Code-based cryptography VI

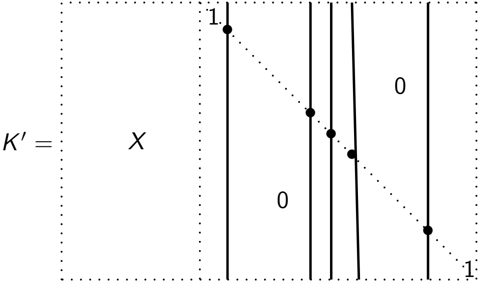
Quantum information-set decoding

Tanja Lange
with some slides by Tung Chou and Christiane Peters

Eindhoven University of Technology

SAC – Post-quantum cryptography

Generic attack: Information-set decoding, 1962 Prange

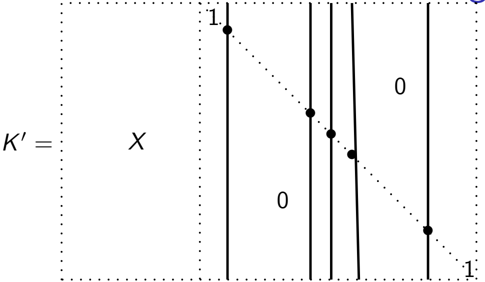


$\mathbf{s}' = K'\mathbf{e}'$

How to apply Grover to this?

1. Permute K and bring to systematic form $K' = (X|I_{n-k})$. (If this fails, repeat with other permutation).
2. Then $K' = UKP$ for some permutation matrix P and U the matrix that produces systematic form.
3. This updates $\mathbf{s}$ to $U\mathbf{s}$.
4. If $\mathrm{wt}(U\mathbf{s}) = t$ then $\mathbf{e}' = (00\ldots0)||U\mathbf{s}$. Output unpermuted version of $\mathbf{e}'$.
5. Else return to 1 to rerandomize.

Quantum information-set decoding. 2010 Bernstein



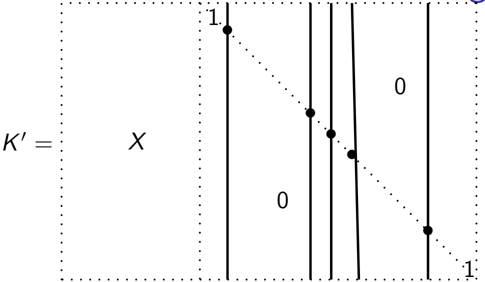
$\mathbf{s}' = K'\mathbf{e}'$

How to apply Grover to this?

1. Permute K and bring to systematic form $K' = (X|I_{n-k})$. (If this fails, repeat with other permutation).
2. Then $K' = UKP$ for some permutation matrix P and U the matrix that produces systematic form.
3. This updates $\mathbf{s}$ to $U\mathbf{s}$.
4. If $\mathrm{wt}(U\mathbf{s}) = t$ then $\mathbf{e}' = (00\ldots0)||U\mathbf{s}$. Output unpermuted version of $\mathbf{e}'$.
5. Else return to 1 to rerandomize.

Turn all this into function f on selected positions, return 0 iff $\mathrm{wt}(U\mathbf{s}) = t$ and 1 otherwise. E.g. output qubit gets ORed with 1 at failure.

Quantum information-set decoding. 2010 Bernstein



$\mathbf{s}' = K'\mathbf{e}'$

Function f is on size $\binom{n}{k}$ search space with $\binom{n}{t}$ roots.
Generalized Grover handles this in $\sqrt{\binom{n}{k}/\binom{n}{t}}$ iterations.

1. Permute K and bring to systematic form $K' = (X|I_{n-k})$. (If this fails, repeat with other permutation).
2. Then $K' = UKP$ for some permutation matrix P and U the matrix that produces systematic form.
3. This updates $\mathbf{s}$ to $U\mathbf{s}$.
4. If $\mathrm{wt}(U\mathbf{s}) = t$ then $\mathbf{e}' = (00\dots0)||U\mathbf{s}$. Output unpermuted version of $\mathbf{e}'$.
5. Else return to 1 to rerandomize.

Turn all this into function f on selected positions, return 0 iff $\mathrm{wt}(U\mathbf{s}) = t$ and 1 otherwise. E.g. output qubit gets ORed with 1 at failure.

Quantum speedups for faster ISD

- Extend function f to include (all) combinations for searching in X.
- This increases the cost for the function evaluation.
- The square-root speedup applies to the number of iterations, i.e., the outer loop.
- Can rebalance inner and outer loop to optimize, e.g., choose a smaller value for p.

Quantum speedups for faster ISD

- Extend function f to include (all) combinations for searching in X.
- This increases the cost for the function evaluation.
- The square-root speedup applies to the number of iterations, i.e., the outer loop.
- Can rebalance inner and outer loop to optimize, e.g., choose a smaller value for p.
- Quantum walks (not covered in our intro to quantum computing) allow to get quantum speedups also in the inner loops.
- Asymptotic results are often stated for constant ratios k/n, but the case of Goppa codes has $(n - mt)/n$ grow with n.

The McEliece system uses $(c_0 + o(1))\lambda^2(\lg \lambda)^2$-bit keys as $\lambda \to \infty$ to achieve 2^λ security against all attacks known today.
Same $c_0 \approx 0.7418860694$.

Quantum speedups for faster ISD

- Extend function f to include (all) combinations for searching in X.
- This increases the cost for the function evaluation.
- The square-root speedup applies to the number of iterations, i.e., the outer loop.
- Can rebalance inner and outer loop to optimize, e.g., choose a smaller value for p.
- Quantum walks (not covered in our intro to quantum computing) allow to get quantum speedups also in the inner loops.
- Asymptotic results are often stated for constant ratios k/n, but the case of Goppa codes has $(n - mt)/n$ grow with n.

The McEliece system uses $(c_0 + o(1))\lambda^2(\lg \lambda)^2$-bit keys as $\lambda \to \infty$ to achieve 2^λ security against all attacks known today.
Same $c_0 \approx 0.7418860694$.

Replacing λ with 2λ stops all known *quantum* attacks.

See https://classic.mceliece.org for a concrete proposed system.