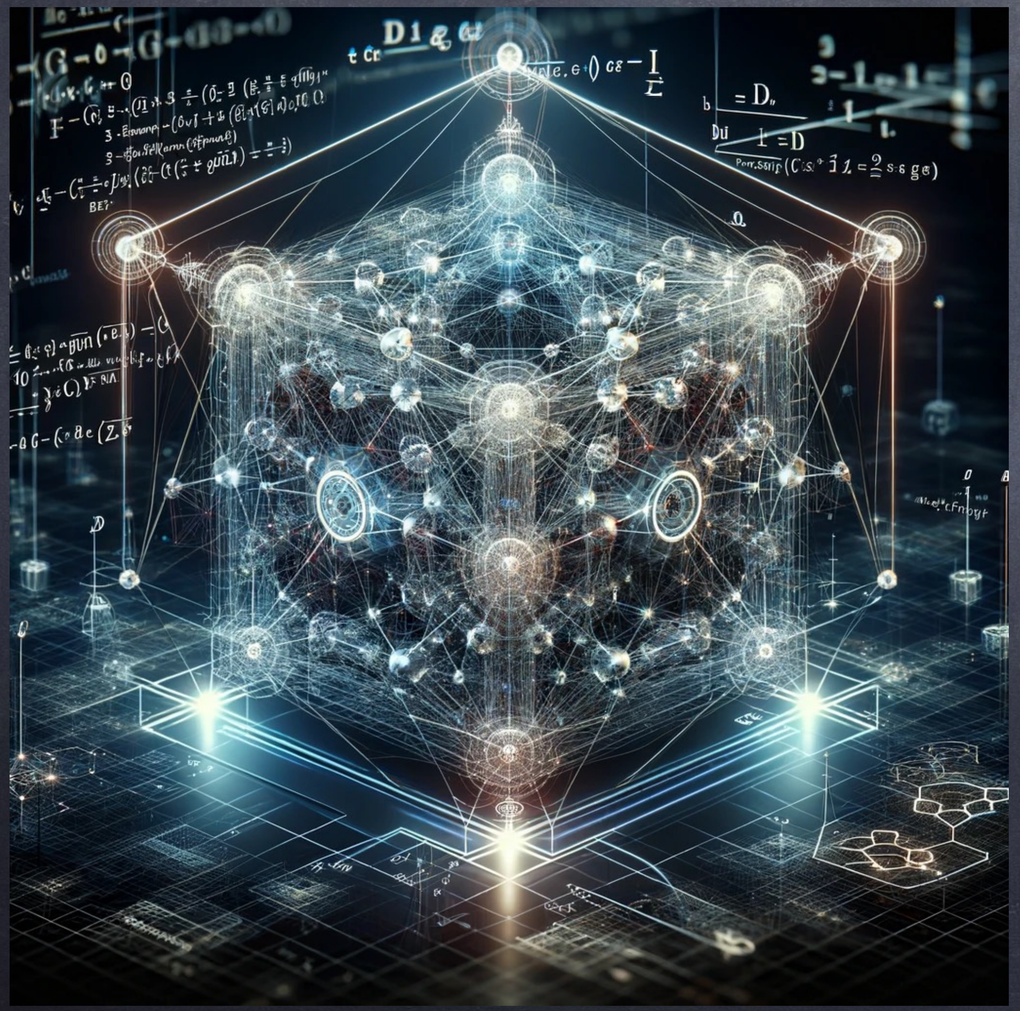
Post-quantum Cryptography



Professor Dr. Delaram Kahrobaei

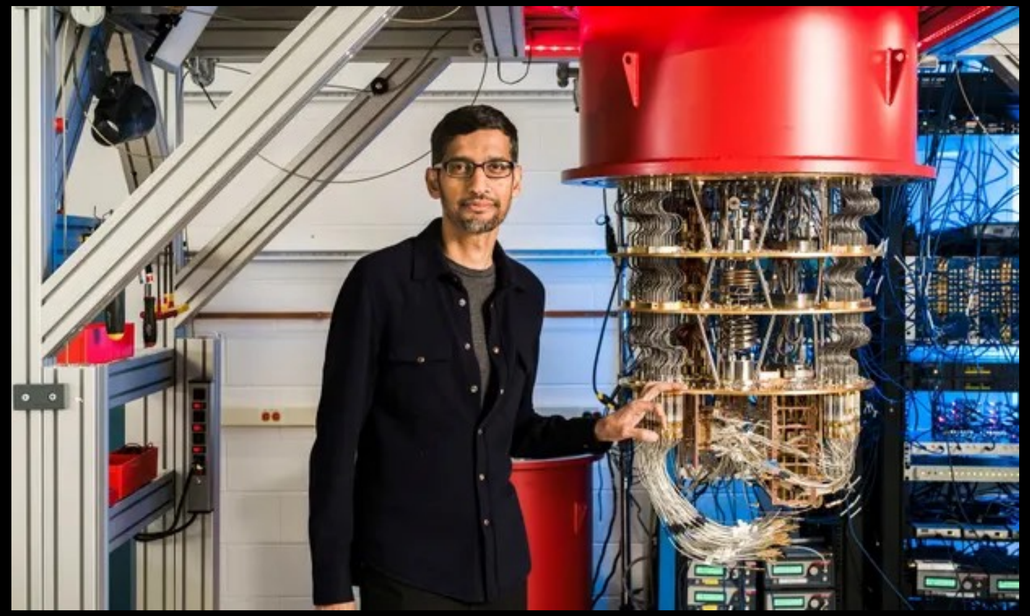
The City University of New York, QC

y

August 28, 2024

QUEENS COLLEGE

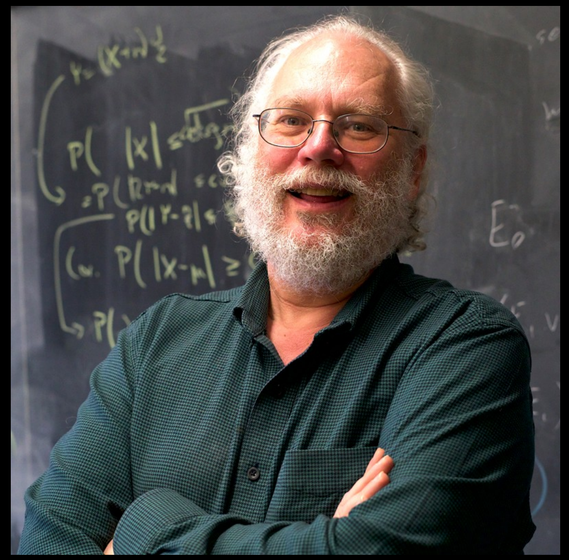
Quantum threat



Sundar Pichai (CEO Google)
Sycamore (53 qubits)

Quantum Polynomial-Time for Factoring (1994)

- RSA2048
  - ➡ Classic ≈ 400 years
  - ➡ Quantum ≈ hours



Peter Shor (MIT)

PASQAL

Generation 1

Currently in production

100 QUBITS Today

200 QUBITS Coming Soon

Generation 2

Currently in research & development.

1,000 QUBITS

Risk status


Scaling IBM Quantum technology
IBM
IBM Q System One (Released)
(In development)
Next family of IBM Quantum systems
2019
2020
2021
2022
2023
and beyond
27 qubits
Falcon
65 qubits
Hummingbird
127 qubits
Eagle
433 qubits
Osprey
1,121 qubits
Condor
Path to 1 million qubits and beyond
Large scale systems
Key advancement
Optimized lattice
Key advancement
Scalable readout
Key advancement
Novel packaging and controls
Key advancement
Miniaturization of components
Key advancement
Integration
Key advancement
Build new infrastructure, quantum error correction

Risk status - cont'd

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

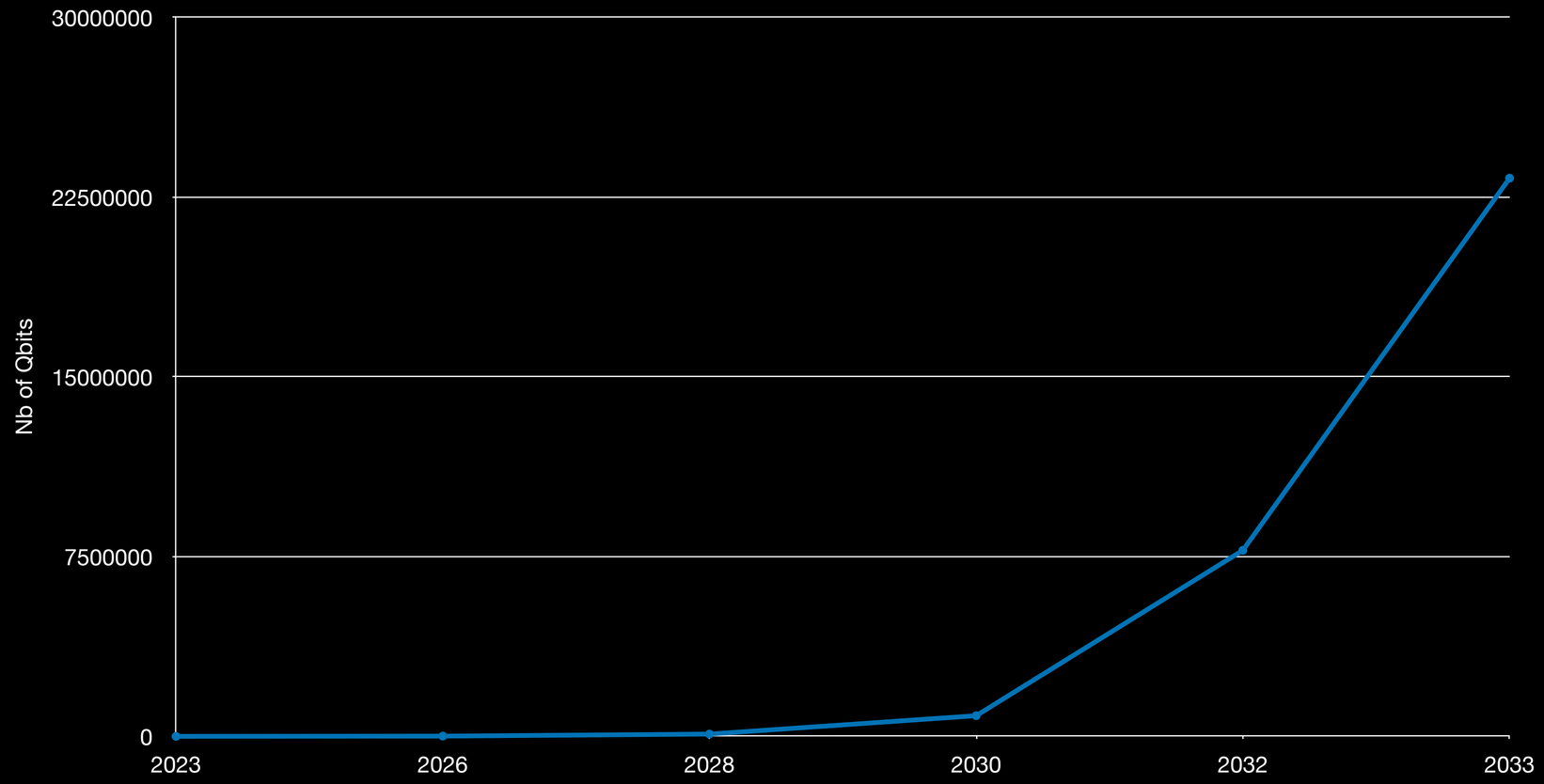
[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

		Parameters						Retry	Volume (megaqubitdays)		Qubits (megaqubits)	Runtime (hours)
n	n_e	d_1	d_2	δ_{off}	c_{mul}	c_{exp}	c_{sep}	Risk	per run	expected	per run	per run
1024	$3(n/2-1)-40$	15	27	5	5	5	1024	6%	0.5	0.5	9.7	1.3
2048		15	27	4	5	5	1024	31%	4.1	5.9	20	5.1
3072		17	29	6	4	5	1024	9%	19	21	38	12
4096		17	31	9	4	5	1024	5%	48	51	55	22
8192		19	33	4	4	5	1024	5%	480	510	140	86
12288		19	33	3	4	5	1024	12%	1700	1900	200	200
16384		19	33	4	4	5	1024	24%	3900	5100	270	350

Risk status - cont’d

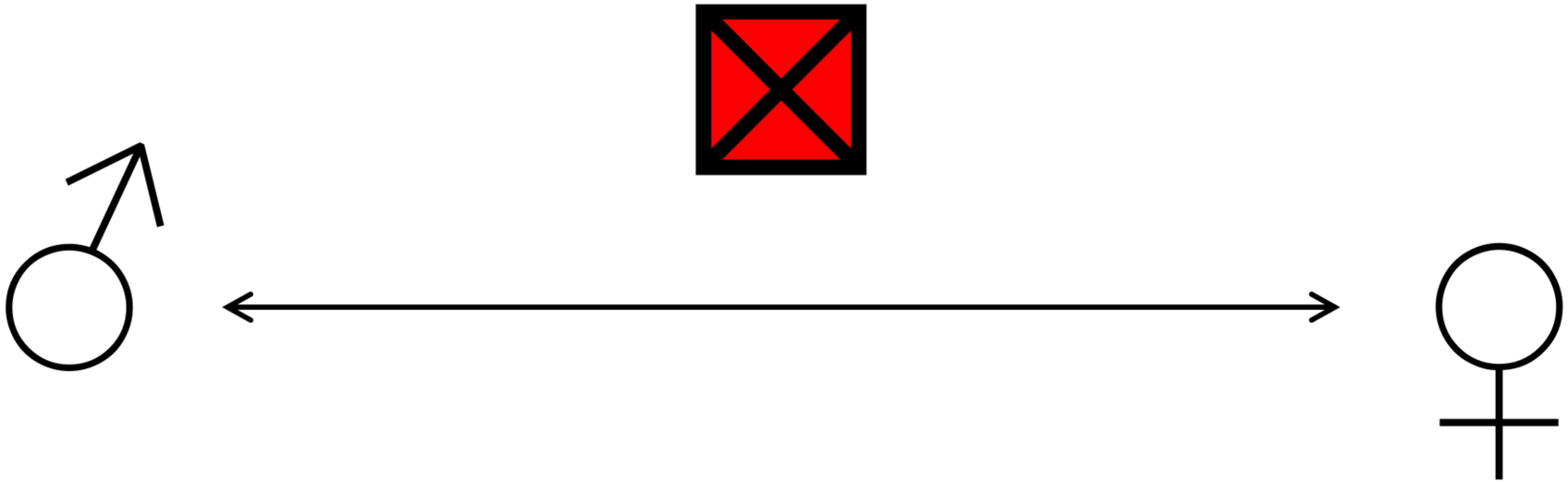
Paranoid estimates

- Breaking RSA1024 ≈ 8 years
- Breaking RSA2048 ≈ 9 years



Store now, decrypt later

Key-Exchange Problem

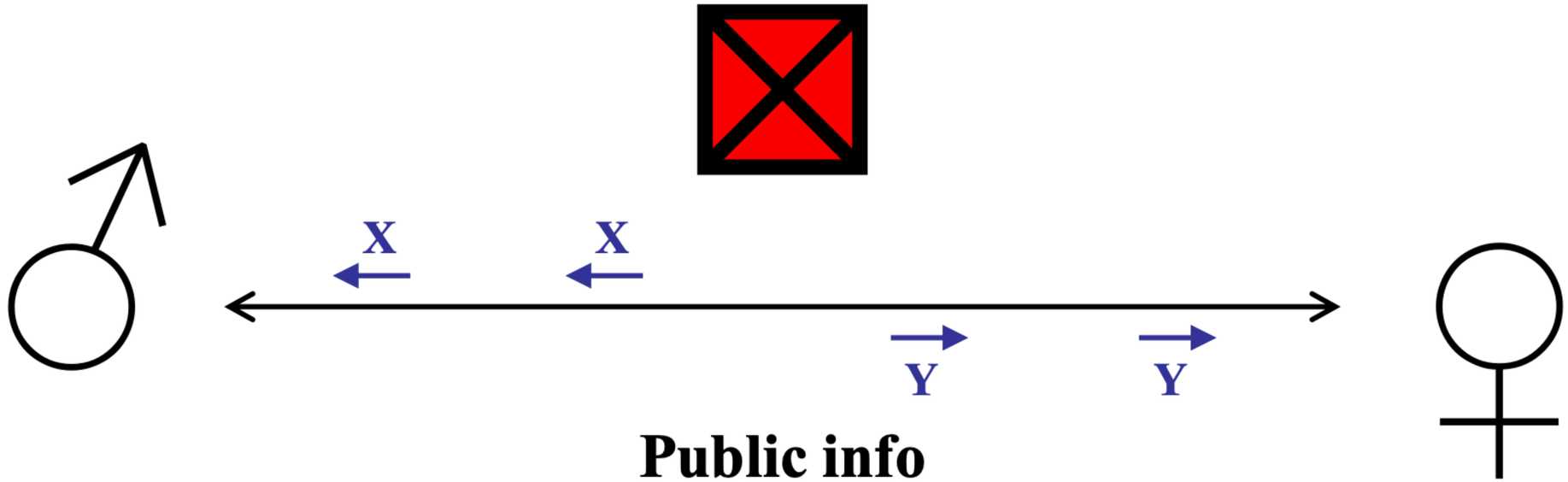


One-way function

$y = f(x)$ easy to compute

$f^{-1}(y) = x$ difficult to determine

Classical Diffie-Hellman (1976)



Public info

m: large prime

$1 < g < m$

$y \in \mathbb{Z}_m$ random

$Y \equiv g^y \bmod m$

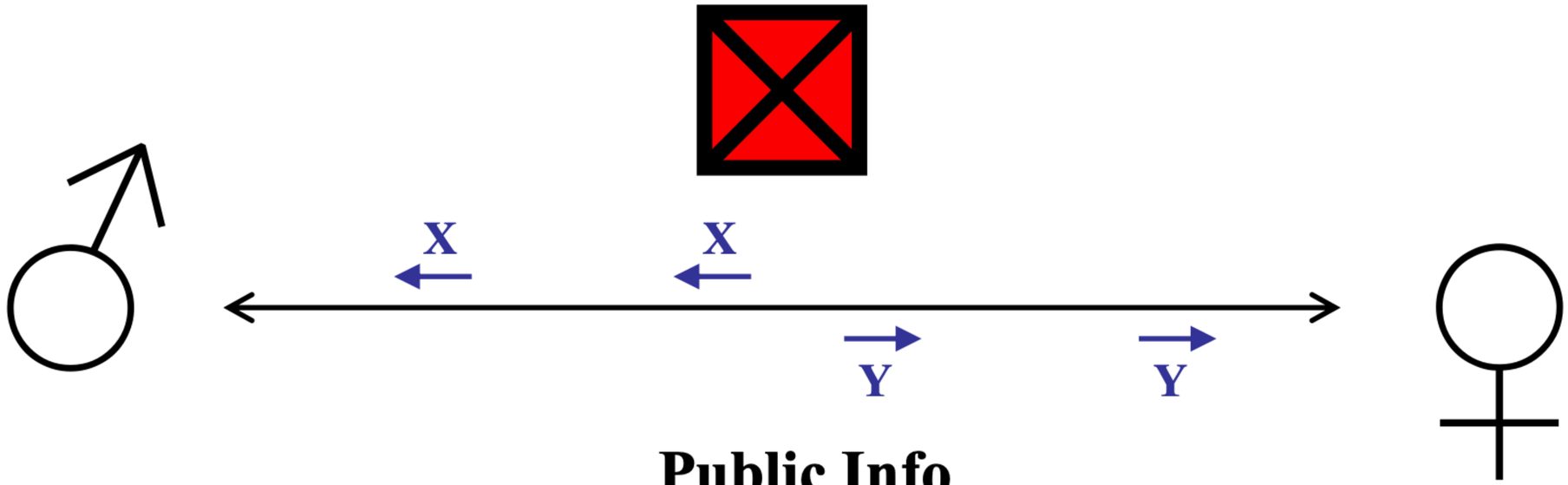
$x \in \mathbb{Z}_m$ random

$X \equiv g^x \bmod m$

$$k' = X^y = (g^x)^y = g^{x\,y} = (g^y)^x = k$$

To Break: Solve discrete log problem

Non-commutative Diffie-Hellman



Public Info

G: non-abelian f.g. group with solvable WP

$g \in G$; $S, T < G$ s.t. $[S, T] = \{1\}$

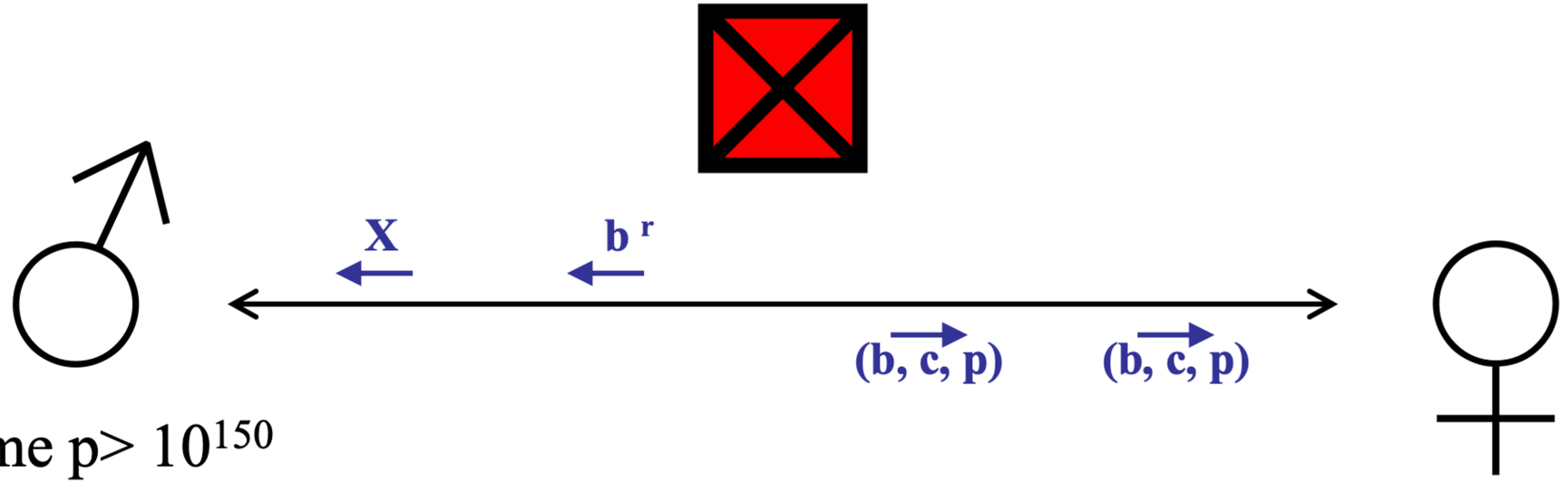
$y \in T$

$Y = g^y = y^{-1}\, g\, y$

$x \in S$

$X = g^x = x^{-1}\, g\, x$

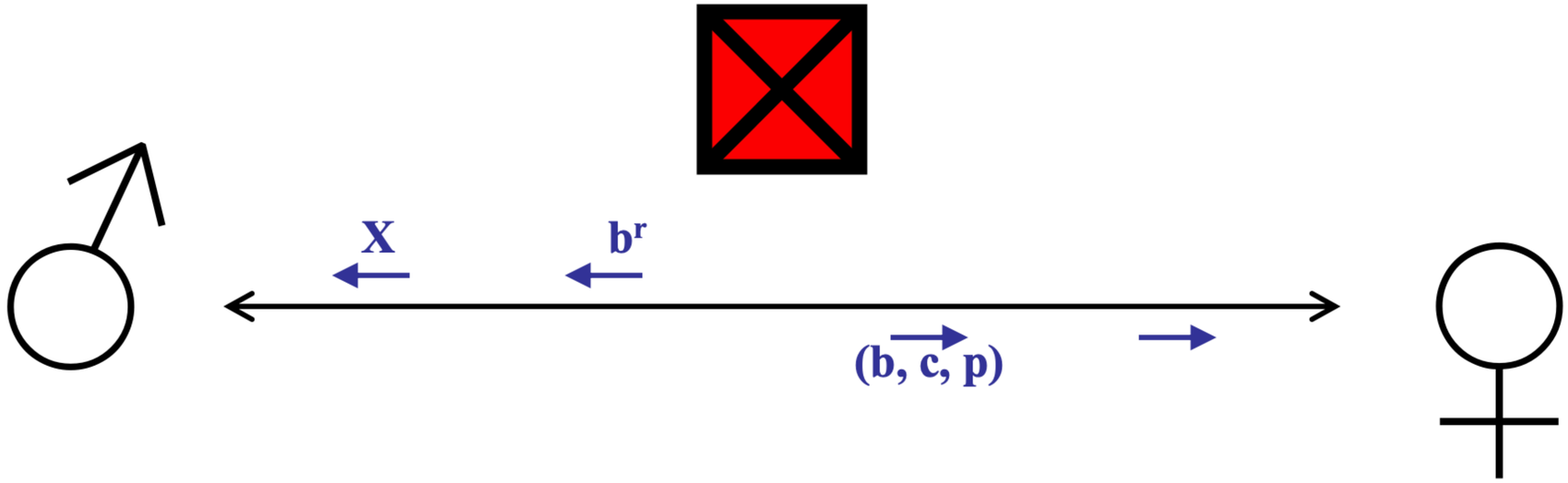
Classical ElGamal



Prime $p > 10^{150}$
Primitive root b mod p
Choose $1<c<p$
$b^l = c \bmod p$
Private key: l

Choose $0<x<p$
$X=(x.c^r) \bmod p$
Header b^r

Classical ElGamal



$(b^r)^l = b^{r.l} = (b^l)^r = c^r \bmod p$

$X.(c^r)^{-1} =$

$x.\ c^r.(c^r)^{-1} = x \bmod p$

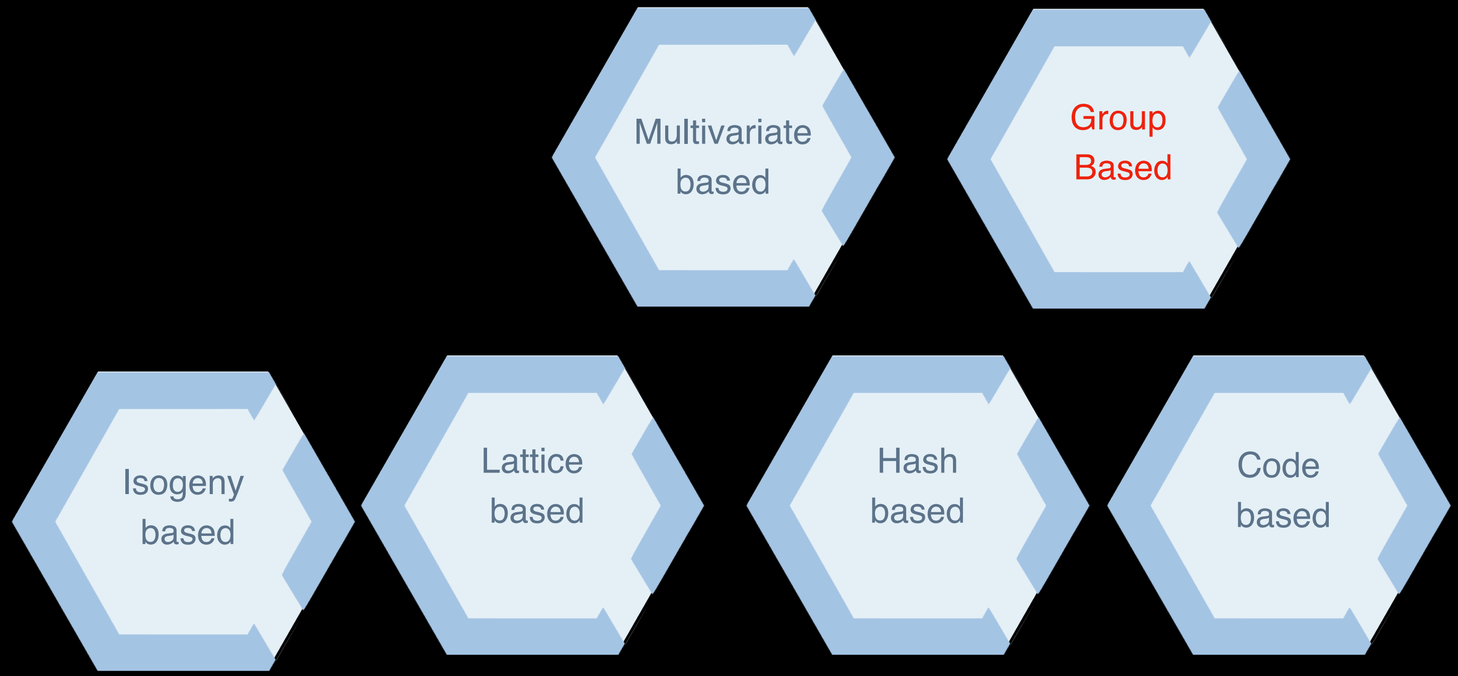
To break: Solve Discrete Logarithm

Given b, c, p $b^x \equiv c \bmod p$

Determine x

Solutions — PQC

Post-Quantum Cryptography : New hard problems secure against the quantum computer



POST-QUANTUM STANDARDIZATION

"Quantum risk is now simply too high and can no longer be ignored" , US NIST, 2016.

ON GOING PROCESS OF NEW QUANTUM RESISTANT CRYPTOGRAPHIC STANDARDS THROUGH NIST

First step of standards : 1 KEM (KYBER) and three DSS (DILITHIUM, FALCON & SPHINCS+)

NIST round 1 - 2016 - 2018

NIST round 2 - 2019 - 2020

NIST round 3 - 2020 - 2022

NIST round 4- 2022

New call for new DSS

A more and more regulated context

- ❑ 01/22 – Memo. on Improving the Cybersecurity of National Security
- ❑ 12/22 – Quantum Computing Cybersecurity Preparedness Act (deadline 2035)
- ❑ 03/2023 – National Cybersecurity Strategy

  Strategic Objective 3.3 : Shift Liability for Insecure Software Products and Services

  Strategic Objective 4.3 : Prepare for Our Post-Quantum Future

TOMAS LINDAHL
Nobel Prize in Chemistry 2015

“Don’t do what everybody else is doing.”

Notices of the American Mathematical Society
ISSN 0002-9920 (print)
ISSN 1088-9477 (online)

FEATURE ARTICLE

May 2023

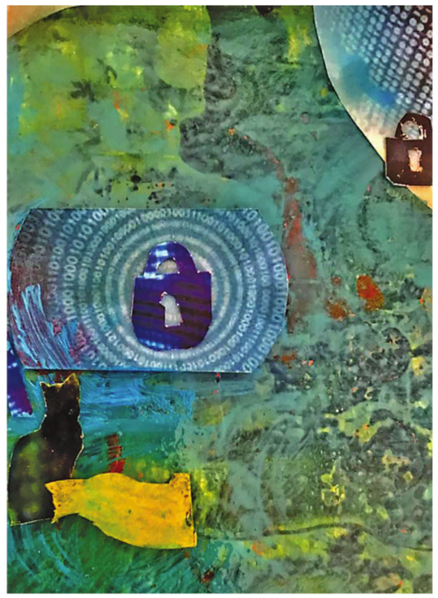
Group-based Cryptography in the Quantum Era

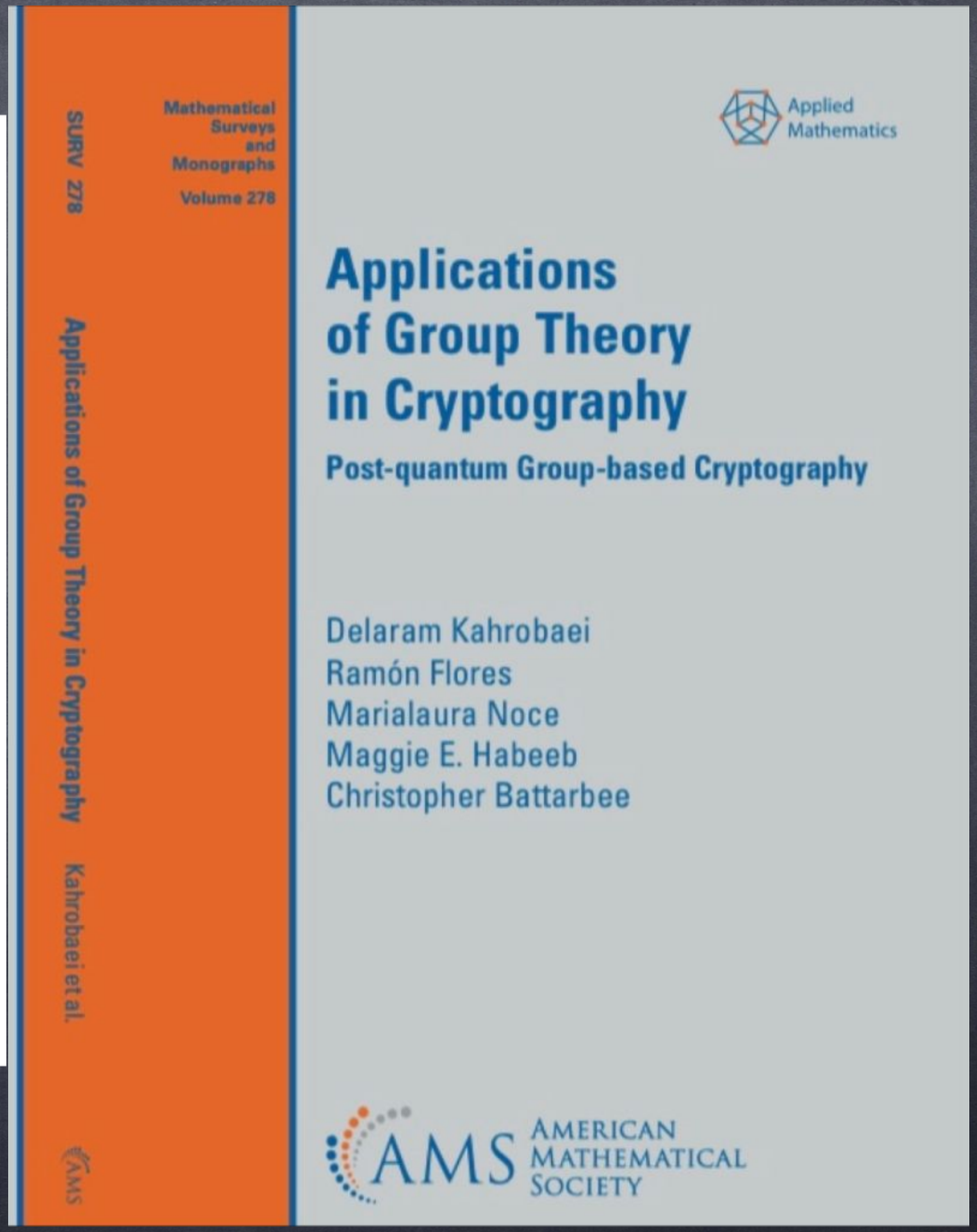
Delaram Kahrobaei
Ramón Flores
Marialaura Noce

Communicated by Notices *Associate Editor Reza Malek-Madani*

1. Introduction

Today's digital infrastructure relies on cryptography in order to ensure the confidentiality and integrity of digital transactions. At the heart of these techniques is public key cryptography, which provides a method for two parties to communicate privately, despite the lack of any pre-arranged security keys.





Motivation for Post-quantum Group-based Cryptography

- Relatively understudied family in post-quantum cryptography with potential due to recent results.
- Diverse roster of computational problems, some proved to be NP-hard.
- The Hidden Subgroup Problem for infinite non-abelian groups has been conjectured to be NP-hard (G. Kuperberg).

Platform Groups for PQC

- Graph (RAAG) Groups: Flores, Kahrobaei, Koberda
- Higher Dimensional Special Linear Groups over Finite fields

(Le Coz, Battarbee, Flores, Koberda, Kahrobaei)

- Simple Groups: Ostrovsky, Skeith, Gonzalez, Kahrobaei, McKemmie
- Arithmetic Groups: Kahrobaei, Mallahi-Karai
- Pro-p Groups, Kahrobaei, Stanojkovski
- Polycyclic Groups: Eick, Kahrobaei
- Automaton Groups: Grigorchuk, Grigoriev, Noce, Kahrobaei, Rodaro
- Hyperbolic Groups: Chatterji, Kahrobaei, Lu
- Nilpotent Groups: Kahrobaei, Tortora, Tota
- Engel Groups: Kahrobaei, Noce
- Free nilpotent p-groups: Kahrobaei, Shpilrain
- Small Cancellation Groups: Habeeb, Kahrobaei, Shpilrain
- Free Metabelian Groups: Shpilrain, Zapata, , Kahrobaei, Habeeb
- Semigroup of Matrices over Group-Rings: Kahrobaei, Koupparis, Shpilrain

- Linear: Groups: Baumslag, Fine, Xu
- Braid Groups: Anshel-Anshel-Goldfeld,Ko-Lee
- Grigorchuk Groups: Petrides
- Groups of Matrices: Grigoriev, Ponameranco
- Thompson: Groups: Shpilrain, Ushakov

Algorithmic Group Theoretic Problems used in Cryptography

- Discrete Logarithm Problem
- Subgroup Isomorphism Problem
- Group Homomorphism Problem
- Root Extraction Problem
- Conjugacy Search Problem
- Power Conjugacy Search Problem
- Word Decision Problem
- Endomorphism Search Problem
- Decomposition Search Problem
- Subgroup membership Problem
- Distorted Subgroup
- Geodesic Length Problem