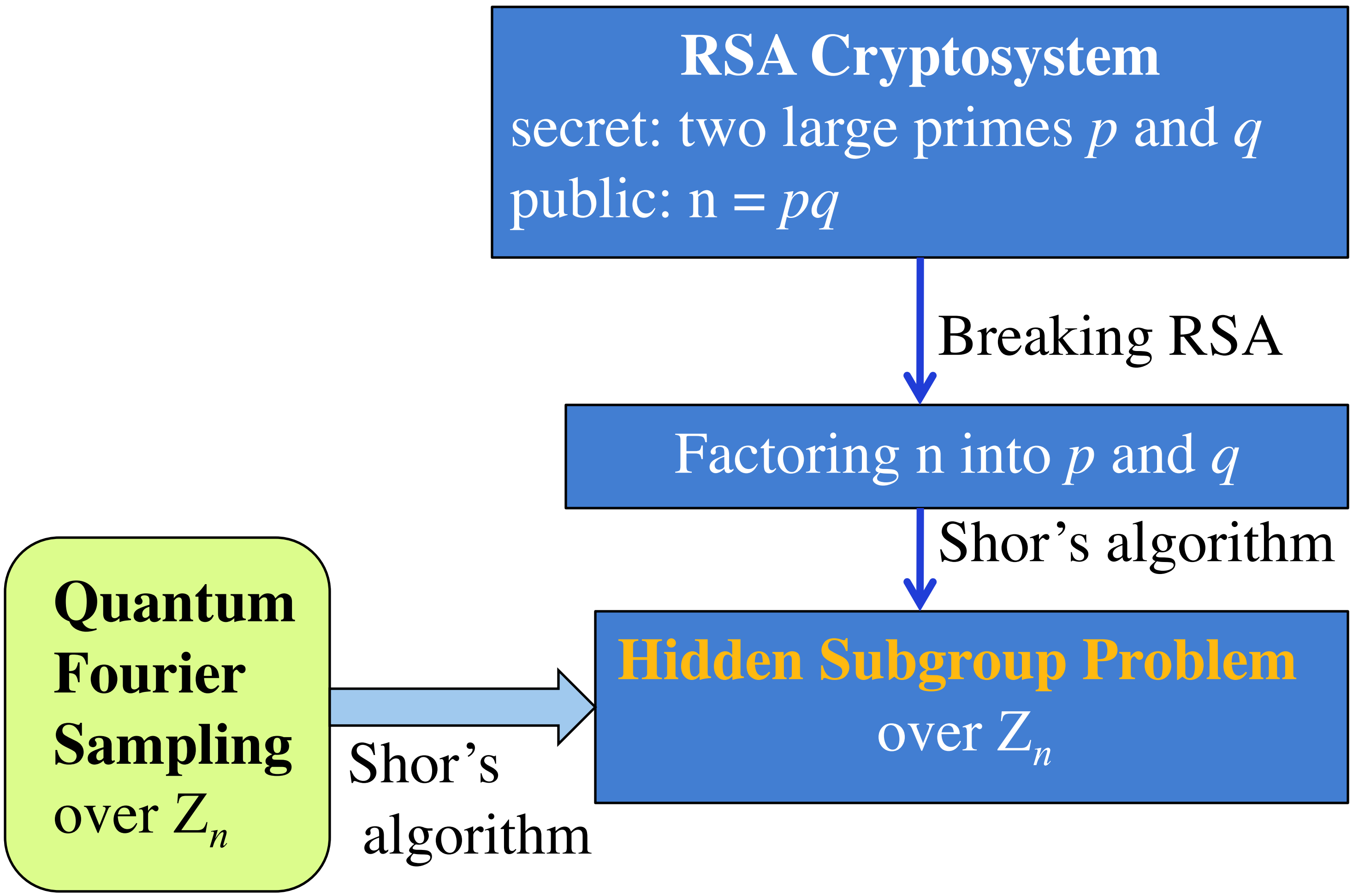
The McEliece Cryptosystem Resists Quantum Fourier Sampling Attack

Hang Dinh
Indiana University South Bend

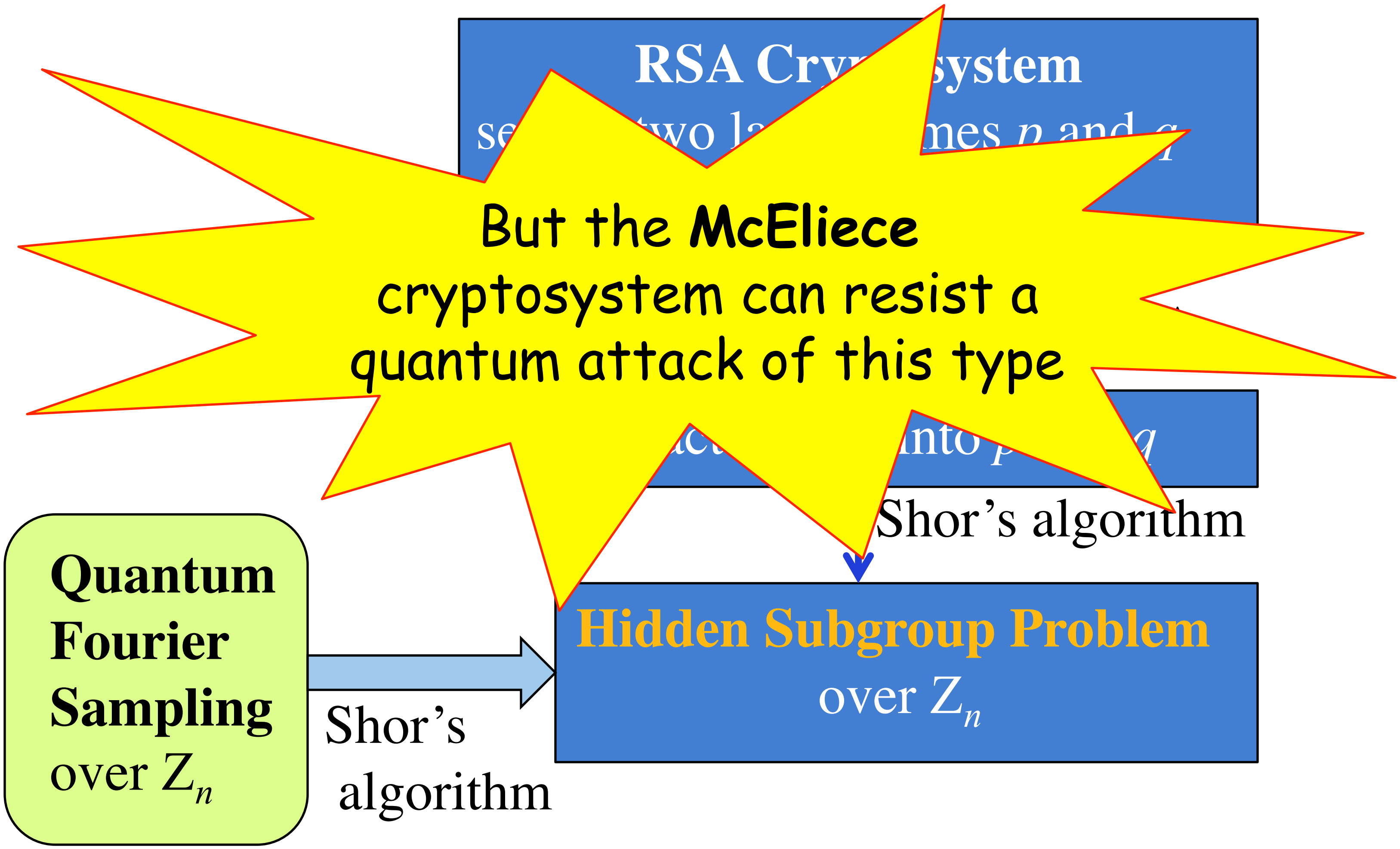
Cristopher Moore
University of New Mexico

Alexander Russell
University of Connecticut

How RSA is Attacked by Quantum Computers



How RSA is Attacked by Quantum Computers



Hidden Subgroup Problem (HSP)

- HSP over a finite group G:
  - Input: function $f : G \rightarrow \{$■,■, …$\}$ that *distinguishes* the left cosets of an unknown subgroup $H < G$

  - Output: H
- Notable reductions to HSP:
  - Simon's problem reduces to HSP over $(Z_2)^n$
  - Shor's factorization reduces to HSP over Z_n
  - Graph Isomorphism reduces to HSP over S_n with $|H| \leq 2$

Quantum Fourier Sampling (QFS)

QFS over G to find hidden subgroup H:

Initial state

Use f

coset state

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle, \text{ for a random } g \in G$$

Quantum Fourier transform

$$\sum_{\rho,i,j} \left(\rho(gH)\right)_{ij} |\rho, i, j\rangle$$

block matrix

Measure

weak → ρ

strong → ρ | i, j

The McEliece Cryptosystem

- Introduced in 1978 by Robert McEliece
- Based on error-correcting codes
  - decoding a general linear code is NP-hard.

- Long keys → require large storage
  - In 1978, not practical: 8KB RAM = $125 ☹
  - In 2011, no problem!: 2GB RAM = $30 ☺

- Considered secure classically
  - use binary Goppa codes, with good choice of parameters
  - leading candidate for post-quantum cryptography

The McEliece Cryptosystem
Key Generation

- Choose a secret linear code C
  - q-ary $[n,k]$-code that can correct t errors
- Private key:
  - M: $k \times n$ generator matrix of C
  - P: $n \times n$ random permutation matrix
  - S: $k \times k$ random invertible matrix over F_q
- Public key: (t, M*)

$$M^* = SMP$$

Scramble (S) — Permute (P)

A QFS Attack on McEliece Private Key

Given: M and M* = SMP → Recover: S and P

↓

Hidden Shift Problem over $GL_k(F_q) \times S_n$ with a hidden shift (S^{-1}, P)

↓

HSP over wreath product $(GL_k(F_q) \times S_n) \wr Z_2$ with a hidden subgroup H characterized by

- automorphism group $Aut(C)$ of the code C
- column rank r of M

nonabelian group

$$|H| \leq 2|Aut(C)|^2 q^{2k(k-r)}$$

How Strong is QFS?

- QFS over abelian groups
  - can be computed efficiently by quantum computers
  - That's how RSA is attacked!
- Recall:
  - the QFS attack on McEliece is over a nonabelian group
- Does QFS work over nonabelian groups?
  - Can QFS efficiently distinguish the conjugates of H from each other or from the trivial hidden subgroup?
  - No, in some cases.

Limitations of QFS over Symmetric group S_n

- Moore-Russell-Schulman, 2008
  - Strong QFS fails for any subgroup $H < S_n$ with $|H|=2$

- Kempe-Pyber–Shalev, 2007
  - Weak QFS fails for any subgroup $H < S_n$ unless H has constant minimal degree

the minimal number of points moved by a non-identity permutation in H

Our Results

- Strong QFS can't resolve the HSP reduced from the attack on McEliece private key if the secret code C is
  - well-permuted: $Aut(C)$ has large minimal degree and small order
  - well-scrambled: generator matrix M has large rank
  - Example:
    - rational Goppa code (generalized Reed-Solomon code)

Warning: This neither rules out other attacks nor violates a natural hardness assumption.

classically attacked by Sidelnokov-Shestakov: given M*=SMP, determine S and MP.

Our Results

- Strong QFS fails over S_n
  - even with hidden subgroups H of order > 2
    - extend Moore-Russell-Schulman's result
  - unless the minimal degree of H is $O(\log |H|)+O(\log n)$
    - prove a Kempe-Pyber–Shalev's version for strong QFS, though weaker in the upper bound on the minimal degree

- Strong QFS fails over $\mathrm{GL}_2(\mathrm{F}_q)$ if
  - H contains no non-identity scalar matrices, and $|H|=O(q)$
  - Example: H is generated by $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$

Key Points of Our Proofs

- Generalize Moore-Russell-Schulman's framework
  - to upper-bound distinguishability of a subgroup $H<G$ by strong QFS over G.
  - Moore-Russell-Schulman's framework: $|H|=2$
  - Our framework: $|H| \geq 2$

difference between information extracted by strong QFS for a random conjugate of H and that for the trivial subgroup.

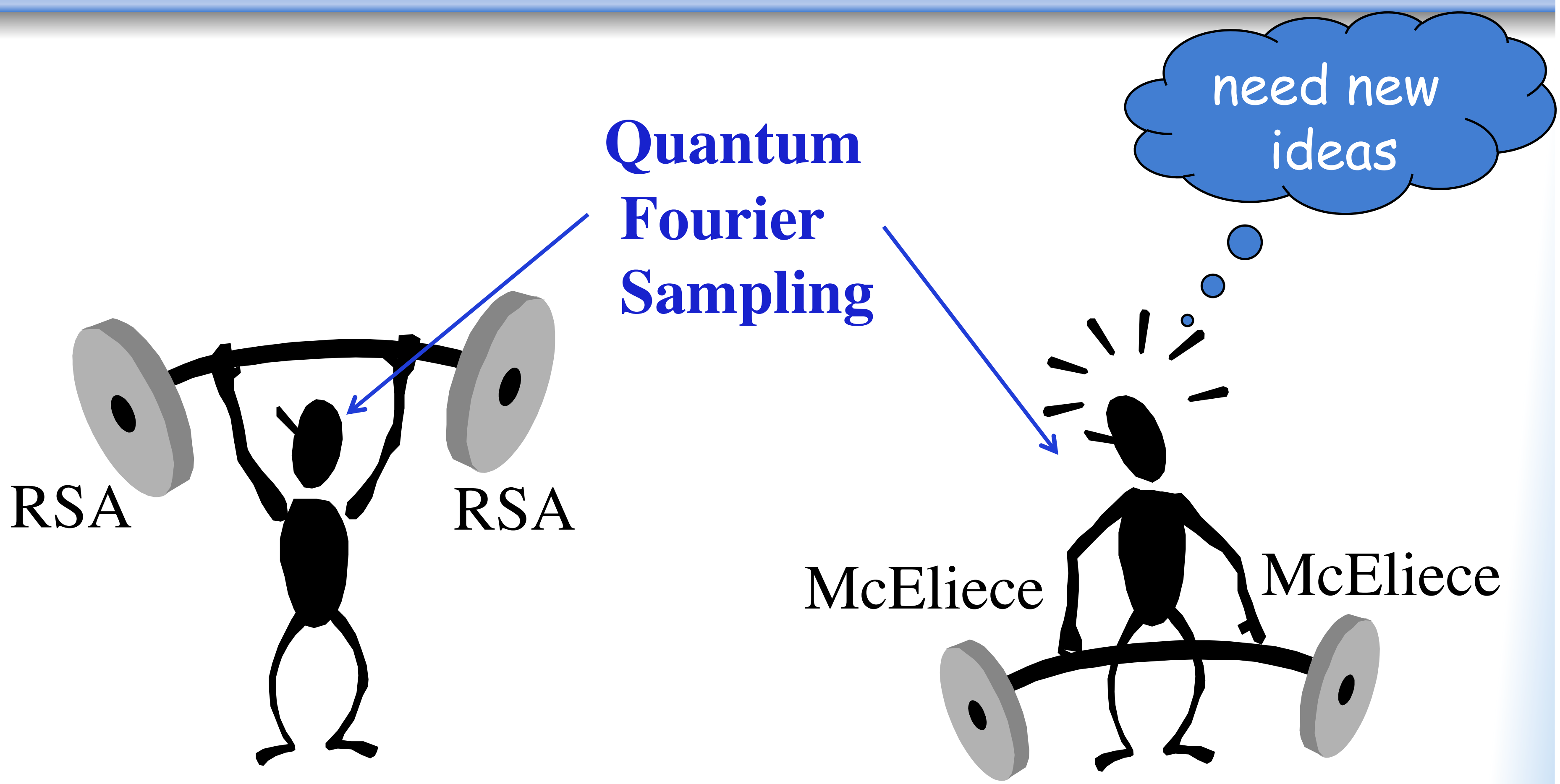
Key Points of Our Proofs

- Apply our general framework to
  - the HSP reduced from the McEliece cryptosystem
    → upper bound depending on
    - minimal degree of $Aut(C)$
    - order of $Aut(C)$
    - column rank of secret generator matrix M

Well-permuted, well-scrambled codes give good bounds

  - S_n and $\mathrm{GL}_2(\mathrm{F}_q)$

Conclusion



need new ideas
Quantum Fourier Sampling
RSA
RSA
McEliece
McEliece

Open Questions

- What are other linear codes that are well-permuted and well-scrambled?

- Can McEliece cryptosystem resist multiple-register QFS attacks?
  - Hallgren et al., 2006: subgroups of order 2 require highly-entangled measurements of many coset states.
  - Does this hold for subgroups of order > 2?

Questions?

Thank you!