Quantum Computing
vs.
Your Privacy

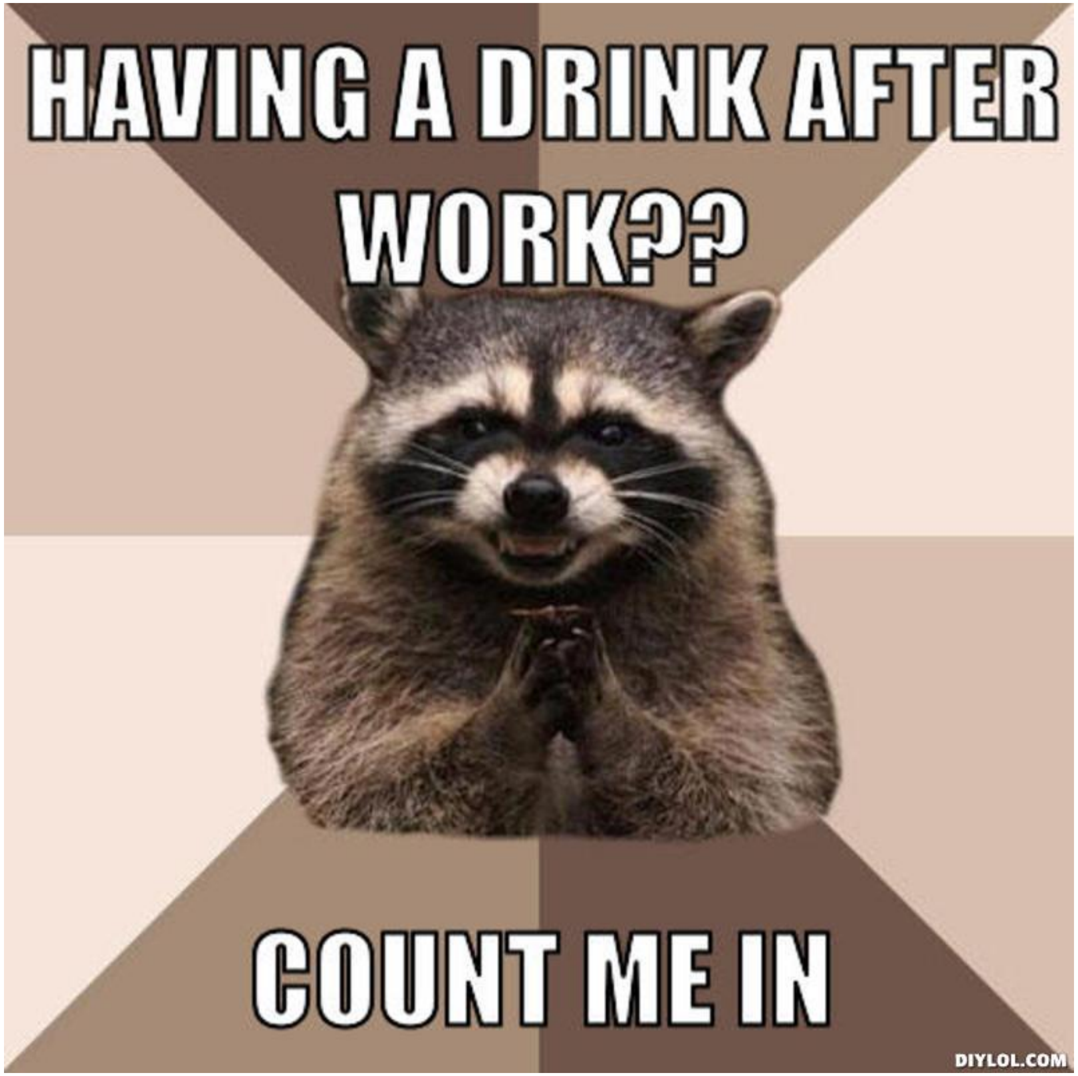
Andreas Hülsing

Privacy?

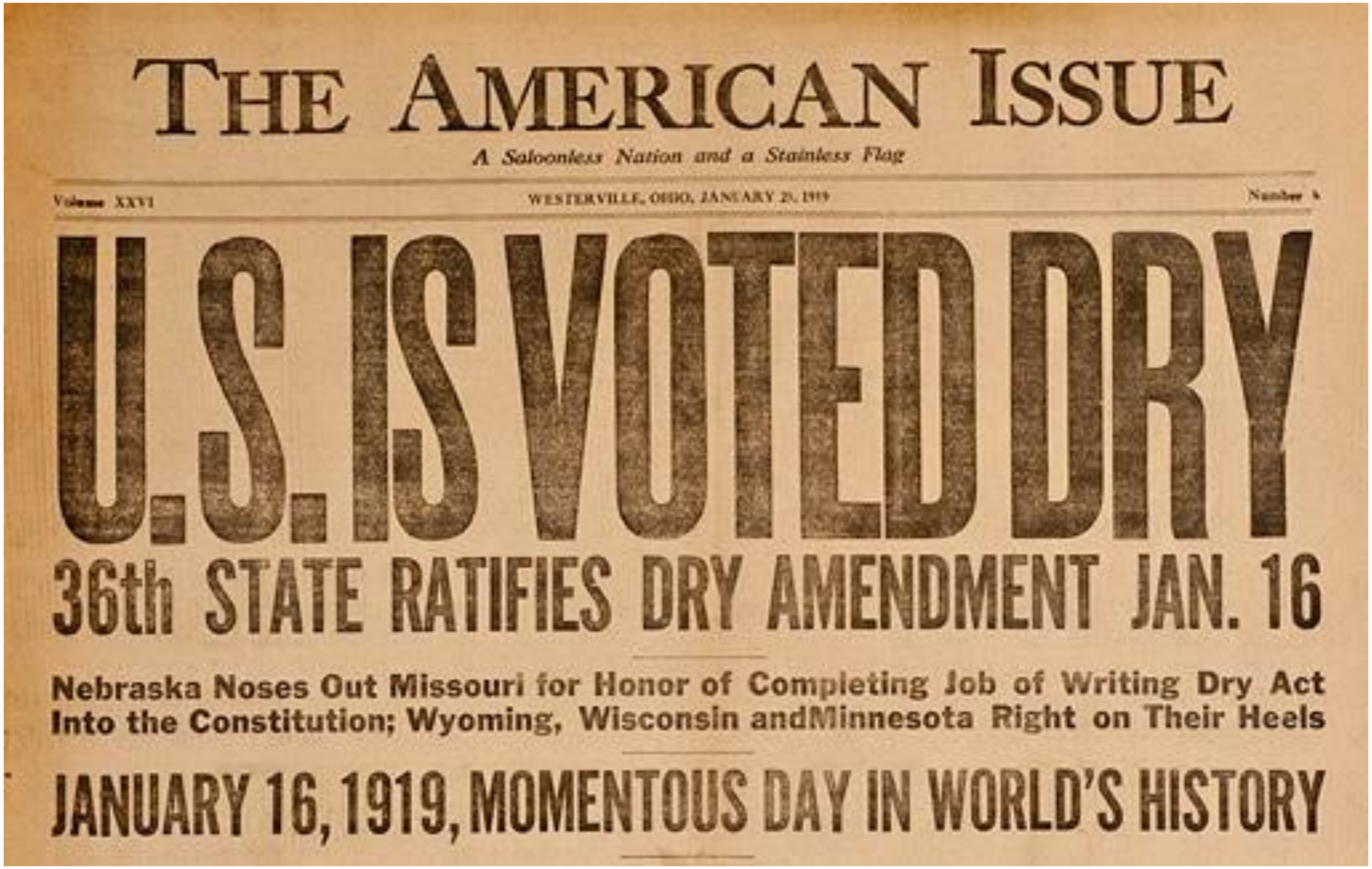
... the Panopticon must not be understood as a dream building: it is the diagram of a mechanism of power reduced to its ideal form.

Michel Foucault, *Discipline and Punish*, 1977

Too abstract?



Too abstract?



THE AMERICAN ISSUE

A Saloonless Nation and a Stainless Flag

Volume XXVI — WESTERVILLE, OHIO, JANUARY 25, 1919 — Number [illegible]

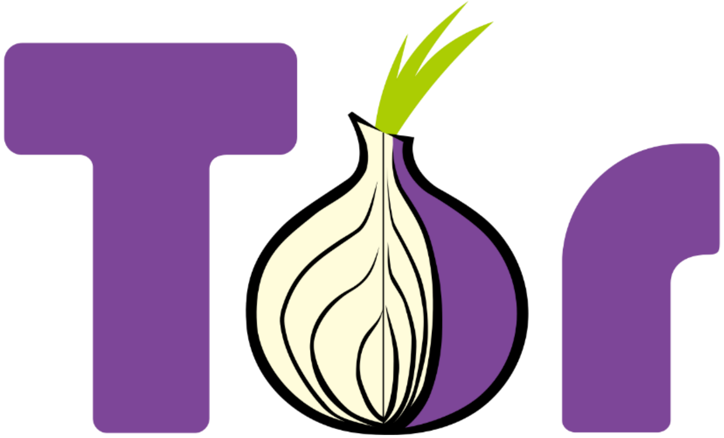
U.S. IS VOTED DRY

36th STATE RATIFIES DRY AMENDMENT JAN. 16

Nebraska Noses Out Missouri for Honor of Completing Job of Writing Dry Act Into the Constitution; Wyoming, Wisconsin andMinnesota Right on Their Heels

JANUARY 16, 1919, MOMENTOUS DAY IN WORLD'S HISTORY

How to achieve privacy?


Tor

DuckDuckGo

Under the hood…

Asymmetric Crypto

- ECC
- RSA
- DSA

Symmetric Crypto

- AES
- SHA2
- SHA1
- …

Combination of both needed!

We need symmetric and asymmetric crypto to achieve privacy!

Quantum Computing

Quantum Computing

“Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.”

-- Wikipedia

Qubits

- Qubit state: $\alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle$ with $\alpha_i \ \in \mathbb{C}$ such that $\alpha_0^2 + \alpha_1^2 = 1$
- Ket: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Qubit can be in state $\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

- Computing with 0 and 1 at the same time!

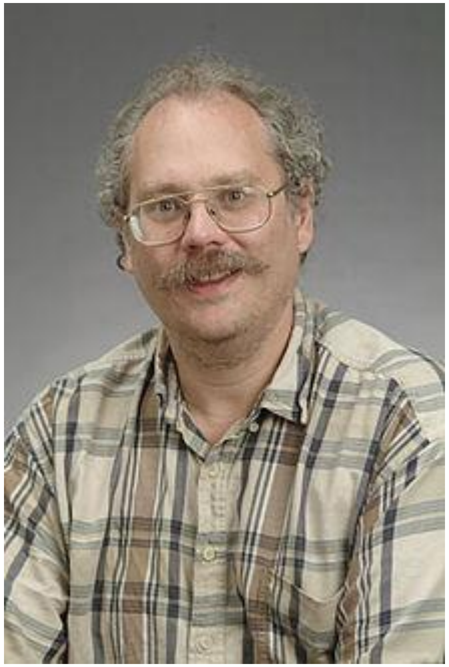
Quantum computers are not almighty

- To learn outcome one has to measure.
  - Collapses state
  - 1 qubit leads 1 classical bit of information
  - Randomized process
- Only invertible computation.
- Impossible to clone (copy) quantum state.

The Quantum Threat

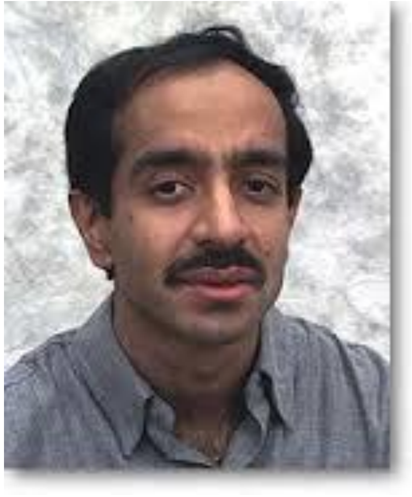
Shor‘s algorithm (1994)

- Quantum computers can do FFT very efficiently
- Can be used to find period of a function
- This can be exploited to factor efficiently (RSA)
- Shor also shows how to solve discrete log efficiently (DSA, DH, ECDSA, ECDH)



Grover‘s algorithm (1996)

- Quantum computers can search N entry DB in $\Theta(\sqrt{N})$
- Application to symmetric crypto
- Nice: Grover is provably optimal (For random function)
- Double security parameter.



To sum up

- All asymmetric crypto is broken by QC
  - No more digital signatures
  - No more public key encryption
  - No more key exchange

- Symmetric crypto survives
  (with doubled key size / output length)
  - NOT ENOUGH!

Why care today?

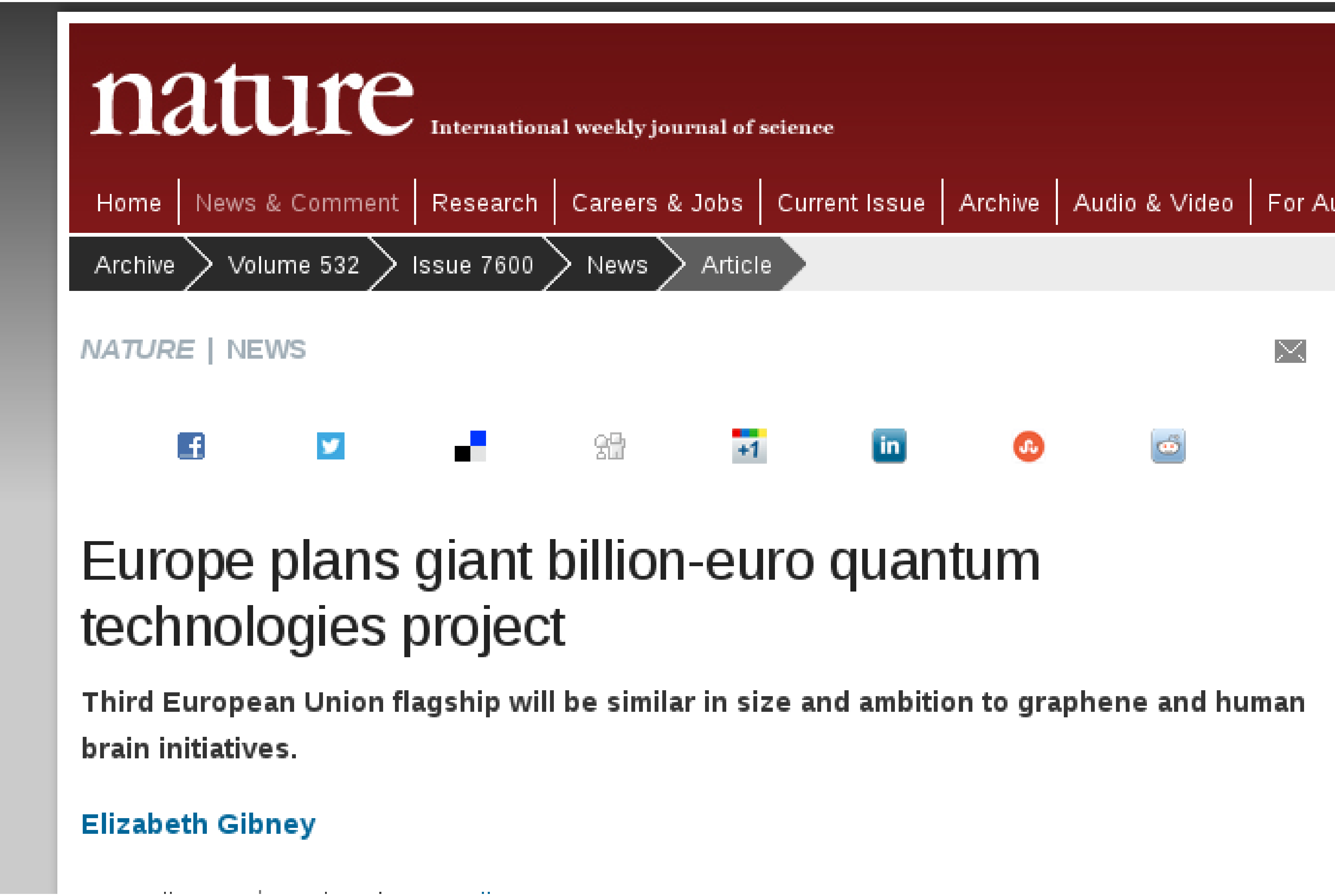
Quantum Computing

"Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data."

-- Wikipedia

Bad news

I will not tell you when a quantum computer will be built!



NATURE | NEWS

Europe plans giant billion-euro quantum technologies project

Third European Union flagship will be similar in size and ambition to graphene and human brain initiatives.

Elizabeth Gibney

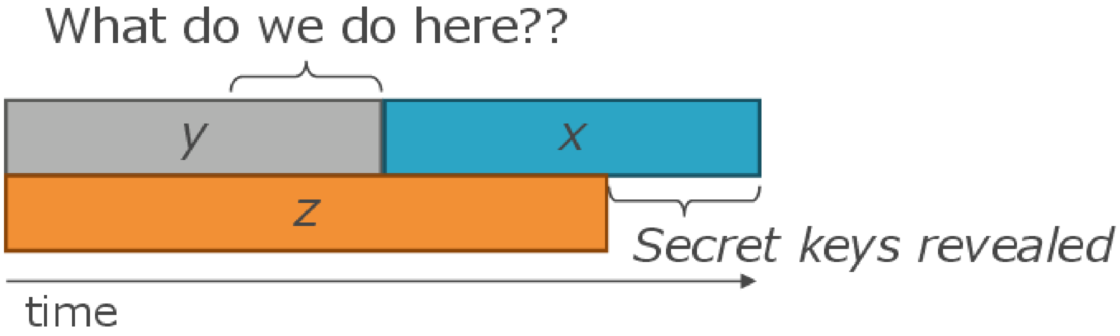
It‘s a question of risk assessment

How soon do we need to worry?

Depends on:

- How long do you need your keys to be secure? (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (*z* years)

Theorem 1: If $x + y > z$, then worry.



Who would store all encrypted data traffic? That must be expensive!

Defending Our Nation. Securing The Citizens.

PQCRYPTO to the rescue

PQCRYPTO
ICT-645622

PQCrypto

Initial recommendations

- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key

Evaluating: Serpent-256, . . .

- **Symmetric authentication** Informati retic MACs:
  - GCM using a 96-bit nonce an bit authenticator
  - Poly1305
- **Public-key encrypti** iece with binary Goppa codes:
  - length $n =$ nension $k = 5413$, $t = 119$ errors

Evaluatin DPC, Stehlé-Steinfeld NTRU, . . .

- **Pu signatures** Hash-based (minimal assumptions):
  - XMSS with any of the parameters specified in CFRG draft
  - SPHINCS-256

Evaluating: HFEv-, . . .

Confidence inspiring solutions are slow, too big, …

TODOs

- Increase confidence for other schemes: (Quantum) cryptanalysis

- Improve existing schemes

- Create code-base

Basis for standards, certification, ... , deployment

If you do not want to look like this... Work on PQCrypto

Thank you!
Questions?