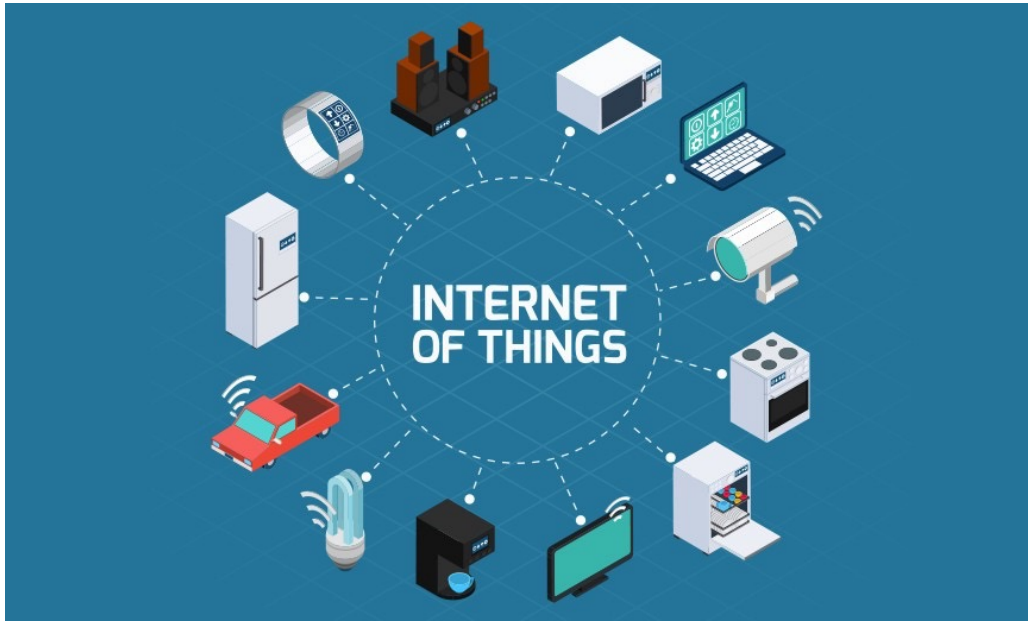
Cryptography in the Presence of Quantum Computing --

New Opportunities and Research Directions

Feng-Hao Liu
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

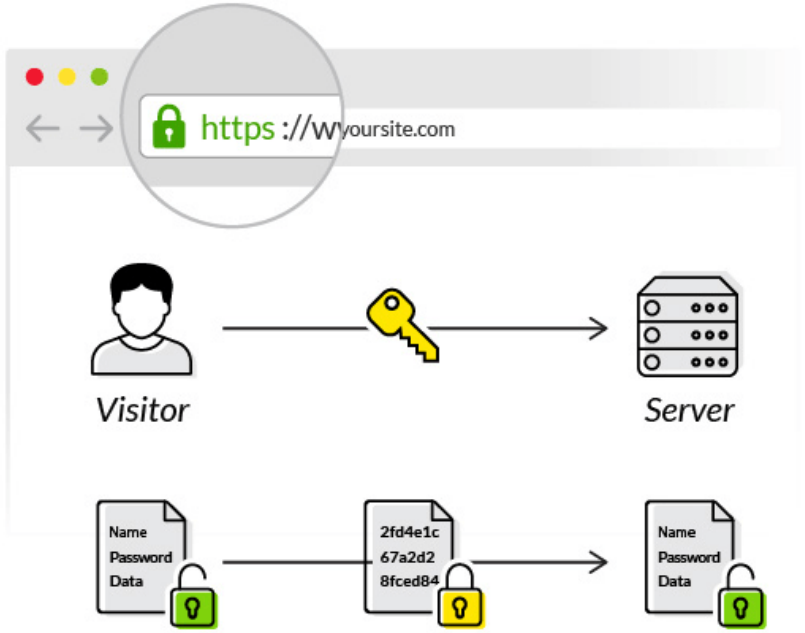
user

Private Data

Server

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:

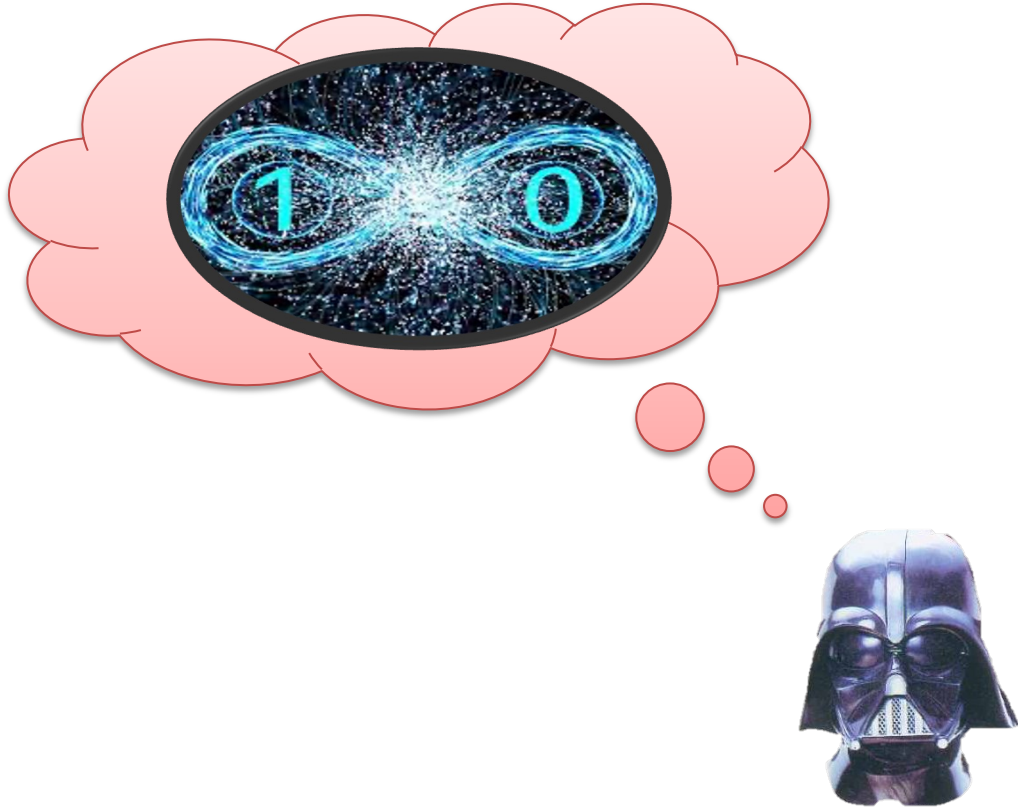
Secret key x, Public key: (g, g^x)

Diffie-Hellman Key Exchange

Foundation is Challenged!

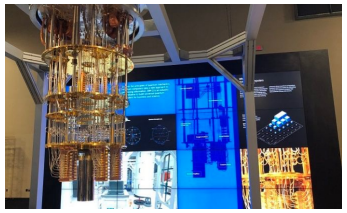
- [Shor94] poly-time quantum algorithm to solve factoring and DLog
  - Quantum is more powerful

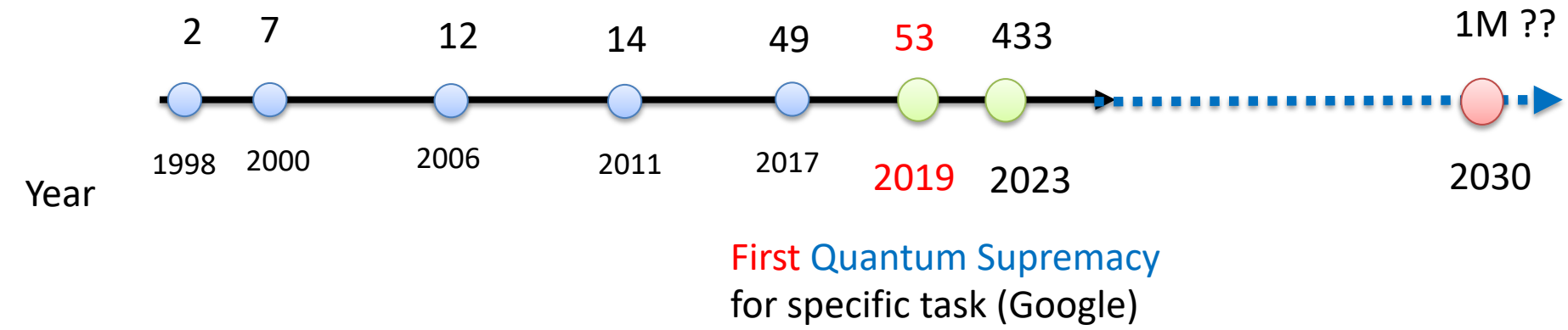
- Technology was not there.
  - E.g., “15 = 3 * 5” (2001)
  - Not practical yet



Technology Advances!

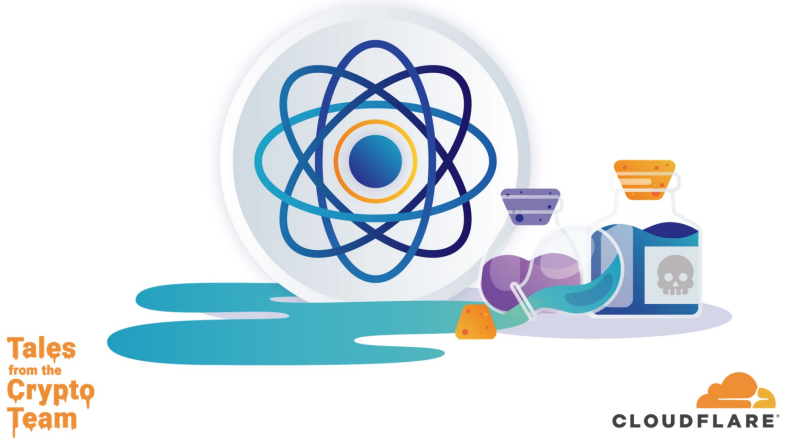
- Towards building larger quantum computers





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

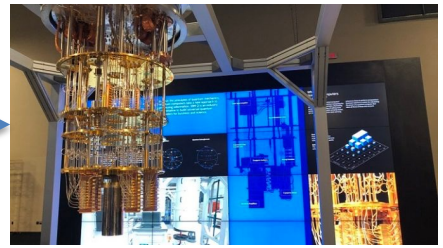
by Andrew Hopkins | on 04 NOV 2019 | in Advanced (300), AWS Key Management Service, Security, Identity, & Compliance | Permalink | Comments | Share

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

Crypto Basics

My Work

High Level Overview

Applications

Vision

Future Opportunities

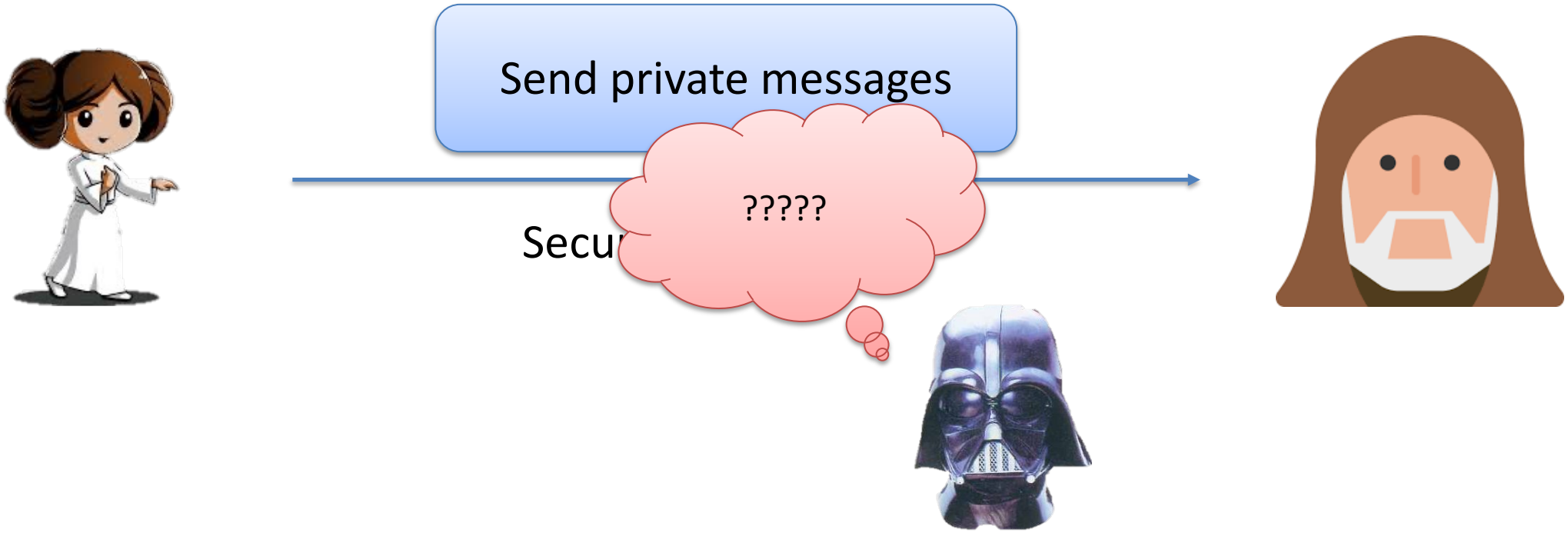
Cryptography in General

- 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

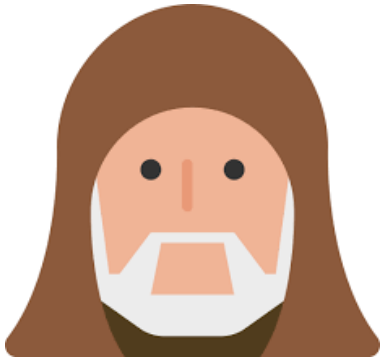
- Define a Clear Security Goal
  - E.g., Secure Channel



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]

[redacted], Obi-Wan Kenobi.
[redacted]



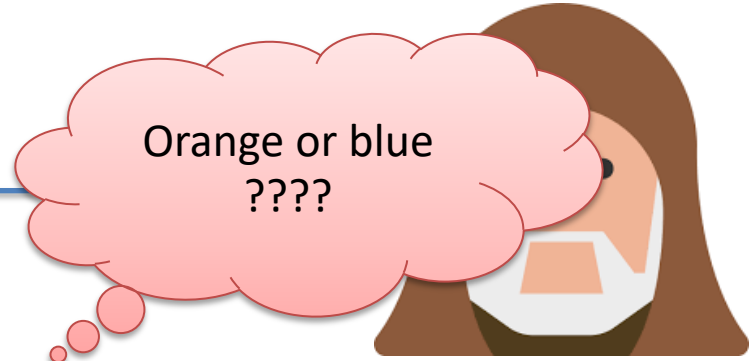
Modern Cryptography

- 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



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 !

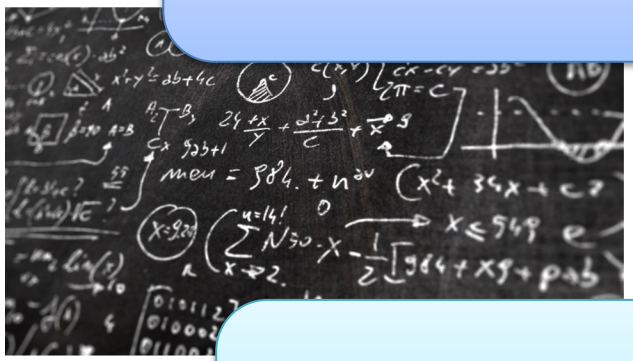
SK

Orange or blue
????

Modern Cryptography

- How do we prove security against infinitely many attacks?
  - The re
    - Har

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



Hard

$\leq$

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

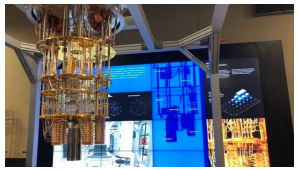
RSA, DL

$\leq$

Reduction

Crypto System

In the Quantum Era



Quantum Computing

Hard Math Problem

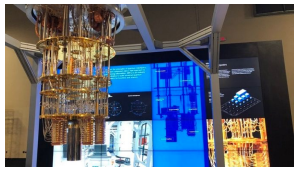
~~RSA, DL~~

$\leq$

Reduction

Crypto System

In the Quantum Era



Quan

What we need:

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

$\leq$

Reduction

Crypto System

Hard Math Problem

~~RSA, DL~~

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
National Institute of Standards and Technology

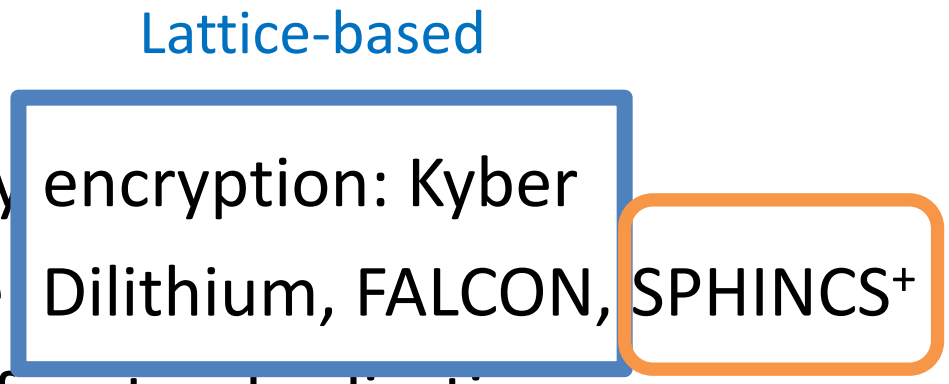
NIST's PQC Call

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

National Institute of Standards and Technology

NIST Current Progress

- 3rd Round:
  - Public-key encryption: Kyber
  - Signature: Dilithium, FALCON, SPHINCS+
  - Selected for standardization
- 4th Round:
  - Ongoing
  - A lot of exciting (heartbreaking) news



National Institute of Standards and Technology

The Nature of Science

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

Roadmap

Background

Crypto Basics

My Work

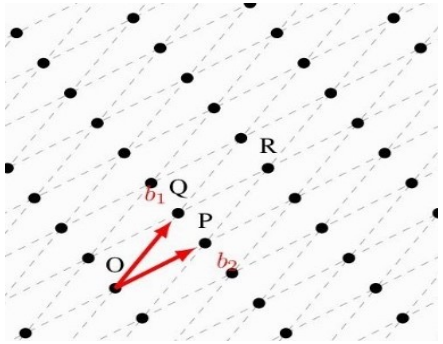
High Level Overview

Applications

Vision

Future Opportunities

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

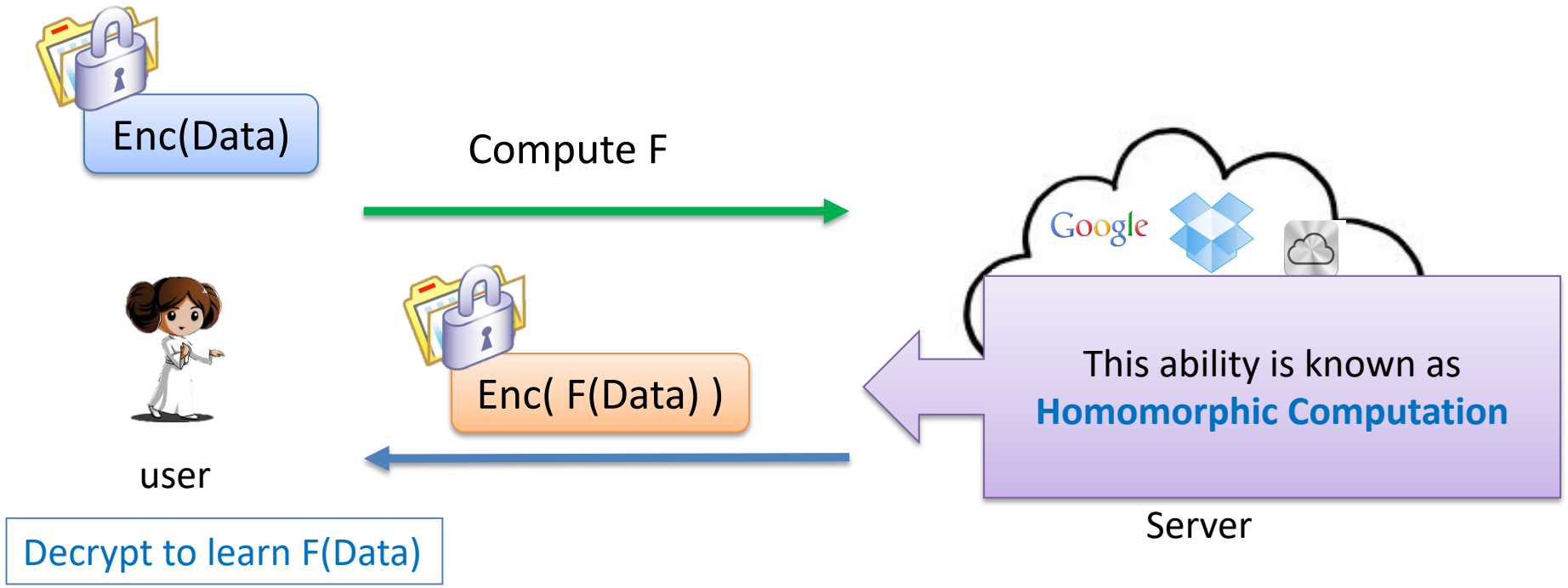
- Learning with errors (LWE) [Regev 2005]
  - Theory [Peikert's survey 16]
  - Practice [NIST ongoing PQC comp]

- New PQ candidates in theory!
  - Public-key encryption
  - Signatures
  - Key exchange
  - Three variants are going to be standardized by NIST

NIST
National Institute of Standards and Technology

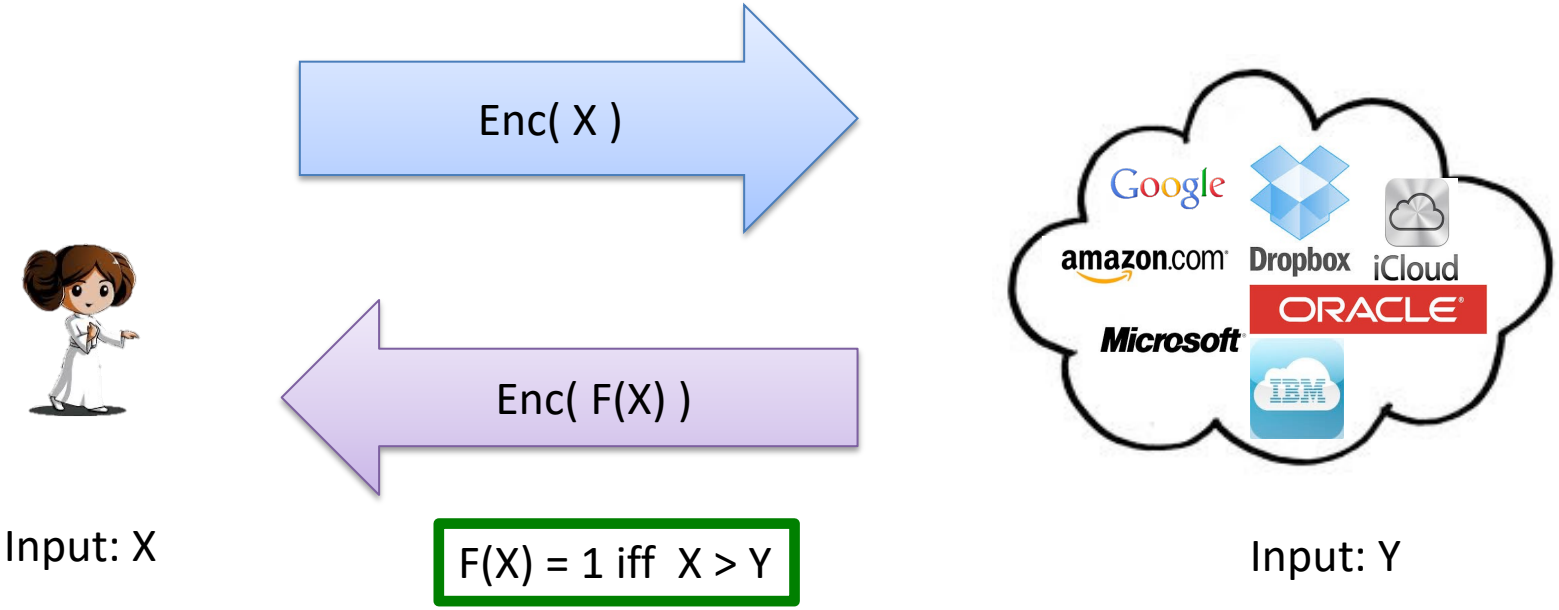
Advanced Capabilities

- 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

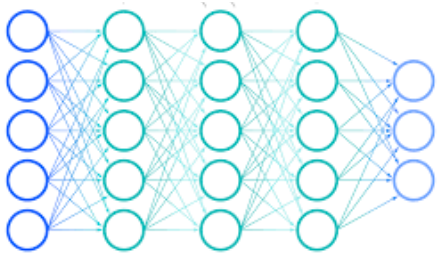
- New solutions to private ML as a Service [2020's]
  - Cloud holds a private ML Model Y
  - User has private data X
  - User wants to outsource analysis of private X without revealing X
  - Cloud does not want to reveal Y

Input: X

Enc(X)

Enc(F(X))

F(X) = 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…

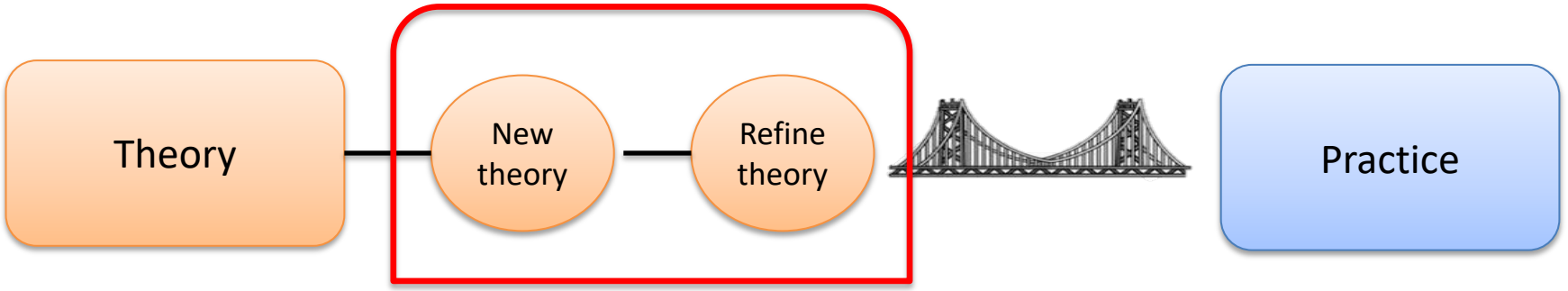
In Praise of LWE

- Gödel Prize 2018 to Regev

- Citation
  - Served as the foundation for countless subsequent works
  - Revolution in cryptography in both theory and practice
  - A simple and yet amazingly versatile foundation for nearly every kind of cryptographic object
    - along with many that were unimaginable until recently, and which still have no known constructions without LWE

Problem Solved?

- LWE offers solutions in theory
- Gap between theory and practice
  - Beyond only engineering efforts
- Need to expand and refine the theory



My work

Determine the Drawbacks

- Fact: Plain-LWE is not efficient
  - Why and How?
- Why: large concrete parameters/computation
  - Large keys in general
  - Cumbersome noise sampling procedure
- Consequence: Plain-LWE based Frodo not selected as finalist by NIST ☹

To Improve Efficiency

- Other variants of LWE
  - Algebraic Rings
  - Other form of errors

- Research questions
  - Are these variants hard?
  - Can we do more for the advanced capabilities?

My Work

- New algebraic techniques
  - Proving some useful variants of LWE is plausibly hard
  - More efficient FHE methods

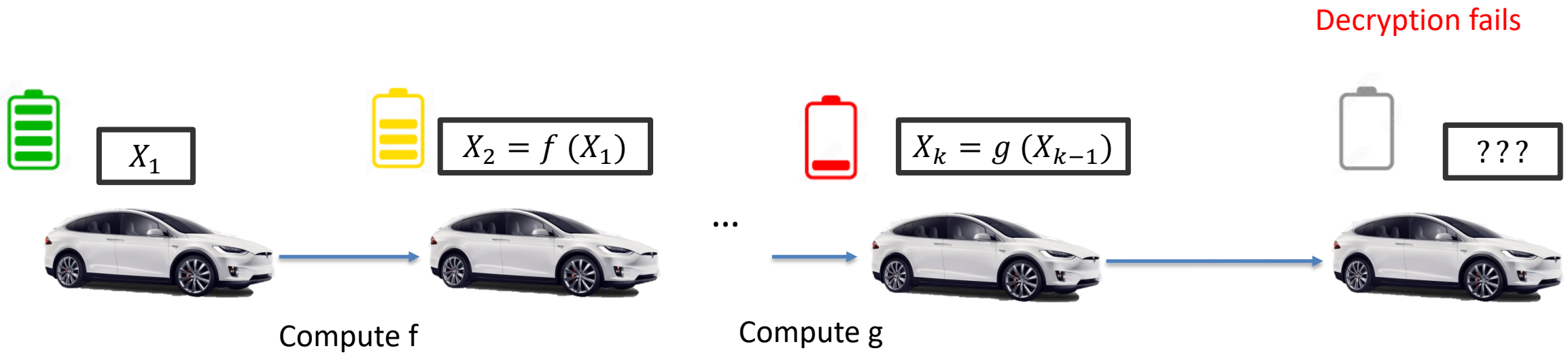
More Efficient FHE

- Fact: ”F”-HE relies on a core technique called bootstrapping
  - Important but slow

- Algebraic techniques => More efficient bootstrapping [LiuWang23a, LiuWang23b]

FHE Computation

- Basic facts:
  - All known FHE ciphertexts contain "noise"
  - Basic operations (e.g., add, mult, NAND) are rather fast
  - Computation increases noise
  - Noise becomes too large => cannot proceed computation



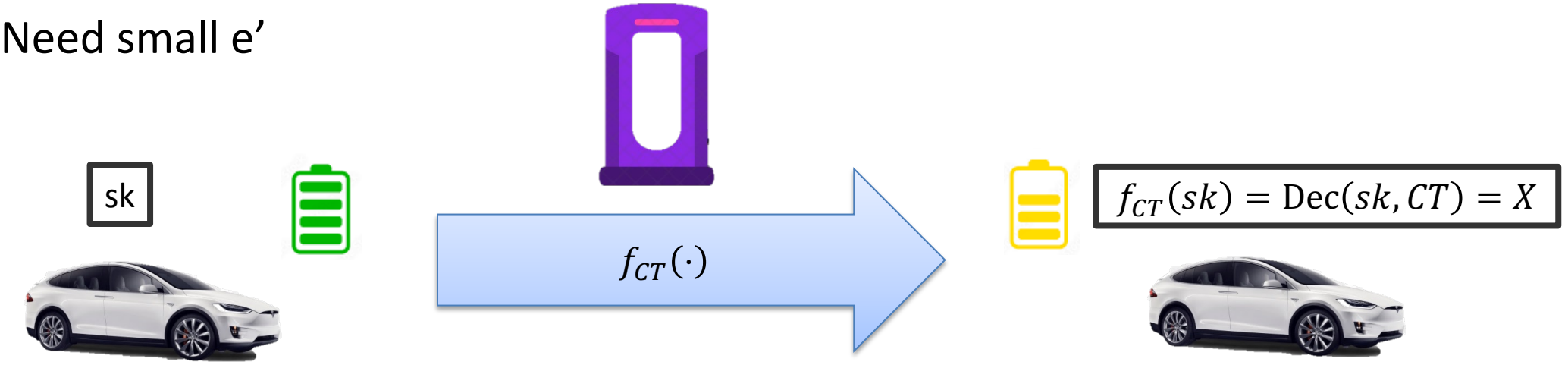
Bottleneck of FHE Computation

- To further compute on ciphertext, need to “clean” noise
  - This is called **Bootstrapping**

- Bootstrapping is significantly slower than other basic operations
  - The bottleneck

Bootstrapping Framework [Gentry]

- Need Bootstrapping Key, i.e., BK = FHE.Enc(sk)
- Input CT = FHE.Enc(X), which might be somewhat noisy
  - Define $f_{CT}(\cdot) = \mathrm{Dec}(\cdot, CT)$
- Eval also incurs noise e'
  - Need small e'



Homomorphic computation

Bootstrapping is Bottleneck

- Was slow: 30 mins to bootstrap one CT
- Significant improvements:
  - Large params/space (10 GB) + SIMD (Single Instruction Multiple Data)
    - 20 seconds to bootstrap 10000 CTs
  - Small params/space (10 MB) + fast bootstrapping
    - 1 sec [FHEW15]
    - 0.1 sec [TFHE16]
    - 30 ms [further optimizations]
    - No SIMD

My Work [LiuWang23a, LiuWang23b]

- A new mathematical framework
  - Small space
  - SIMD

- Open question:
  - Optimize the framework, more refined math techniques?
  - Determine the concrete parameters
  - Implementation and Deployment

Roadmap

Background

Crypto Basics

My Work

High Level Overview

Applications

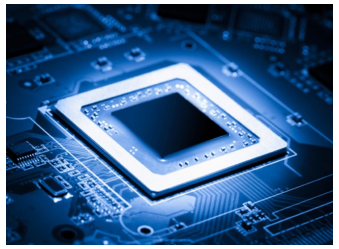
Vision

Future Opportunities

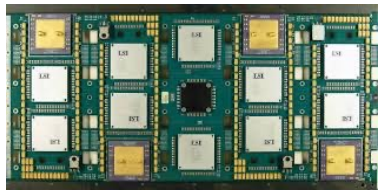
Future Direction 1 – Core FHE

- New Foundation of FHE
  - Confirm and optimize the theoretic framework
  - Determine the concrete improvements over existing solutions
  - Expand the existing FHE libraries

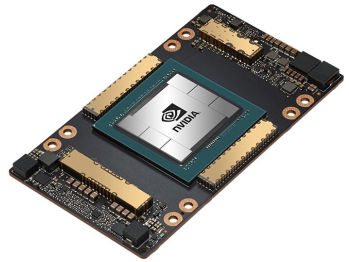
ASIC



Multi-core CPU



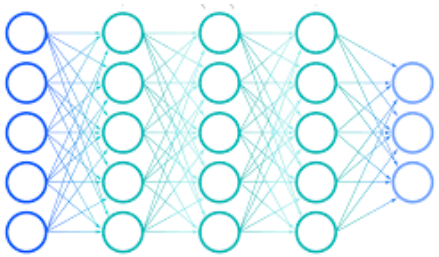
GPU



Future Directions 2 – Applications to ML

- Applications in private ML and data analytics
  - New ML-friendly FHE computation architecture
  - New FHE-friendly ML models

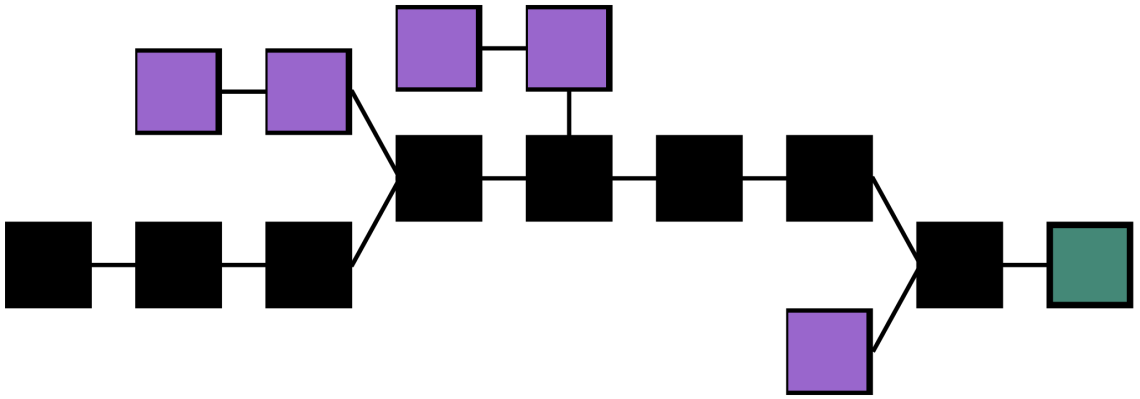
- New collaborative opportunities !

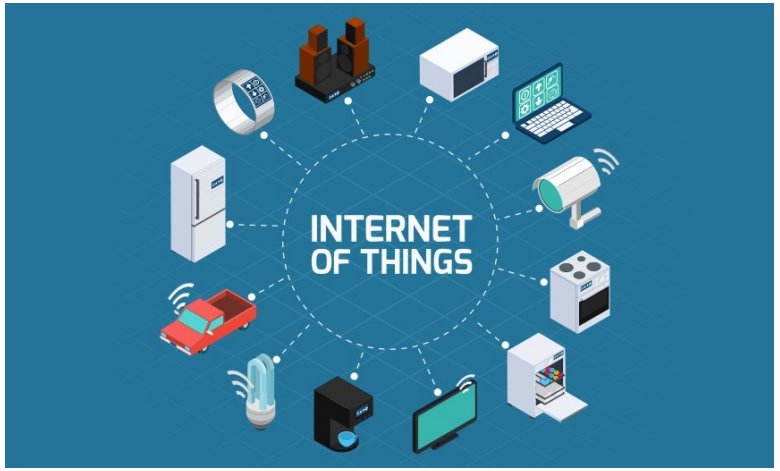


Future Direction 3 – For Future Applications

- Efficient Advanced Crypto Capabilities
  - PQ zero-knowledge proofs
  - PQ anonymous credentials
  - Efficient and scalable MPC over large datasets
  - More …

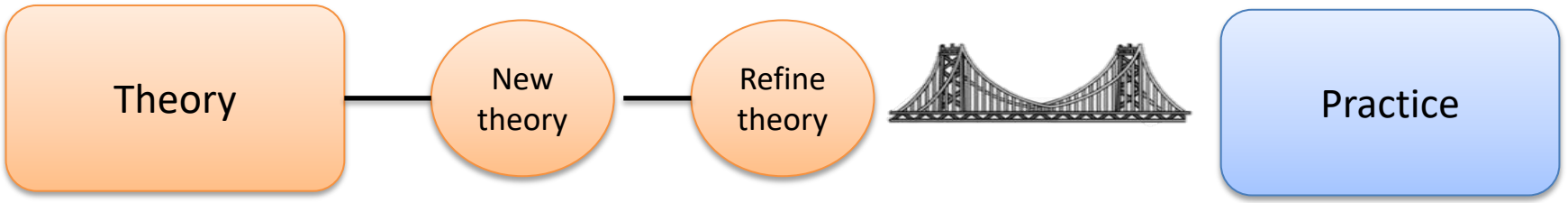
- Efficient PQ privacy enhancing technologies for the future





Vision

- 2005 – 2023: LWE implies nearly every kind of cryptographic object imaginable
  - Extremely successful theory
- 2023 and after: New techniques to make theory a reality
  - Develop new theory
  - Refine existing theory
  - Continue bridging the gap between theory and practice



Thank You!