McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks

<u>Hang Dinh</u>

Indiana University South Bend

joint work with

Cristopher Moore

University of New Mexico

Alexander Russell

University of Connecticut

Post-quantum cryptography

- Shor's quantum algorithms for Factoring and Discrete Logarithm break RSA, ElGamal, elliptic curve cryptography...

- Are there "post-quantum" cryptosystems?
    - cryptosystems we can carry out with classical computers
        - [unlike quantum cryptosystems, which require quantum facility]
    - which will remain secure even if and when quantum computers are built.

Post-quantum cryptography

- Candidates for post-quantum cryptosystems:
  - lattice-based
  - code-based (the McEliece system and its relatives)
  - hash-based
  - multivariate
  - secret-key cryptography
- Bernstein, 2009:
  - These systems are *believed* to resist quantum computers.
  - "*Nobody has figured out a way to apply Shor's algorithm to any of these systems.*"

We show that

some McEliece and Niederreiter cryptosystems resist the natural analog of Shor's quantum attack.

How Shor's algorithm works

Breaking RSA private key

Integer Factorization

Hidden Subgroup Problem
over a cyclic group Z_N

Quantum Fourier Sampling
over Z_N

Breaking ElGamal, elliptic curve cryptography

Discrete Logarithm

Hidden Subgroup Problem
over an abelian group $Z_N \times Z_N$

Quantum Fourier Sampling
over $Z_N \times Z_N$

Hidden Subgroup Problem (HSP)

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

H	g_2H	g_3H	…	g_kH

  - Output: H
- Notable reductions to nonabelian HSP:
  - Unique Shortest Vector Problem → HSP over D_n [Regev'04]
  - Graph Isomorphism → HSP over S_n with $|H| \leq 2$

Quantum Fourier Sampling (QFS)

QFS over G to find hidden subgroup H:

Uniform superposition over G

Use input function f

random coset state $|gH\rangle$

uniform superposition over coset gH

Quantum Fourier transform

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

block matrix corresponding to irreducible representation ρ of G

Measure

weak: ρ

strong: ρ | column j

McEliece/Niederreiter Cryptosystems

- Private key:
  - M: $k \times n$ matrix over a finite field F_{q^l} containing F_q
  - P: $n \times n$ random permutation matrix
  - S: $k \times k$ random invertible matrix over F_q
- Public key includes the matrix

$$M^* = SMP$$

Scramble M's rows

Permute M's columns

McEliece/Niederreiter Cryptosystems

McEliece system	Niederreiter system
• $\mathrm{F}_q = \mathrm{F}_{q^l} (l = 1)$ • M is a generator matrix of an $[n, k]$-code over F_q. • Originally used classical binary Goppa codes (q=2)	• $\mathrm{F}_q \subseteq \mathrm{F}_{q^l} (l \geq 1)$ • M is a parity check matrix of an $[n, k']$-code C over F_q. • Equivalent to the McEliece system using C, if $k' = n - lk$. • Originally used rational Goppa codes (GRS codes)

Security of McEliece and Niederreiter Systems

- Two basic types of attacks
  - Decoding attacks [previous talk]
  - Attacks on private key [this talk]
    - Recover S, M, P from M*
- Security against known classical attacks
  - Still secure if using classical Goppa codes [EOS'07]
  - Broken if using rational Goppa codes (*Ouch*!)
    - Sidelnokov & Shestakov's attack factors SMP into S and MP.

McEliece/Niederreiter's security reduces to HSP

Scrambler-Permutation Problem

- Given: M and M* = SMP for some $(S, P) \in GL_k(F_q) \times S_n$
- Find: S and P

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

- the column rank of matrix M, and
- the *automorphism group* of M:

$$Aut(M) = \{P \in S_n \mid \exists S \in GL_k(F_q): SMP=M\}$$

Can this HSP be solved by strong QFS?

Our Answer (1)

- Strong QFS yields negligible information about hidden (S, P) if M is *good*, meaning
  - M has column rank $r \geq k - o(\sqrt{n})/l$,
  - $|Aut(M)| \leq e^{o(n)}$, and
  - Minimal degree of $Aut(M)$ is $\Omega(n)$.

the minimal number of points moved by a non-identity permutation in $Aut(\mathrm{M})$

- Next question:
  - Are there matrices M satisfying the conditions above?

Our Answer (2)

- Matrix M is good if it is of the form:

$$M = S\begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{bmatrix}$$

$$S \in \mathrm{GL}_k(\mathrm{F}_{q^l}),$$
$$v_i \in \mathrm{F}_{q^l} - \{0\},$$
$$\alpha_i \in \mathrm{F}_{q^l} \cup \{\infty\},$$
$$\alpha_i\text{'s are distinct.}$$

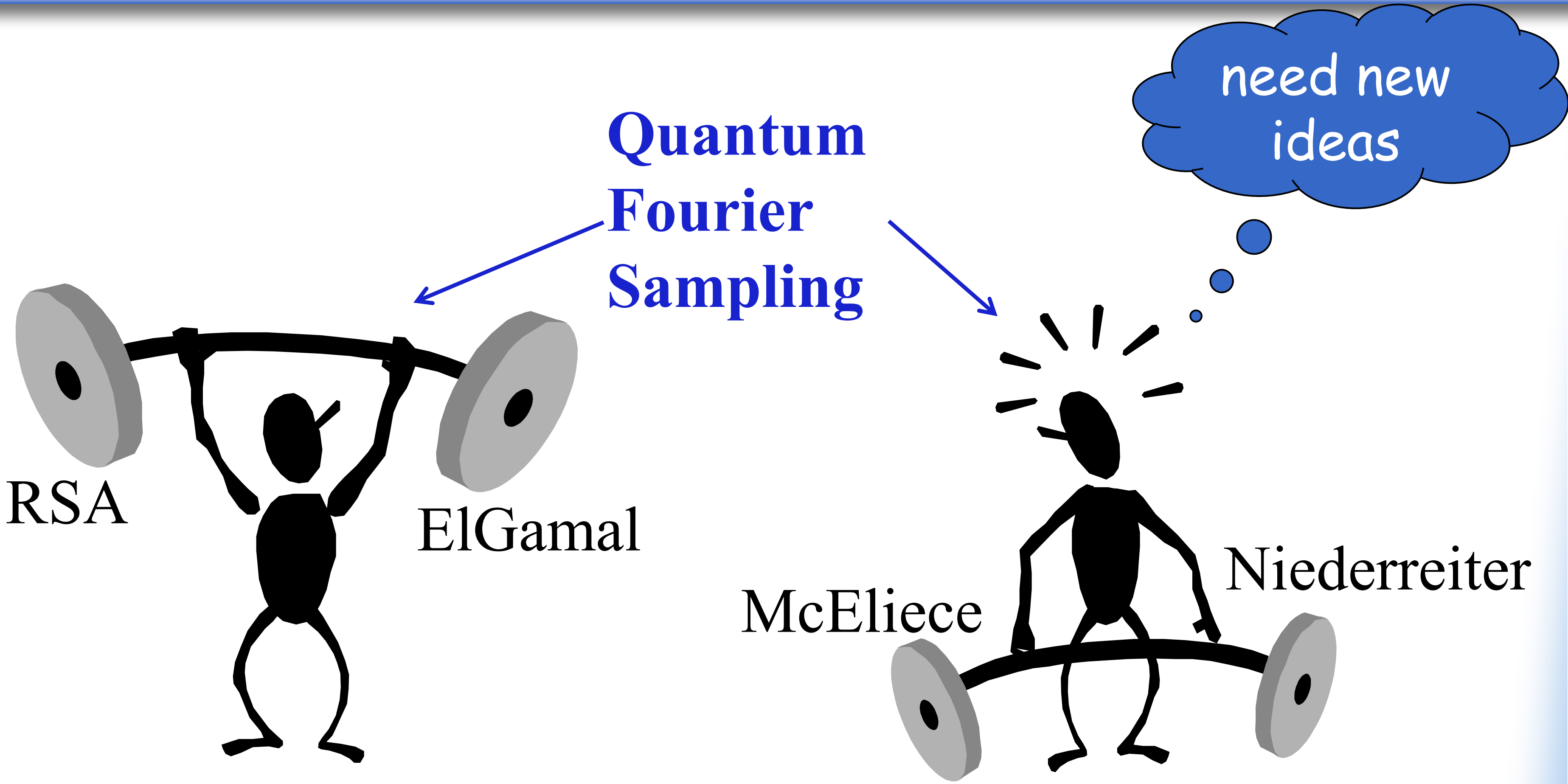
- In particular, these are
  - generator matrices of rational Goppa $[n, k]$-codes over F_{q^l}.
  - parity check matrices of classical Goppa codes of length n over subfield F_q.

Conclusion

- The following cryptosystems resist the natural analog of Shor's QFS attack:
  - McEliece systems using rational Goppa codes
  - Niederreiter systems using classical Goppa codes.
  - In general, any McEliece/Niederreiter system using linear codes with *good* generator/parity check matrices.

Warning: This neither rules out other quantum (or classical) attacks nor violates a natural hardness assumption.

Conclusion (Moral)



Open Questions

- What are other linear codes that possess good generator/parity check matrices?

- Can these cryptosystems resist stronger quantum attacks, e.g., 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 all for staying till the last minute!*

Parameters

- In case of Niederreiter systems using a classical q-ary Goppa code C, we need

$$q^{k^2} \leq n^{0.2n} \text{ and } q^{3l} \leq \mathrm{e}^{o(n)}$$

- Typically, $n = q^l$, then we only need $k^2 \leq 0.2nl$,
  - which implies C must have large dimension:

$$\dim C \geq n - kl \geq n - \sqrt{0.2n}\, l^{3/2}$$