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

![Diagram showing user and server with private data exchange]
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

# of qubits

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>2</td>
<td>7</td>
<td>12</td>
<td>14</td>
<td>49</td>
<td>53</td>
<td>433</td>
<td>1M</td>
</tr>
</tbody>
</table>

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
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**
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

Send private messages

?????

Secure

?????

Send private messages
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

Empire is the best!

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

Orange or blue ????

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!

Orange or blue ????

SK
Modern Cryptography

• How do we prove security against infinitely many attacks?
  – The reduction framework
    • Hard math problem, design, and reduction (proof of security)

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

  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 \(\Rightarrow\) Secure Crypto

\[ \text{Hard Math Problem} \leq \text{Reduction} \]

\(\text{RSA, DL}\)
In the Quantum Era

Quantum Computing

Hard Math Problem

\[ \leq \]

Reduction

Crypto System

RSA, DL
In the Quantum Era

What we need:
- New hard math problem against quantum
- New design and proof of security

Hard Math Problem
- RSA, DL

Reduction

Crypto System
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 Current Progress

• 3rd Round:
  – Public-key encryption: Kyber
  – Signature: Dilithium, FALCON, SPHINCS+
  – Selected for standardization

• 4th Round:
  – Ongoing
  – A lot of exciting (heartbreaking) news
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
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]

This ability is known as Homomorphic Computation
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

\[ F(X) = 1 \text{ iff } X > Y \]
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

\[
\text{Input: } X \rightarrow \text{Enc}(X) \rightarrow \text{F}(X) = \text{analysis using param } Y
\]

\[
\text{Input: } Y \rightarrow \text{Enc}(Y)
\]
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

![Diagram showing the relationship between Theory, New theory, Refine theory, and Practice. My work highlighted in red.](image)
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

\[ X_1 \Rightarrow X_2 = f(X_1) \Rightarrow \ldots \Rightarrow X_k = g(X_{k-1}) \Rightarrow \text{Decryption fails} \]
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 $f_{CT}(\cdot) = \text{Dec}(\cdot, CT)$

- Eval also incurs noise $e'$
  - Need small $e'$

Homomorphic computation

$f_{CT}(sk) = \text{Dec}(sk, CT) = X$
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
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!