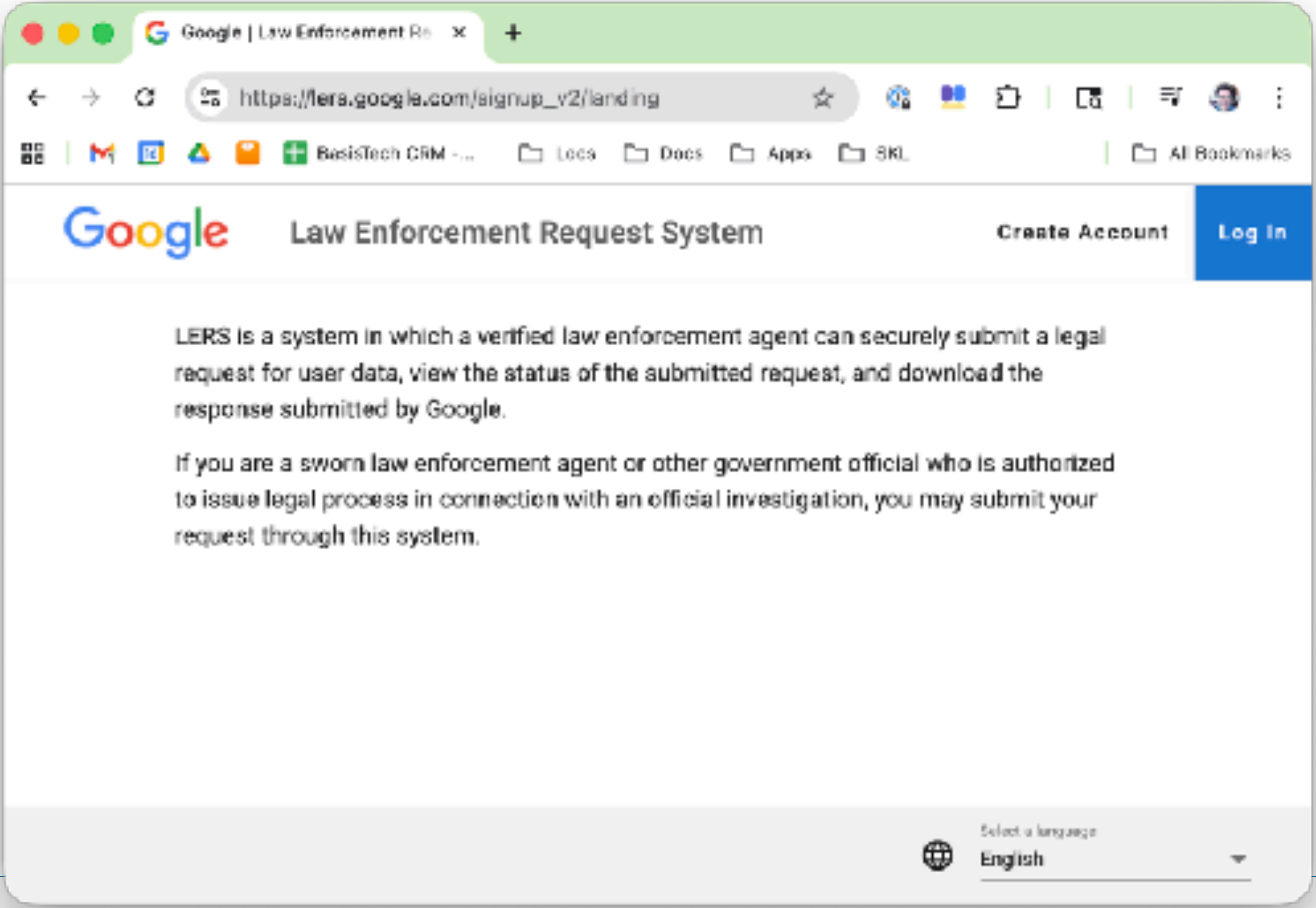
Passkey

Passkey uses WebAuthn which uses
RSA, ECDSA, EdDSA…

But it will easily be upgraded to post-quantum standards.

Quantum computers likely won't get us new evidence.

Today, law enforcement simply *asks* for data that's in the cloud.



Law Enforcement Request System

LERS is a system in which a verified law enforcement agent can securely submit a legal request for user data, view the status of the submitted request, and download the response submitted by Google.

If you are a sworn law enforcement agent or other government official who is authorized to issue legal process in connection with an official investigation, you may submit your request through this system.

How about wiretaps?

Yes, a CRQC could decrypt TLS 1.3

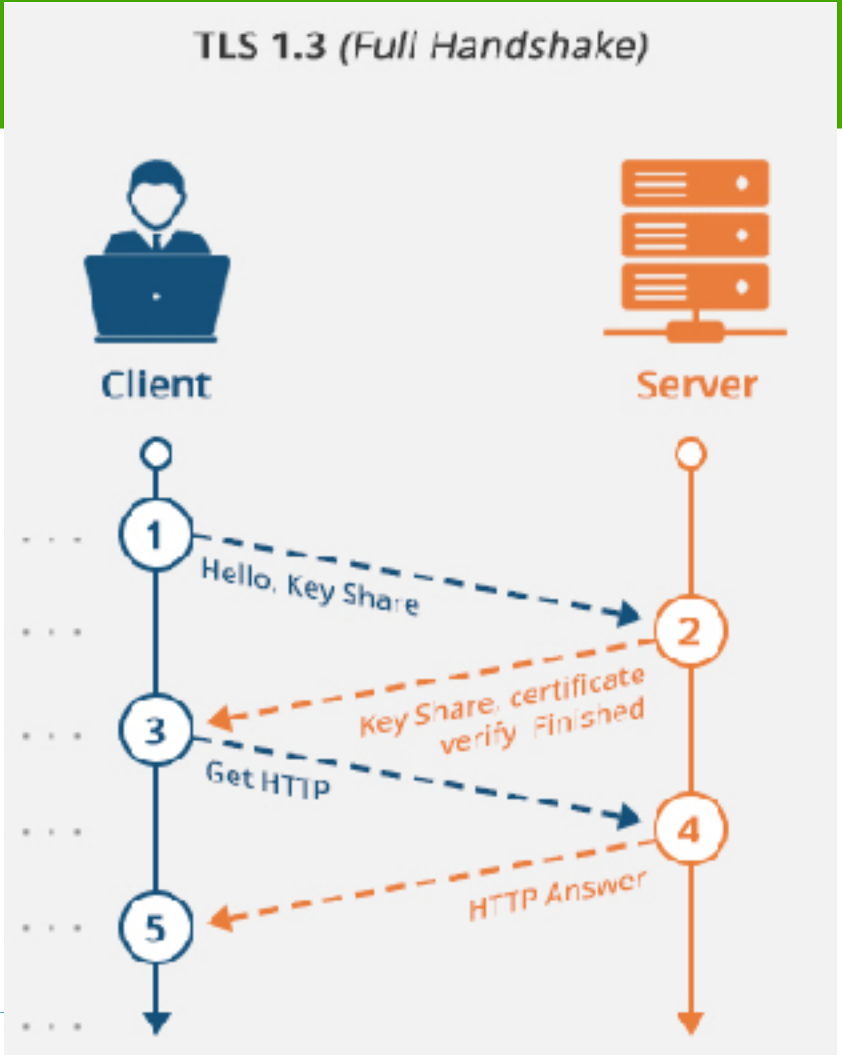
But, you would need to…

- Get a wiretap order TODAY
- Record the data
- Wait 15-30 years for a CRQC
- Convince the CRQC orders to decrypt your data.

“Capture now, decrypt later.”

What about 15-30 years from now?

- We will complete the PQ transition by 2030.

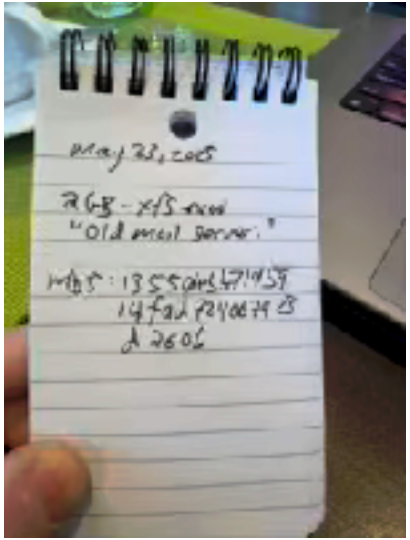


How about authentication of digital evidence?

Today “authentication” is based on MD5 (and sometimes SHA1), not on PKI.

Let’s pretend:

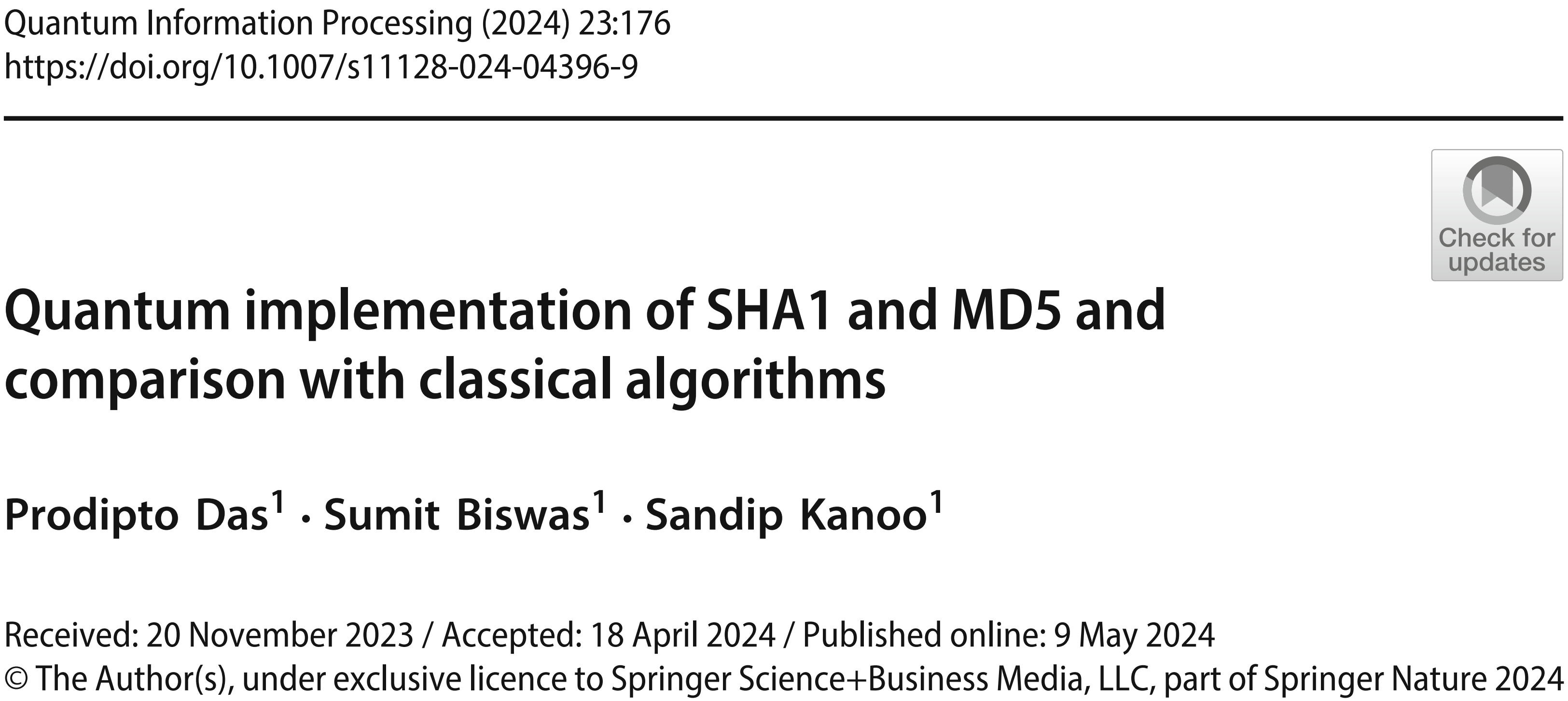
- We have a CRQC & quantum implementation of MD5
- Law enforcement is still using MD5
- MD5 is still has *pre-image resistance*



Question — is Grover’s algorithm a threat to MD5?

- Recall Grover’s algorithm changes MD5 work factor from $O(2^{128})$ to $O(\sqrt{2^{128}})$ = $O(2^{64})$

Several researchers have implemented MD5 and SHA1 for quantum computers.



Quantum Information Processing (2024) 23:176
https://doi.org/10.1007/s11128-024-04396-9

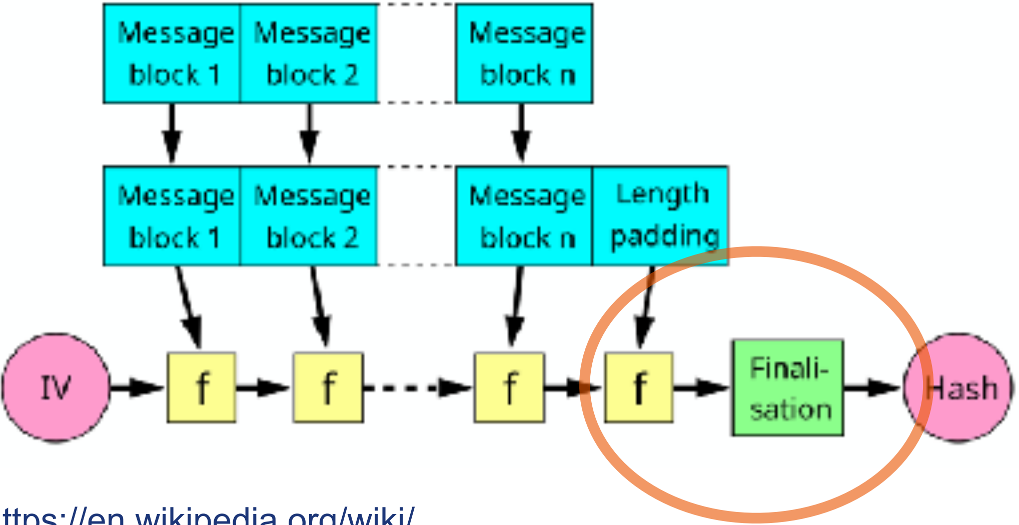
Quantum implementation of SHA1 and MD5 and comparison with classical algorithms

Prodipto Das[1] · Sumit Biswas[1] · Sandip Kanoo[1]

Received: 20 November 2023 / Accepted: 18 April 2024 / Published online: 9 May 2024

MD5 uses the Merkle–Damgård hash construction

It’s only necessary to attack the final computation.



https://en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction#

To estimate time to crack:

1. Compute how long it would take a CRQC compute a single MD5.
2. Multiply this time by 2^{64} (instead of 2^{128}).

A straightforward application of Grover won’t crack MD5

If the entire MD5 can be computed in 1 ms, it will take:

$$\frac{2^{64}}{1000 \times 60 \times 60 \times 24} = 213{,}503{,}982{,}334 \text{ days}$$

If we can compute MD5 in 1ns, it will take 213,503 days ~ 584 years

The fastest quantum cycle time for the foreseeable future is 1μs

→ 584 x 1000 = 584,000 years

Caveat

The fastest quantum cycle time for the foreseeable future is 1μs

→ 584 x 1000 = 584,000 years

This assumes:

No MD5 inversion (mathematical breakthrough)

No quantum implementation of MD5 inversion (algorithmic breakthrough)

Quantum computers do not scale to (billion devices on a chip) @ 1 nsec clock

If you have a billion devices that can crack a billion keys/sec, and run Grover on each, the time to crack MD5 would be:

$$\frac{\sqrt{2^{128}}}{10^9 \times 10^9} \approx 18\text{s}$$

The likely impact of quantum computing on the extraction and authentication of digital evidence

Evidence extraction

— probably no impact.

Evidence authentication

— possibly render MD5 technically unusable for evidence authentication.

— SHA-1 is unusable by policy since it has been deprecated by NIST

— MD5 is worse.

Important caveats

— absent a significant breakthrough in physics

— absent a significant breakthrough in algorithms

Email me: Simson Garfinkel, Chief Scientists, BasisTech, LLC: simsong@basistech.com

So what good are quantum computers?

Quantum chemistry

- Bulk materials
- Surface coatings
- Catalysts

Quantum biology

- New drugs

Quantum Physics

Email me: Simson Garfinkel, Chief Scientists, BasisTech, LLC: simsong@basistech.com