

---

---

# RSA, Quantum Computing

8 May 2025  
Lecture 6

Some Slide Credits: Steve Zdancewic (UPenn)

# Topics for Today

---

- RSA Algorithm
  - Homomorphic Property
- Quantum and Post-Quantum Cryptography
- Sources:
  - HAC 8.2, 10.1-10.3
  - NIST SP 800-38D

# Homomorphic Property

- RSA is exponentiation, so preserves mathematical properties

Public key  $n=3337$ ,  $e=79$

Private key  $n=3337$ ,  $d=1019$

Message1: 75 (K)

Message2: 39 (')

Message1: Encrypted  
 $75^{79} \bmod 3337 = 2213$

Message2 Encrypted  
 $39^{79} \bmod 3337 = 2739$

$$2213 \times 2739 \bmod 3337 = 1415$$

Message1×Message2:  $75 \times 39 = 2925$

Message1×Message2 Encrypted:  
 $2925^{79} \bmod 3337 = 1415$

# Homomorphic Property (!)

---

- In short:  $(m_1 \times m_2)^e \equiv m_1^e \times m_2^e \equiv c_1 \times c_2 \pmod{n}$
- Means that messages are not totally random!

Solutions:

## Fixed message formats

- Will get ruined by multiplication

## Padding algorithms (PKCS1 and OAEP)

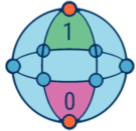



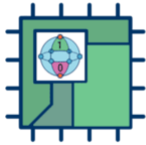
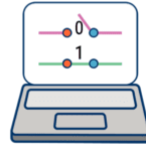


- Helps also with IND-CPA

# So Far

---

- RSA Algorithm
  - Homomorphic Property
- Quantum and Post-Quantum Cryptography

# Quantum Problems?

Quantum Computing	Vs.	Classical Computing
 <p>Calculates with qubits, which can represent 0 and 1 at the same time</p>		 <p>Calculates with transistors, which can represent either 0 or 1</p>
 <p>Power increases exponentially in proportion to the number of qubits</p>		 <p>Power increases in a 1:1 relationship with the number of transistors</p>
 <p>Quantum computers have high error rates and need to be kept ultracold</p>		 <p>Classical computers have low error rates and can operate at room temp</p>
 <p>Well suited for tasks like optimization problems, data analysis, and simulations</p>		 <p>Most everyday processing is best handled by classical computers</p>

<https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/>

CBINSIGHTS

# Quantum Algorithms

---

## Shor's Algorithm

- Attacks RSA and Elliptical Curve
- Theory - Billions of operations on thousands of qubits
- Fault tolerant – trillions of operations on millions of qubits

## Grover's Algorithm

- Search unordered database quickly
- Reduces  $N$  to  $\sqrt{N}$  in runtime

# RSA and Quantum Computers

---

RSA security is based on how long it takes to factor very large numbers

Shor's algorithm for quantum computers can factor numbers very fast

- 2021 paper showed how to factor 2048 RSA key in 8 hours
- Need ~20M qubits
- Max qubit size today is 70

How long until quantum computers reach millions of qubits?

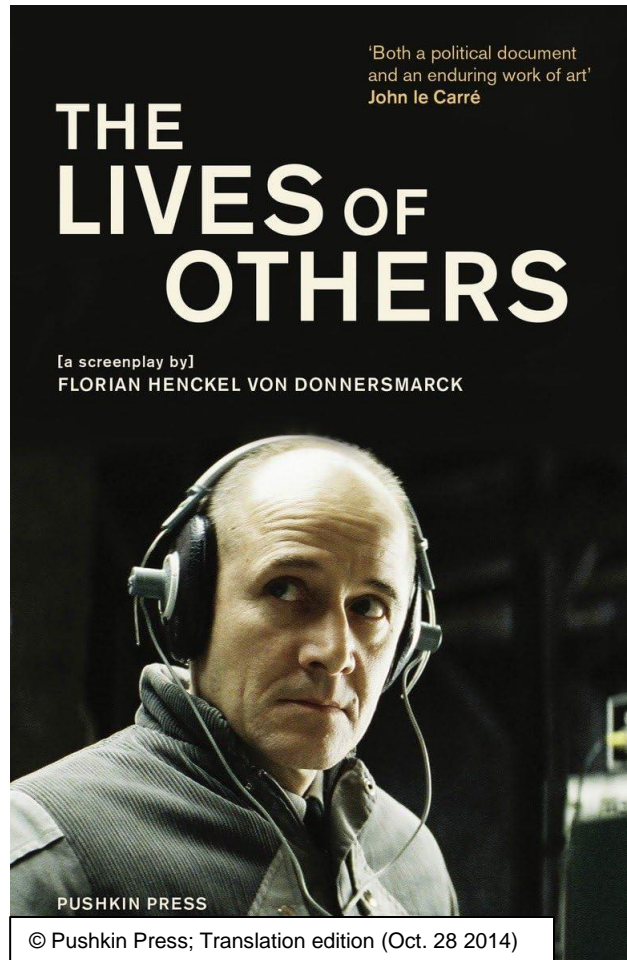
- 5 years?
- 20 years?
- 25 years?

Research and governments working on post-quantum algorithms today

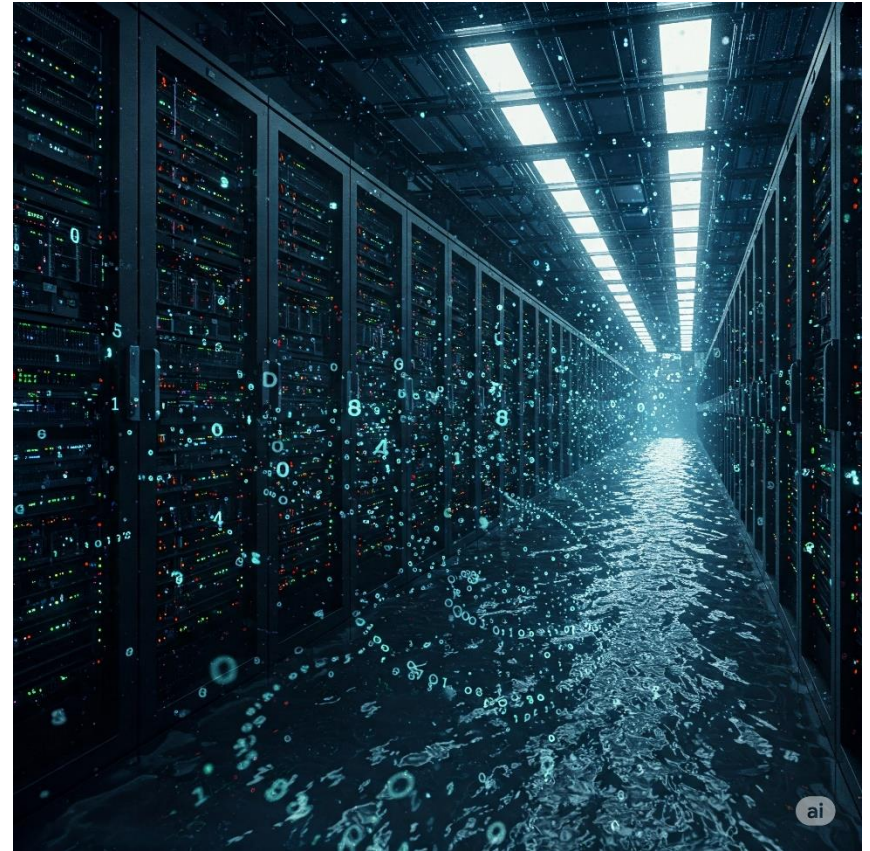


# Record Now Decrypt Later

Today



When a Quantum Computer Arrives



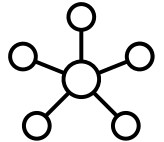
# Post Quantum Crypto

## Code based encryption

- Error correcting algorithms
- Intentionally introduce errors
- Keys are big – 1MB

## Lattices

- Encryption - 8KB public keys
- Signatures too



## Multivariate quadratic equation signatures

- Small signatures, very complicated
- $a_i + \sum_j b_{i,j}x_j + \sum_{j<k} c_{i,j,k}x_jx_k$
- $a_i, b_{i,j}, c_{i,j,k} \in \mathbf{F}_2$

## Hash based signatures

- One time signatures
- Can organize as Merkle Tree for efficiency

# Standardizing Post-Quantum

---

2016

- NIST issues call for proposals for Quantum Safe Crypto
- 8 Classes of Algorithms
- 82 Algorithms submitted

2019 Round 2

- 6 Classes
- 26 Algorithms

2020-1 Round 3

- 3 Classes
- 7 finalists
- 8 Alternatives

# 2024 PQC First Round Standards

---

## Public/Private Keys

- Lattice Based and Learning with Errors – CRYSTALS-Kyber

## Digital Signatures

- Lattice Based – CRYSTALS-Dilithium, FALCON
- Hash based – SPHINCS+

# In the Pipeline

---

## Backup Public/Private

- Code-based HQC
- In case CRYSTALS-Kyber has problems

## Additional Digital Signature

Type	Signature
Lattice	HAWK
Code-Based	CROSS LESS
MPC in the Head	Mirath MQOM PERK RYDE SDitH
Multivariate	MAYO QR-UOV SNOVA UOV
Supersingular Elliptic Curve Isogeny	SQIsign
Symmetric based	FAEST

# Conclusion

---

- RSA Algorithm
  - Homomorphic Property
- Quantum and Post-Quantum Cryptography