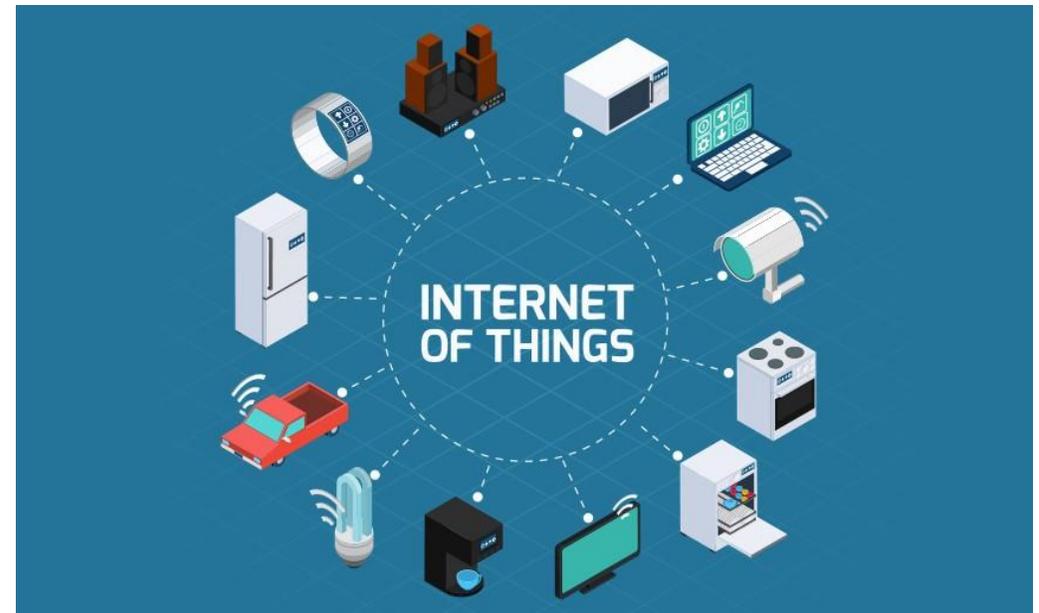


Post-Quantum Cryptography

Feng-Hao Liu
feng-hao.liu@wsu.edu
Associate Professor
Washington State University

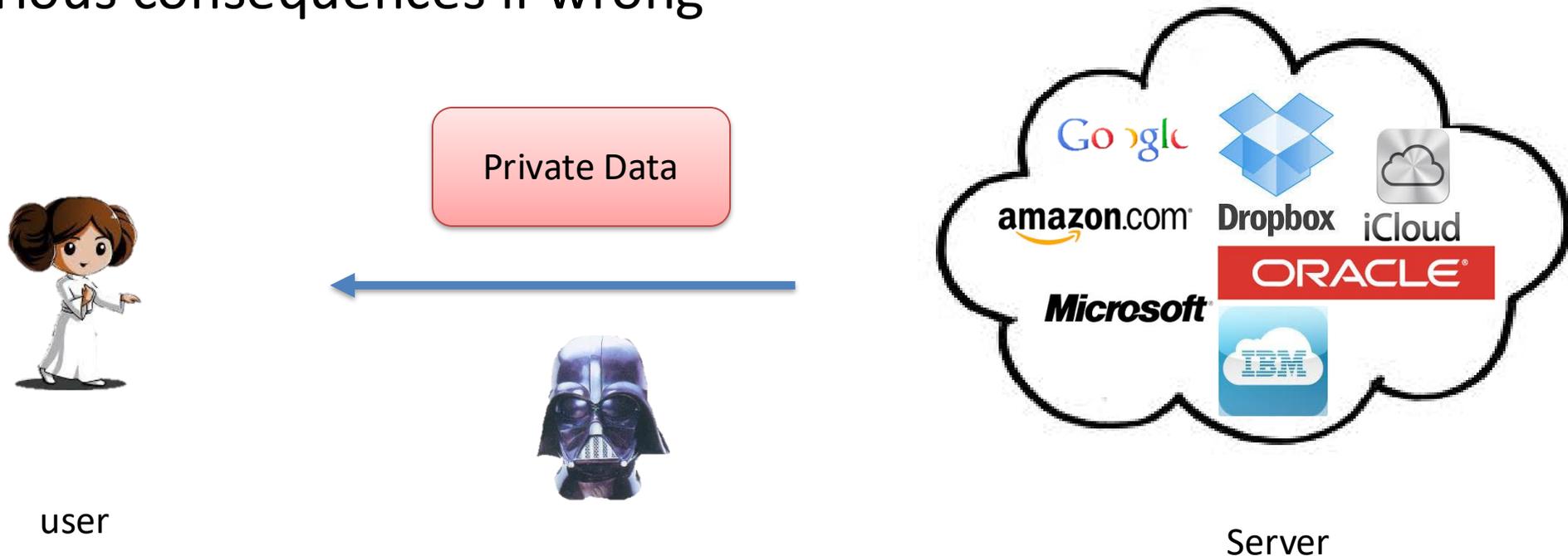
Internet Technology

- Build a **connected** world
 - Online/mobile banking
 - Email
 - Social media
 - Online conference



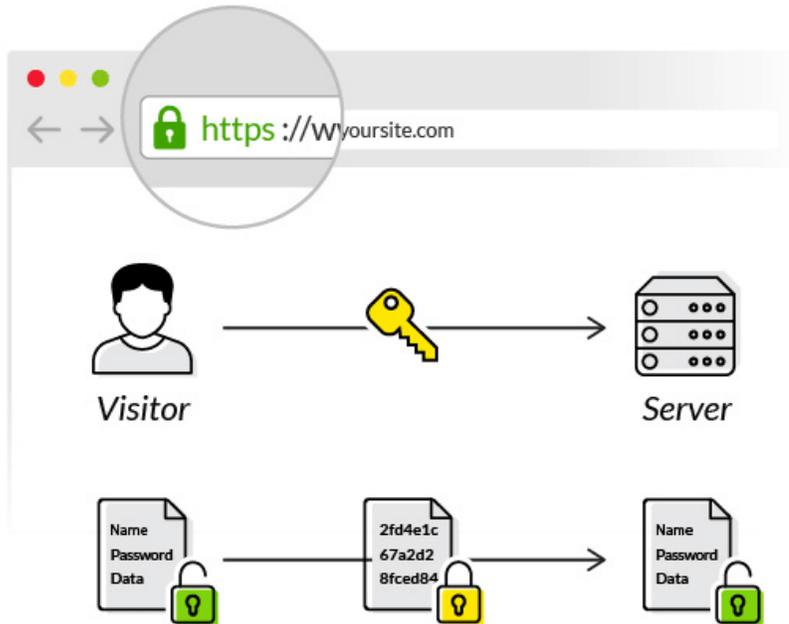
Security of Cyberspace

- **Privacy** and **Authentication** are important!
 - **Sensitive** data in cyberspace
 - Serious consequences if wrong



Important Technology

- Public-key cryptography (PKC)
 - Foundation of https
 - Email, secure payment, social media logins, etc.



Foundation of PKC

- Need math problems **not** solvable by even super computers
 - Only **a few** candidates

Factoring:

Secret key: (p, q) , Public key: $N=pq$
RSA crypto systems

Discrete Log:

Secret key x , Public key: (g, g^x)
Diffie-Hellman Key Exchange



Foundation is Challenged!

- [Shor94] **poly-time quantum** algorithm to **solve** factoring and DLog
 - Quantum is **more powerful**
- Technology was **not** there.
 - E.g., “ $15 = 3 * 5$ ” (2001)
 - Not practical yet



Technology Advances!

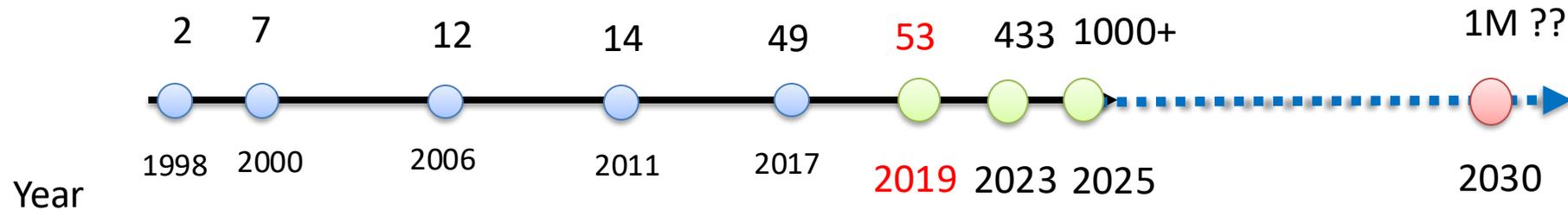
- Towards building larger quantum computers



IBM



of qubits



First Quantum Supremacy
for specific task (Google)

Facing New Reality

- NIST: Post Quantum (PQ) PKC standardization call [2016 - ongoing]
- Industry: Evaluate performances of PQ candidates



[AWS Security Blog](#)

Post-quantum TLS now supported in AWS KMS

by Andrew Hopkins | on 04 NOV 2019 | in [Advanced \(300\)](#), [AWS Key Management Service](#), [Security, Identity, & Compliance](#) | [Permalink](#) | [Comments](#) | [Share](#)

NIST
National Institute of
Standards and Technology

Traditional PKC Crisis

- **Obsolete** eventually at some point...
 - New security infrastructure
- Critical time to develop new sciences
 - New **foundation** for PQ Crypto
 - New advanced Crypto **capabilities**



Cryptography



Quantum Computing

My Research

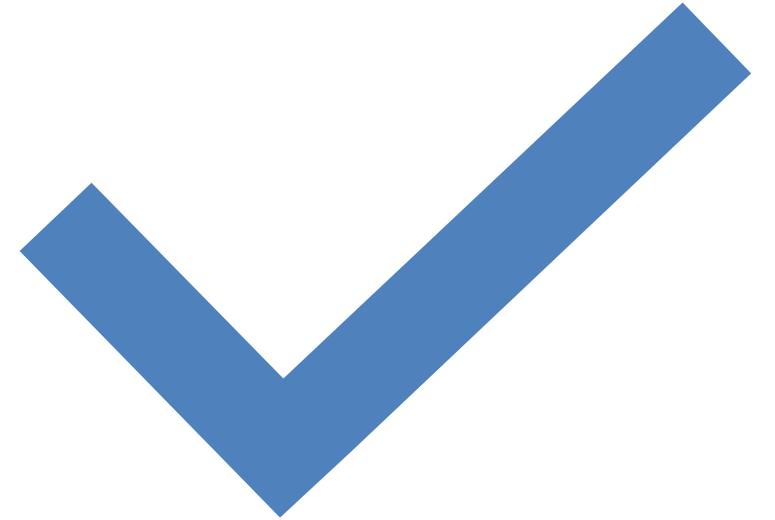
- Basic Mission: **Rebuild** basic crypto tools **against** quantum computing
 - Post-quantum (PQ) cryptography [NIST current efforts]
 - Future security of internet applications



- Vision: Enable **efficient richer** crypto capabilities
 - Computing on encrypted data, **Fully homomorphic encryption (FHE)**
 - Applications to **private ML and data analytics**
 - Numerous **advanced** crypto designs

Roadmap

- Background
- Recent Progress
- Challenges and Vision



Cryptography in General

- **What** is “security”?
 - No attacker can “break” the system
 - What does that mean?
- **How** to achieve “security”?
 - How to defend against infinitely many possible attacks?

Modern Cryptography

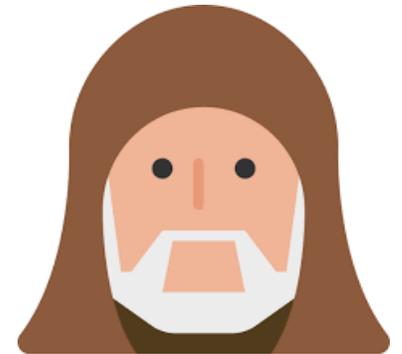
- Define a Clear Security Goal
 - E.g., Secure Channel



Send private messages

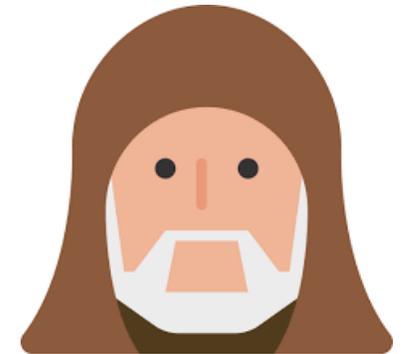
Secure

?????



Modern Cryptography

- Define Security
 - Formulate a **notion** that captures “secure” channel
 - Not able to **recover** the whole plaintext?
 - We need: “attacker **cannot learn** anything” [Goldwasser-Micali82]



Modern Cryptography

- Define Security
 - Formulate a **notion** that captures “secure” channel
 - Not able to **recover** the whole plaintext?
 - We need: “attacker **cannot learn** anything” [Goldwasser-Micali82]
 - Explicitly requested in the **NIST PQC** call

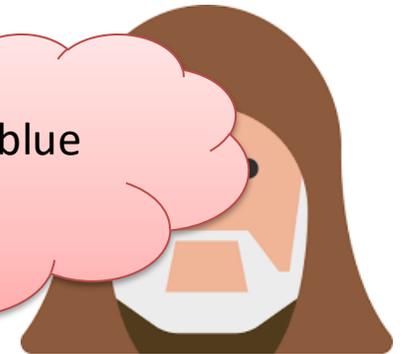


Help me, Obi-Wan Kenobi.
You're my only hope !

Empire is the best !

Imaginary dummy message

Orange or blue
????



Modern Cryptography

- How to realize the secure goal?
 - **No real** physical secure channel
 - Construct a “droid” using **math** – “encryption.”



Help me, Obi-Wan Kenobi.
You're my only hope !

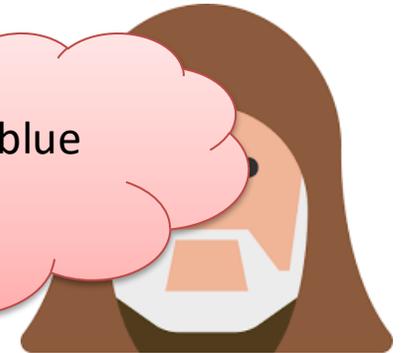
Empire is the best !



Help me, Obi-Wan Kenobi.
You're my only hope !



Orange or blue
????



Modern Cryptography

- How do we prove security against infinitely many attacks?

- The re

- Hard

If an **adversary** can break the crypto system, then there exists a **reduction** (that uses the adversary) that can solve the math problem.



Hard



Reduction



If the math problem is not solvable, then no **adversary** can break the crypto system => Crypto system is secure



Modern Cryptography

- We have some candidates
 - e.g., RSA, Discrete Log => Secure Crypto



Hard Math Problem

RSA, DL



Reduction



Crypto System



In the Quantum Era

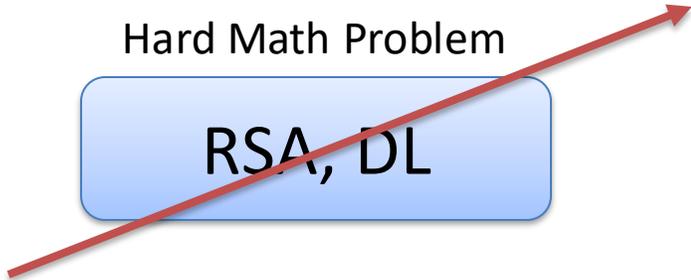


Quantum Computing



Hard Math Problem

RSA, DL



∇

Reduction



Crypto System



In the Quantum Era



Quan



What we need:

- New hard math problem against quantum
- New design and proof of security



Hard Math Problem

~~RSA, DL~~

∇

Reduction



Crypto System



Cryptography Lessons We've Learned

- Theoretical foundation (pre-quantum) matters
 - Modular design – plug-and-play
 - **CPTS 327** !!!!!

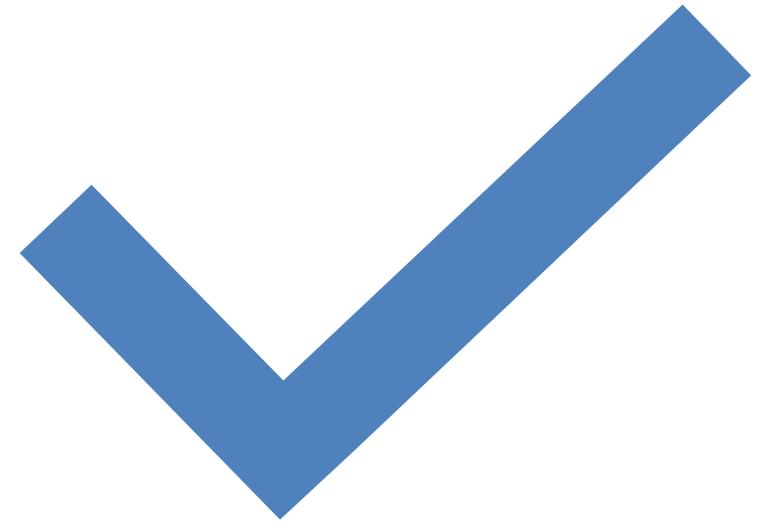


Roadmap

- Background

- Recent Progress

- Challenges and Vision



NIST's PQC Call

- Aim to standardize future PQC [2016 - now]
 - Take **more than** 20 years for migration
- Challenges
 - Hard to find plausible math problems
 - Setting specific parameters for efficiency + security
 - Implementation-level details
 - Real-world deployment

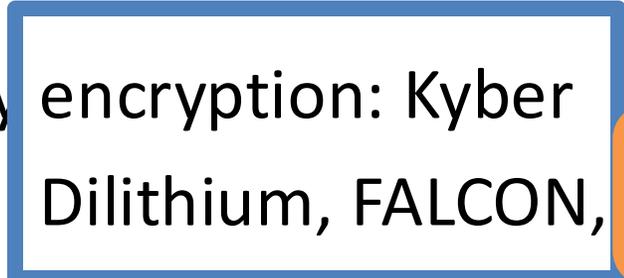
NIST's PQC Call

- New math hard problems and crypto designs
 - Code-based
 - Lattice-based
 - Hash-based
 - Isogeny-based
 - Multivariate-based
 - More...

NIST Progress

- 3rd Round:
 - Public-key encryption: Kyber
 - Signature Dilithium, FALCON, SPHINCS+
 - Selected for standardization
- 4th Round:
 - Public-key encryption HQC (Selected 2025)
 - A lot going on

Lattice-based



Hash-based

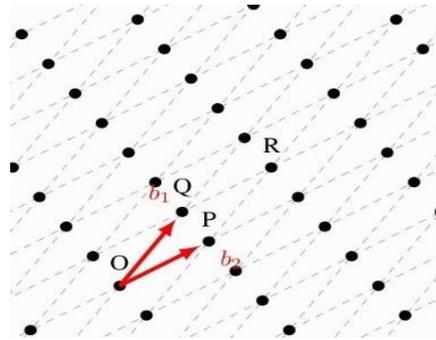


Code-based

Sleepless Cryptographers

- Many candidates were broken
 - Rainbow (multivariate) [Crypto 2022]
 - SIKE (isogeny) [Eurocrypt 2023]
 - More ...
- Still plausible
 - Lattice
 - Hash
 - Code
 - Perhaps isogeny ???

New Hope: Lattice-based Cryptography



- Advantages of Lattices:
 - **Efficient** operations
 - **Resistance** to quantum attacks (plausible)
 - **Foundation** of advanced crypto systems for richer crypto capabilities and applications

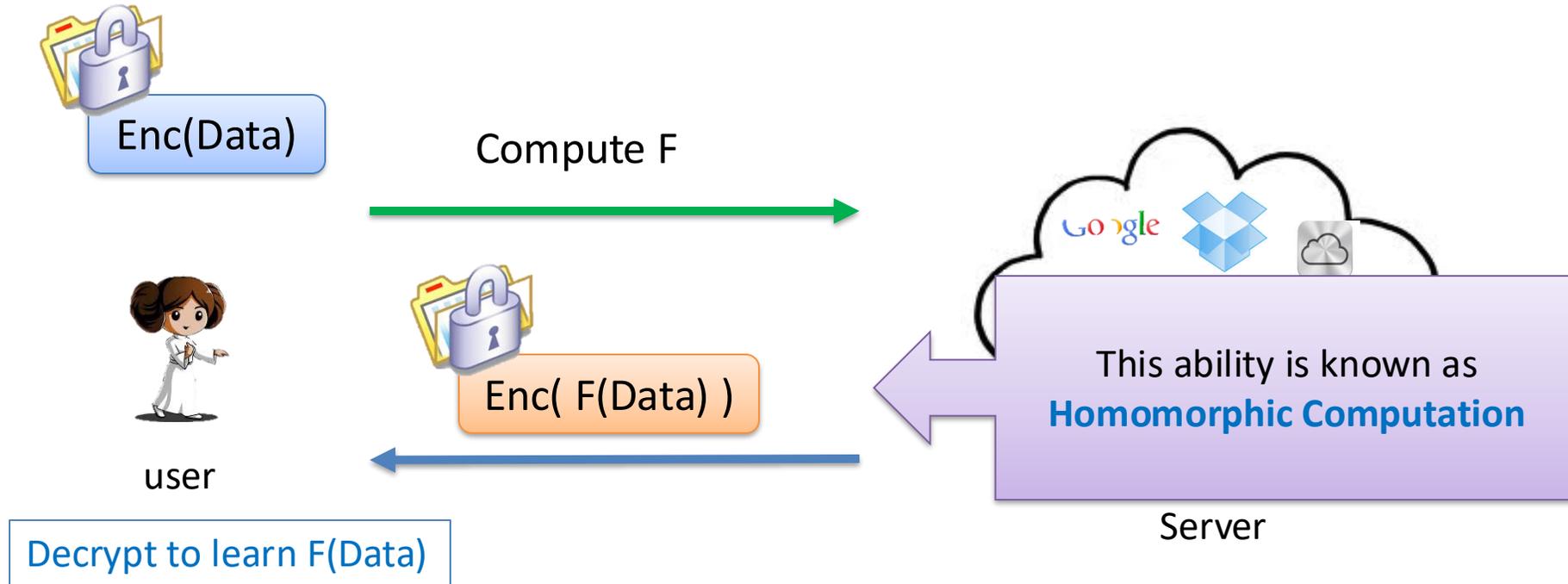
New Hard Problem

- Learning with errors (LWE) [Regev 2005]
 - Theory [Peikert's survey 16]
 - Practice [NIST ongoing PQC comp]
- New PQ candidates in theory!
 - Public-key encryption
 - Signatures
 - Key exchange
 - Three variants are standardized by NIST



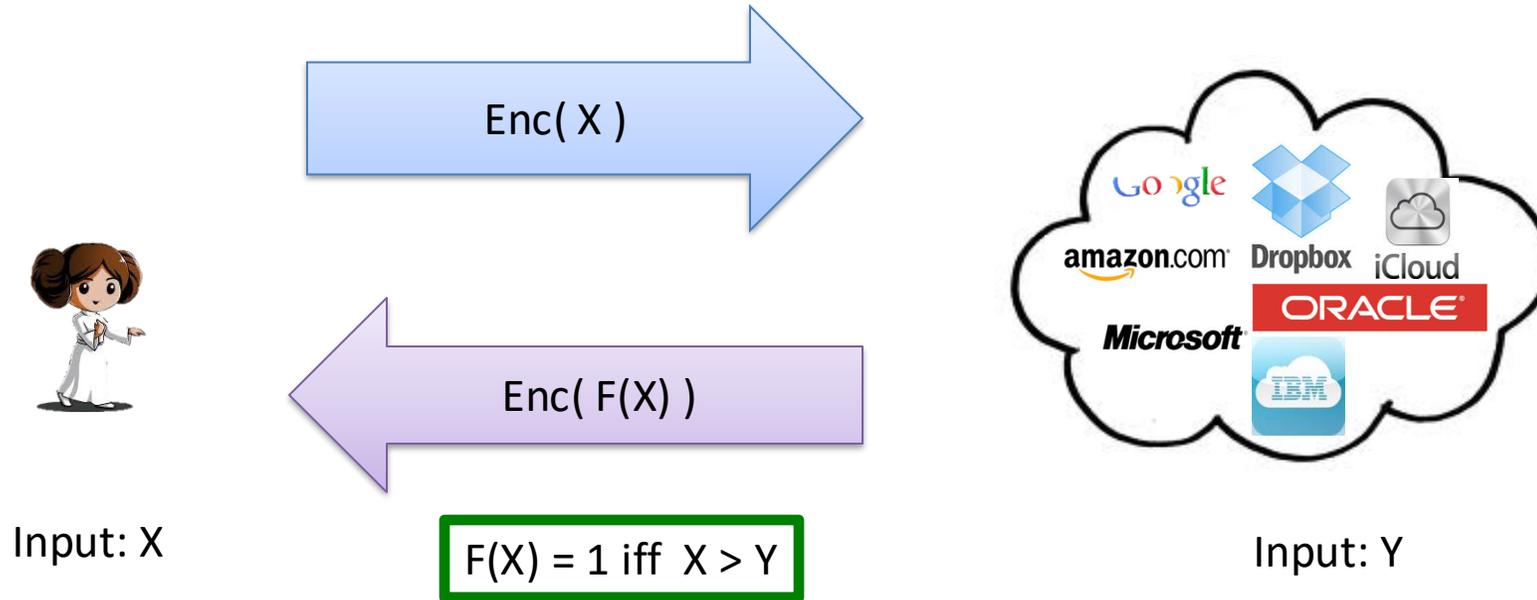
Advanced Capabilities

- Computation on **encrypted** data
 - Fully Homomorphic Encryption (**FHE**) [Gentry, BV, GSW]
 - Outsource computation
 - **Holy grail** to keep data secure while in use [DARPA DPRIVE]



Application to MPC

- An **elegant** solution to classic **Yao's Millionaire Problem** [1980's]
 - Two parties hold private inputs X and Y . Determine which is larger **without** revealing what they are
 - E-finance, e.g., compare numbers that are confidential

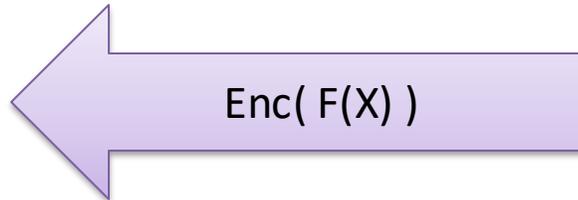
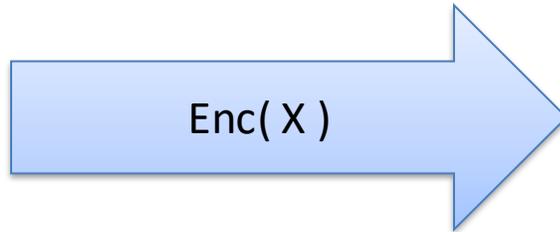


New Applications – Private MLaaS

- New solutions to **private ML as a Service** [2020's]
 - Cloud holds a private ML Model Y
 - User has private data X
 - User wants to outsource analysis of private X **without** revealing X
 - Cloud does **not** want to reveal Y



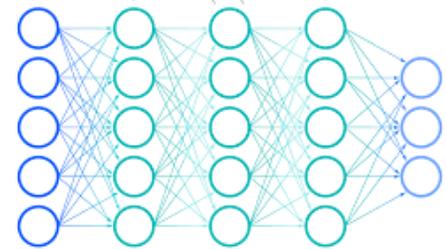
Input: X



$F(X) = \text{analysis using param } Y$



Input: Y



Triumph of Crypto Theory

- Theorem 1 [Regev]
 - Under hardness LWE, there exists a **PQ Public-key Encryption** (PKE)
- Theorem 2 [Gentry, BV, BGV, GSW, AP...]
 - Under hardness of LWE, there exists a **PQ fully homomorphic encryption** (FHE) for **any arbitrary** function of homomorphic computation
- Theorems 3, 4, 5....
 - Under hardness of LWE, there exists **a wide array** of advanced **PQ** cryptosystems, e.g., identity-based encryption, attributed-based encryption, functional encryption, and more...

In Praise of LWE



Learning with Errors (LWE) [Regev]

- Parameters: $n, m, q \in \mathbb{N}$ and error distribution χ over \mathbb{Z} .
- Task:** learn secret $\mathbf{s} \in \mathbb{Z}_q^n$ given many “noisy inner products”



$$\mathbf{a}_1 \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n, \quad \mathbf{b}_1 = \langle \mathbf{a}_1, \mathbf{s} \rangle + \mathbf{e}_1 \in \mathbb{Z}_q$$

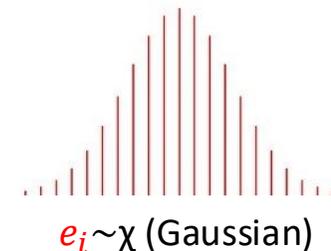
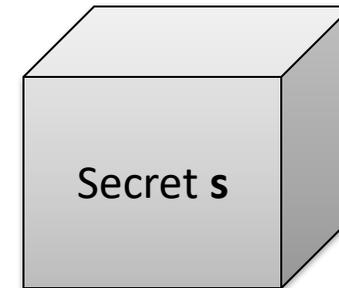
$$\mathbf{a}_2 \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n, \quad \mathbf{b}_2 = \langle \mathbf{a}_2, \mathbf{s} \rangle + \mathbf{e}_2 \in \mathbb{Z}_q$$

⋮

$$\mathbf{a}_m \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n, \quad \mathbf{b}_m = \langle \mathbf{a}_m, \mathbf{s} \rangle + \mathbf{e}_m \in \mathbb{Z}_q$$

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \in \mathbb{Z}_q^m.$$

and \mathbf{s}



Even powerful
(quantum) adversary
cannot learn the secret

However...

- LWE-based constructions are not efficient
 - Large Key
 - Large Ciphertext
 - Slow in computation...

How Inefficient?

- E.g., the original PKE of [Regev05]
 - Later FHEs [BV11, GSW13] build on this

Research Goal

Improve LWE, leading to practical solutions

- Future cybersecurity infrastructure
- Advanced crypto capabilities

PK Length	1MB
Noise Sampling in Encryption	<ul style="list-style-type: none">• 100 cycles per sample• Need 1000 samples• 30 – 40% of the process



- **Large efficiency loss** compared with pre-quantum RSA
 - E.g., 3072 or 4096 bits of PK length
- No NIST candidate really uses this [exact] sampling

To Improve Efficiency

- More **algebraic structures** [SSTX, LPR]
 - Use (polynomial, algebraic) rings
 - Called (Module) Ring LWE

- Use **rounding** [BPR]
 - Use elementary integer (INT) operation
 - Called (Module) Ring LWR [Rounding]
 - Imply pseudorandom functions (PRF)

Fundamental Questions

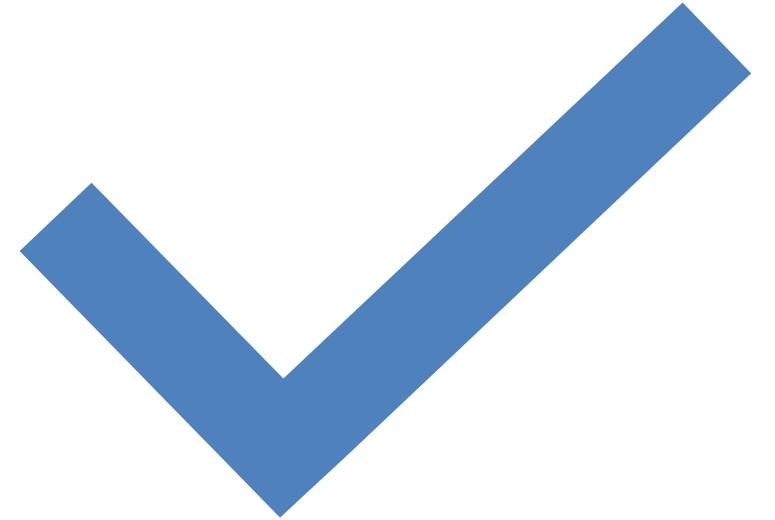
- Are the variants of LWE hard?
 - Would additional structures (ring and rounding) **affect** security?
 - The adversary might take advantage of ...
- Crypto is **subtle** and **sensitive** ...
 - **Insecurity** comes from **nuances**

Some of my Research

- Show formally **Ring + Rounding** variant is **as hard** as **Ring**
- Prior work
 - **Ring LWE** is **as hard** as some **ideal lattice problem**
- **Ring + rounding** is **as hard** as some **ideal lattice problem**
 - Currently no known algorithm for ideal lattice problem

Roadmap

- Background
- Recent Progress
- Challenges and Vision



More Challenges

- On Apr 10, 2024, Yilei Chen claimed a new **quantum poly-time algorithm** that solves LWE
 - 9-step algorithm
 - [eprint/2024/555](https://eprint.iacr.org/2024/555)
- Implications
 - PKE/Sig submitted to NIST are **not** affected under parameter range of the attack
 - **Several variants of FHEs** are not post-quantum (only 3rd gen remains secure)
 - LWE might not be post-quantum at all
- A lot of discussions....
 - <https://scottaaronson.blog/?p=7946>
 - <https://nigelsmart.github.io/LWE.html>
- On Apr 18, 2024, a fatal **mistake** was discovered
 - **LWE and their variants remain post-quantum secure**

Vision

- **LWE +**
 - New algebraic techniques to improve speed/security for PKE, FHE, etc
 - Analysis of the security foundation
 - Software + hardware acceleration
- **LWE –**
 - Make the algorithm great again !!!

Science wins either way



Silvio Micali
Turing Award 2012



Thank You!

