Post-quantum-secure public-key encryption from the Learning With Errors problem

Course 01410, Crypto I

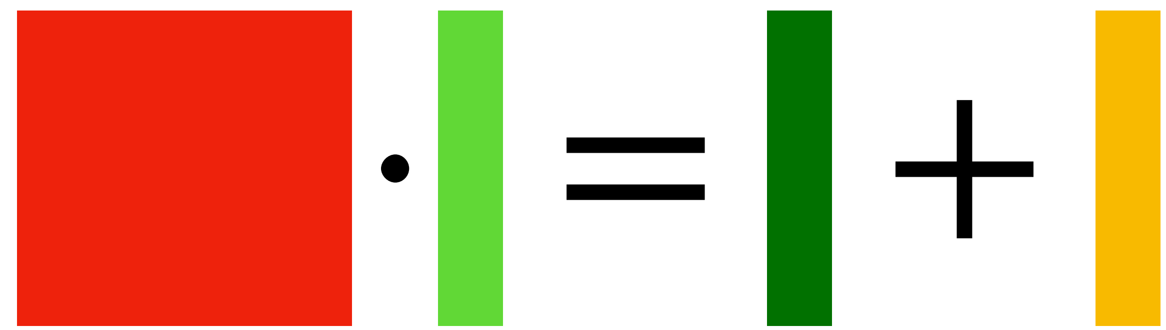
Christian Majenz

Associate Professor, Cybersecurity Engineering Section, DTU Compute

Plan for today

NIST

Part I



Part II

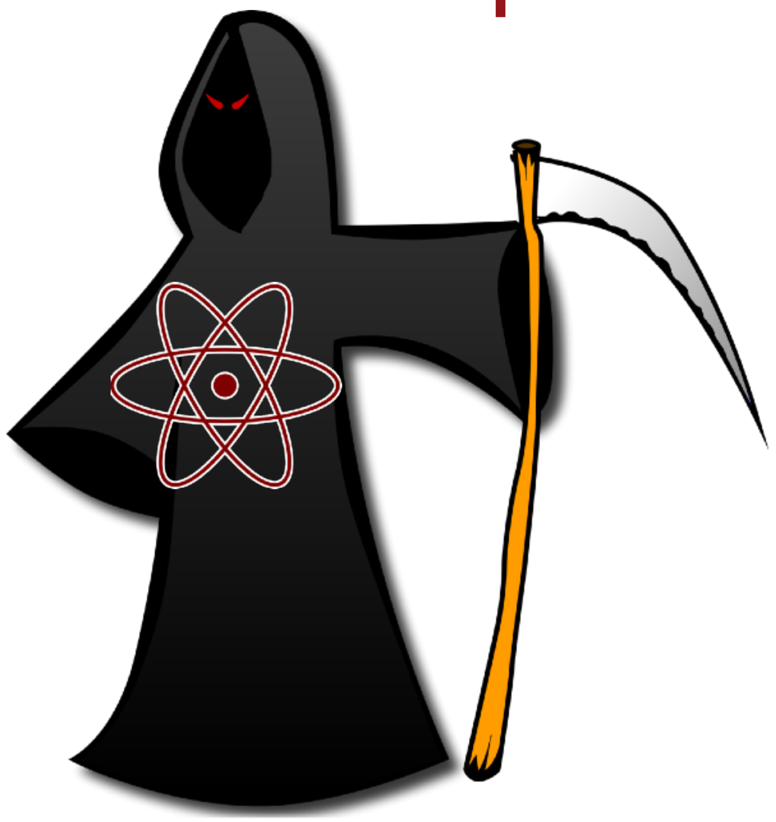
Part III

Post-quantum public-key cryptography and the NIST competition

Plenty of alternative hard problems

RSA

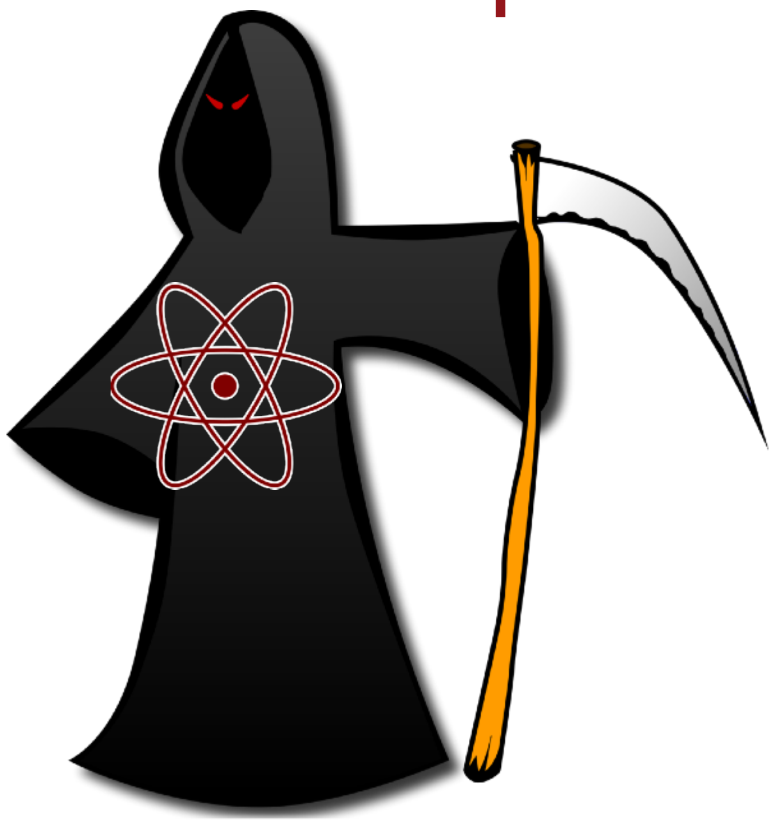
DH



Plenty of alternative hard problems

RSA

DH

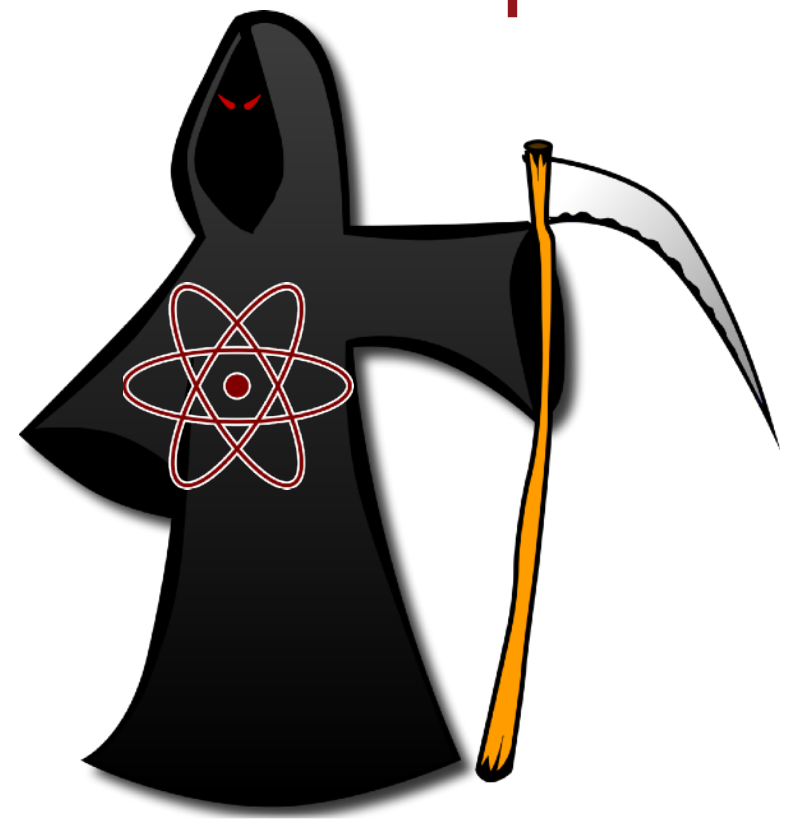


Luckily, public-key encryption and key exchange can also be constructed based on the hardness of

Plenty of alternative hard problems

RSA

DH



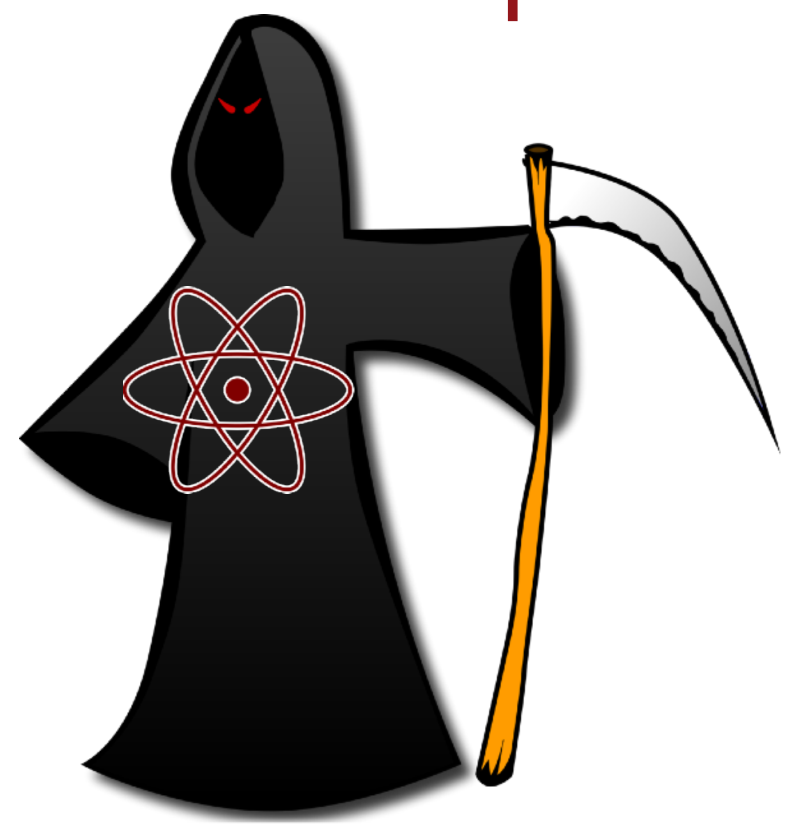
Luckily, public-key encryption and key exchange can also be constructed based on the hardness of

- Lattice problems

Plenty of alternative hard problems

RSA

DH



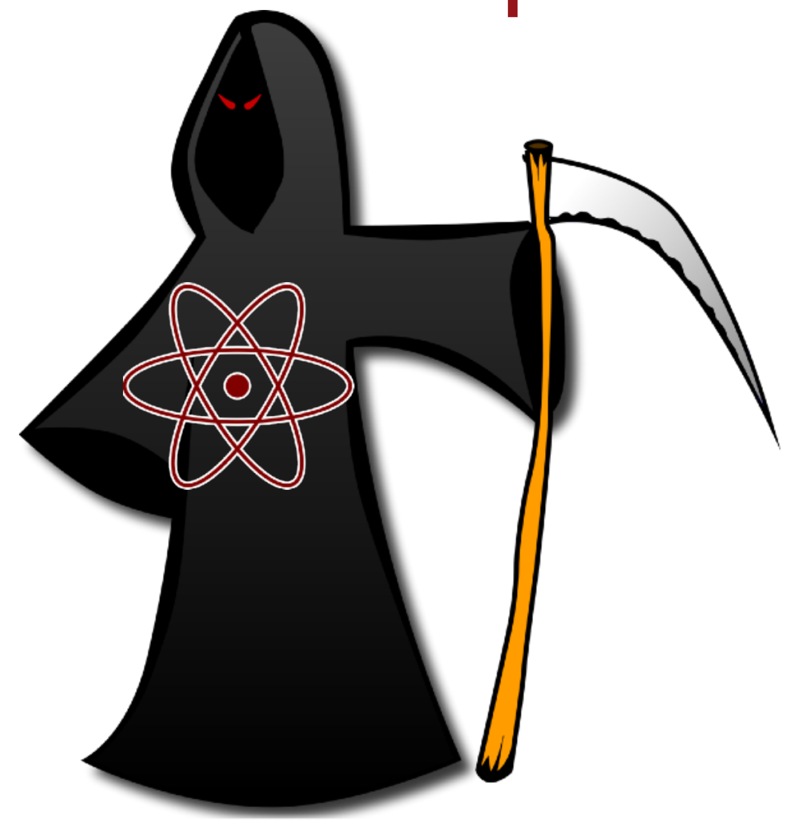
Luckily, public-key encryption and key exchange can also be constructed based on the hardness of

- Lattice problems
- Solving systems of multivariate polynomial equations

Plenty of alternative hard problems

RSA

DH



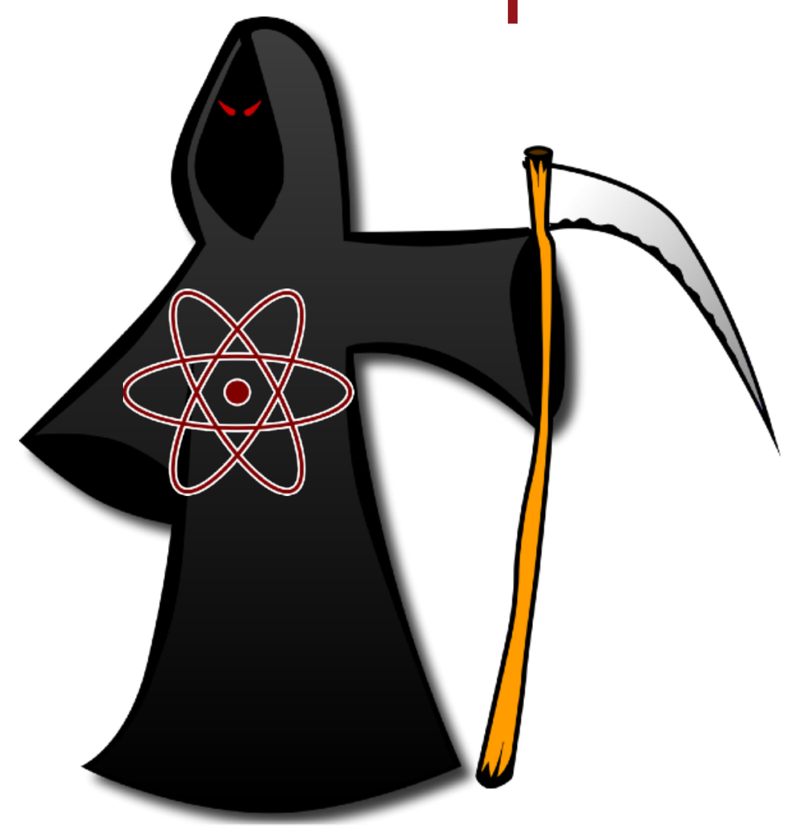
Luckily, public-key encryption and key exchange can also be constructed based on the hardness of

- Lattice problems
- Solving systems of multivariate polynomial equations
- Decoding “obfuscated” error correction codes

Plenty of alternative hard problems

RSA

DH



Luckily, public-key encryption and key exchange can also be constructed based on the hardness of

- Lattice problems
- Solving systems of multivariate polynomial equations
- Decoding “obfuscated” error correction codes
- Finding an isogeny between supersingular elliptic curvers

Post-quantum cryptography

$\Rightarrow$We have

- Lattice-based
- Multivariate-polynomial-based
- Code-based
- Isogeny-based

Public-key encryption/key exchange

Digital signatures are "easier"! Additionally

- Hash-based signatures
- MPC-in-the-head signatures

NIST post-quantum crypto standardization

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)
- Initially: All classes represented

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)
- Initially: All classes represented
- To be standardized:

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)
- Initially: All classes represented
- To be standardized:
  - 1 Lattice KEM: Crystals-Kyber

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)
- Initially: All classes represented
- To be standardized:
  - 1 Lattice KEM: Crystals-Kyber
  - 3 DSS: 2 based on lattices: Crystals-Dilithium&Falcon, 1 hash-based: SPHICS+

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)
- Initially: All classes represented
- To be standardized:
  - 1 Lattice KEM: Crystals-Kyber
  - 3 DSS: 2 based on lattices: Crystals-Dilithium&Falcon, 1 hash-based: SPHICS+
- 4th round: New call for signature proposals, 3 code-based KEMs under consideration

NIST post-quantum crypto standardization

- Goal: Standardize at least one PQ-secure scheme of each:
  - Key Encapsulation Mechanism (KEM, ~public-key encryption)
  - Digital Signature scheme (DSS)
- Initially: All classes represented
- To be standardized:
  - **1 Lattice KEM: Crystals-Kyber**
  - 3 DSS: 2 based on lattices: Crystals-Dilithium&Falcon, 1 hash-based: SPHICS+
- 4th round: New call for signature proposals, 3 code-based KEMs under consideration

Remainder of today’s lecture:

- The Learning With Errors (LWE) problem
- The Regev encryption scheme
- Short outlook: What’s missing to get to Kyber?

Part II: The Lerning With Errors problem (LWE)

Warm-up: Gaussian elimination

- Exercise: Solve the following linear system over $\mathbb{Z}_{23}$ using Gaussian elimination:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 13 \\ 20 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \\ 1 \end{pmatrix} \mod 23$$

Hint: $21^{-1} = 11 \mod 23$

A slightly harder problem

- Exercise: Solve the following "noisy" linear system over $\mathbb{Z}_{23}$ using Gaussian elimination:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 9 \\ 10 \end{pmatrix} = \begin{pmatrix} 6 \\ 19 \\ 13 \end{pmatrix} + \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \end{pmatrix} \mod 23$$

Promise: $\epsilon_i \in \{-1,0,1\}$ for $i = 1,2,3$

Hint: $21^{-1} = 11 \mod 23$

A slightly harder problem

- E[illegible]cise: Solve the following "noisy" linear system over $\mathbb{Z}_{23}$ using [illegible]limination:

$$\begin{pmatrix} 1 & [illegible] \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} [illegible] \\ 10 \end{pmatrix} = \begin{pmatrix} 6 \\ [illegible] \\ [illegible] \end{pmatrix} + \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ [illegible] \end{pmatrix} \mod 23$$

Essentially the LWE problem!

Promise: $\epsilon_i \in \{-1,0,1\}$ for $i =$ [illegible]

Hint: $21^{-1} = 11 \mod 23$

Part III: Regev encryption