Algorithms for integer syndrome decoding problem

Vlad-Florin Dragoi[1], Alin-Tiberiu Lacatus[1], Alexandru Popoviciu[2]
vlad.dragoi@uav.ro

Aurel Vlaicu University of Arad Romania

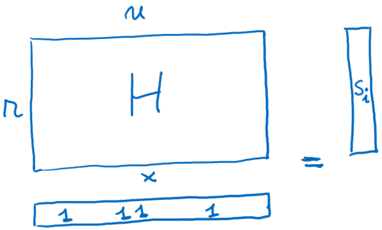
West University of Timisoara

9th International Workshop on Soft Computing Applications
27-29 Nov-2020 Arad, Romania (Virtual)

Given $(H, t, \vec{s})$ where

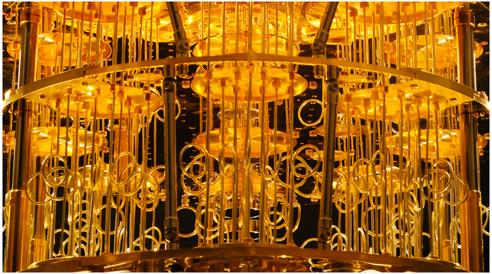
$H \in \{0,1\}^{r \times n}$, $t \in \mathbb{N}$ and $\vec{s} \in \mathbb{N}^r$

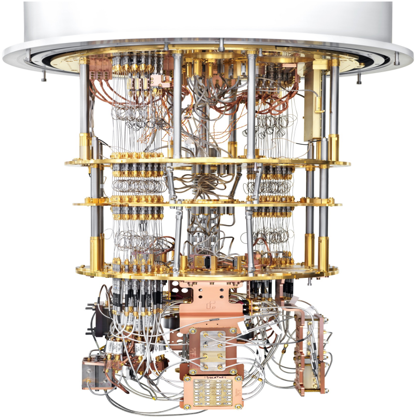
Find $\vec{e} \in \{0,1\}^n$ st. $\begin{cases} H \cdot \vec{e} = \vec{s} \\ \|\vec{e}\|_H \leq t \end{cases}$



Post-quantum Cryptography

Quantum computers could be used for breaking public-key cryptographic schemes [1]





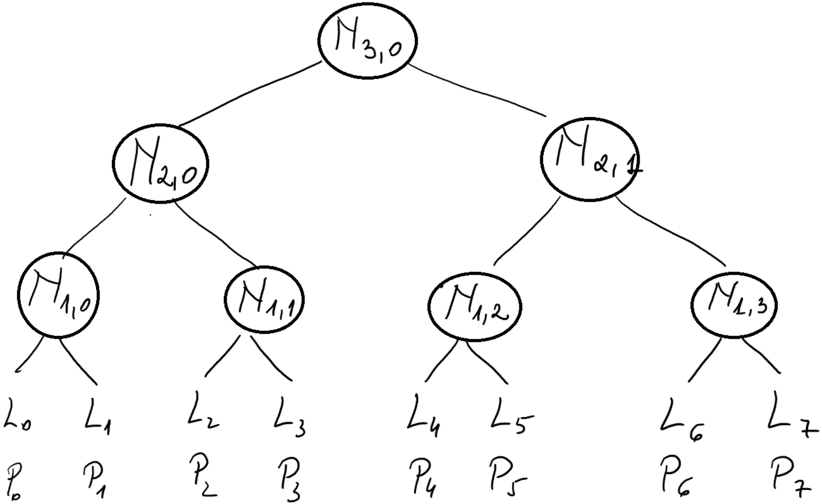
1. 1997. Peter W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer."

Post-quantum Cryptography

NIST proposal [2] – post-quantum cryptography project

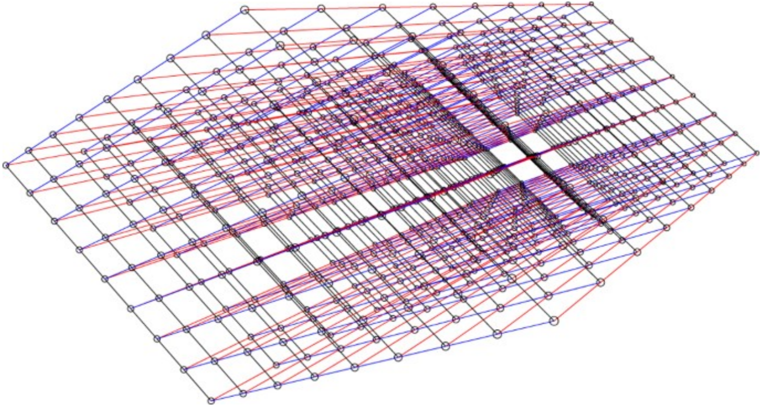
Post-quantum Cryptography

NIST proposal[2] – post-quantum cryptography project



Post-quantum Cryptography

NIST proposal[2] – post-quantum cryptography project



2. http ://csrc.nist.gov/groups/ST/post-quantum-crypto/

Table of contents

Error correcting codes

Definition 1

A q-ary linear code $\mathscr{C}$ *defined over* $\mathbb{F}_q$*, of length* n *is a* k *dimension sub-vector space of* $\mathbb{F}_q^n$*.*

Error correcting codes

Definition 1

A q-ary linear code $\mathscr{C}$ defined over $\mathbb{F}_q$, of length n is a k dimension sub-vector space of $\mathbb{F}_q^n$.

Definition 2 (Hamming weight and distance)

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ *and* $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$

$$|\boldsymbol{x}|_H \stackrel{def}{=} |\{i \mid x_i \neq 0\}| \quad \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} |\{i \mid x_i \neq y_i\}|$$

Error correcting codes

Definition 1

A q-ary linear code $\mathscr{C}$ defined over $\mathbb{F}_q$, of length n is a k dimension sub-vector space of $\mathbb{F}_q^n$.

Definition 2 (Hamming weight and distance)

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$

$$|\boldsymbol{x}|_H \stackrel{def}{=} |\{i \mid x_i \neq 0\}| \quad \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} |\{i \mid x_i \neq y_i\}|$$

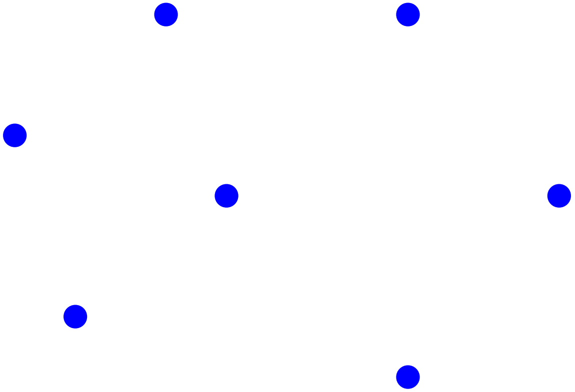
Example

Let $q = 2$ and $\boldsymbol{x} = (1, 0, 0, 1, 0)$, $\boldsymbol{y} = (1, 0, 0, 1, 1)$.
Then

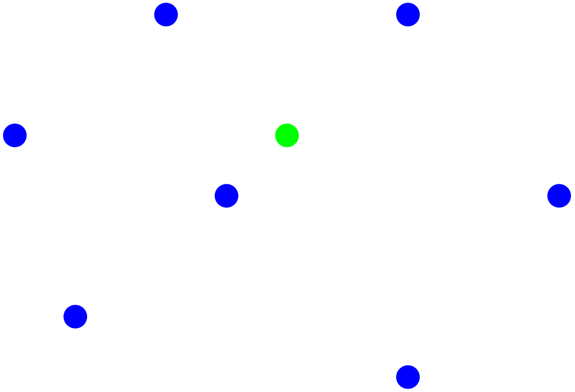
$$|\boldsymbol{x}|_H = 2 \quad \text{et} \quad \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) = 1$$

Complete decoding

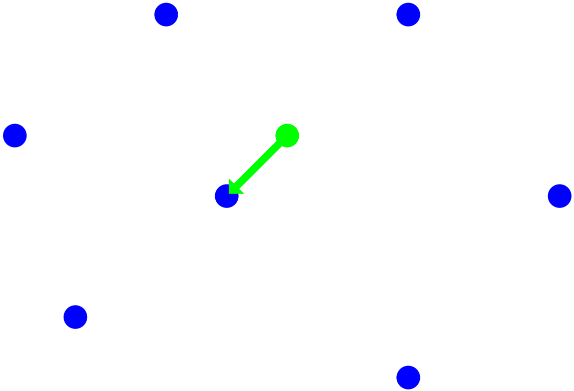
Complete decoding



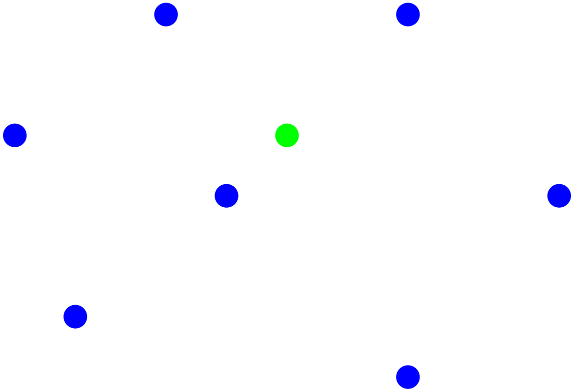
Complete decoding



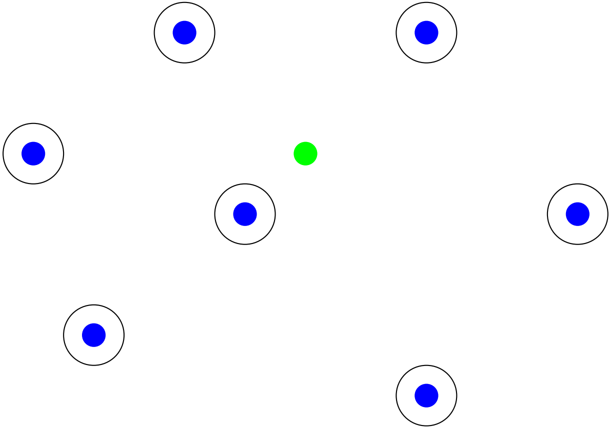
Complete decoding



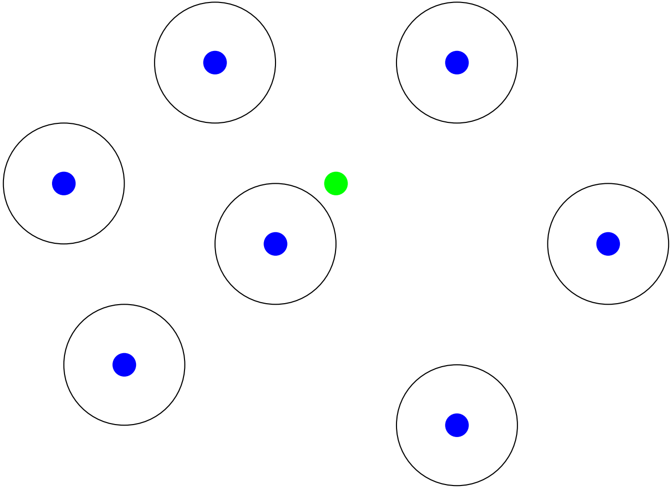
Bounded decoding



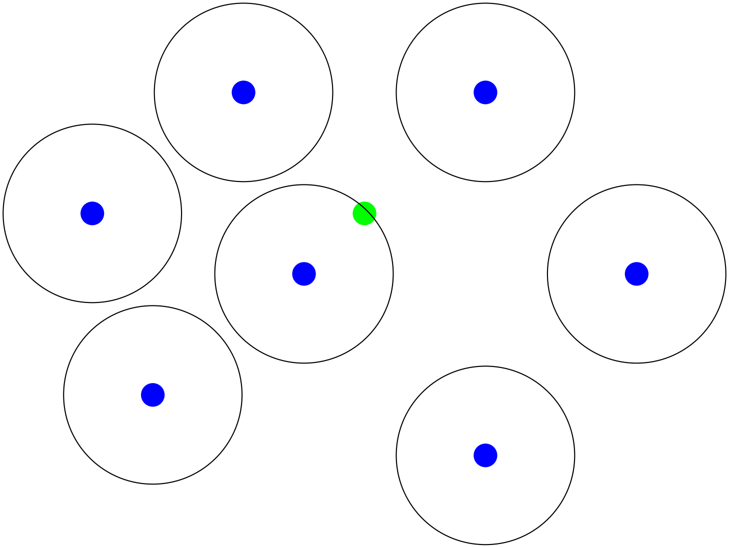
Bounded decoding



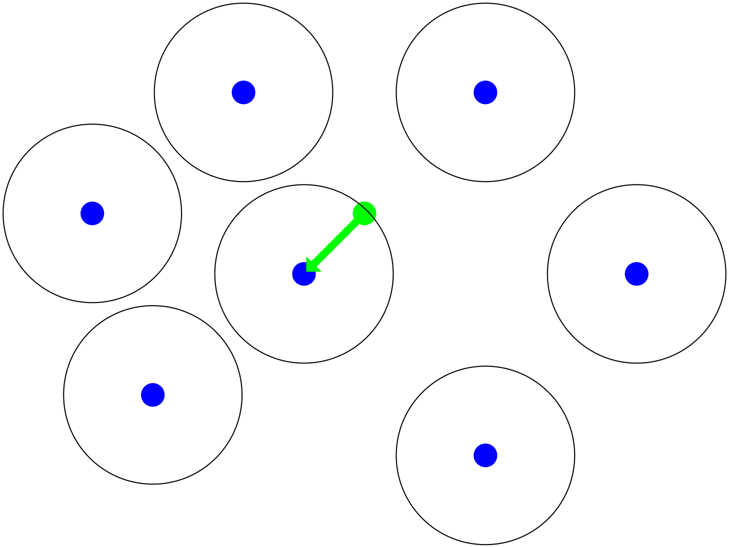
Bounded decoding



Bounded decoding



Bounded decoding



Syndrome decoding [3]

Definition 1 (SDP)

Instance : $\boldsymbol{H} \in \mathcal{M}_{n-k,n}\left(\mathbb{F}_2\right), \boldsymbol{s} \in \mathbb{F}_2^{n-k}, t \in \mathbb{Z}^+$

Question : Is there a vector $\boldsymbol{x} \in \mathbb{F}_2^n$ of weight $\leq t$, such that $\boldsymbol{Hx} = \boldsymbol{s}$?

3. 1978. Berlekamp E., McEliece R.J., Van Tilborg "On the inherent intractability of certain coding problems."

Syndrome decoding[3]

Definition 1 (SDP)

Instance : $\boldsymbol{H} \in \mathcal{M}_{n-k,n}\left(\mathbb{F}_2\right), \boldsymbol{s} \in \mathbb{F}_2^{n-k}, t \in \mathbb{Z}^+$

Question : Is there a vector $\boldsymbol{x} \in \mathbb{F}_2^n$ of weight $\leq t$, such that $\boldsymbol{Hx} = \boldsymbol{s}$?

Number of solutions of the SDP – unique for t smaller than the Gilbert-Varshamov bound

3. 1978. Berlekamp E., McEliece R.J., Van Tilborg "On the inherent intractability of certain coding problems."

Syndrome decoding[3]

Definition 1 (SDP)

Instance : $\boldsymbol{H} \in \mathcal{M}_{n-k,n}(\mathbb{F}_2)$, $\boldsymbol{s} \in \mathbb{F}_2^{n-k}$, $t \in \mathbb{Z}^+$

Question : Is there a vector $\boldsymbol{x} \in \mathbb{F}_2^n$ of weight $\leq t$, such that $\boldsymbol{Hx} = \boldsymbol{s}$?

Number of solutions of the SDP – unique for t smaller than the Gilbert-Varshamov bound

GV Bound

Given n, k the Gilbert-Varshamov distance is the largest d_{GV} s.t.

$$|\mathcal{B}(0, d_{GV} - 1)| \leq 2^{n-k} \tag{1}$$

$\mathcal{B}(\boldsymbol{x}, t) = \{yv \in \mathbb{F}_2^n | d(\boldsymbol{x}, \boldsymbol{y}) \leq t\}$ - n-dimensional ball of radius r centered in $\boldsymbol{x}$.

3. 1978. Berlekamp E., McEliece R.J., Van Tilborg "On the inherent intractability of certain coding problems."

Neiderreiter cryptosystem

Key Generation

1. Choose $\mathscr{C}$ a t-error corecting code ($\boldsymbol{H}$ -parity-check matrix)
2. Mask the structure by $\boldsymbol{S}$ and $\boldsymbol{P}$,

$$\boldsymbol{H}_{pub} = \boldsymbol{SHP} \tag{2}$$

Neiderreiter cryptosystem

Key Generation

1. Choose $\mathscr{C}$ a t-error corecting code ($\boldsymbol{H}$ -parity-check matrix)
2. Mask the structure by $\boldsymbol{S}$ and $\boldsymbol{P}$,

$$\boldsymbol{H}_{pub} = \boldsymbol{SHP} \tag{2}$$

Encryption

Let $\boldsymbol{m} \in \mathbb{F}_q^k$,

1. Encode $\boldsymbol{m}$ into $\boldsymbol{e} \in \mathbb{F}_q^n$ a random vector of Hamming weight t
2. Encrypt $\boldsymbol{c} = \boldsymbol{H}_{pub}\boldsymbol{e}$

Neiderreiter cryptosystem

Key Generation

1. Choose $\mathscr{C}$ a t-error corecting code ($\boldsymbol{H}$ -parity-check matrix)
2. Mask the structure by $\boldsymbol{S}$ and $\boldsymbol{P}$,

$$\boldsymbol{H}_{pub} = \boldsymbol{SHP} \tag{2}$$

Encryption

Let $\boldsymbol{m} \in \mathbb{F}_q^k$,

1. Encode $\boldsymbol{m}$ into $\boldsymbol{e} \in \mathbb{F}_q^n$ a random vector of Hamming weight t
2. Encrypt $\boldsymbol{c} = \boldsymbol{H}_{pub}\boldsymbol{e}$

Decryption

1. Compute $\boldsymbol{z}^* = \boldsymbol{S}^{-1}\boldsymbol{z}$ $\qquad \boldsymbol{z}^* = \boldsymbol{HPe}$
2. Compute $\boldsymbol{e}^* = Decode_{\boldsymbol{H}}(\boldsymbol{z}^*)$ $\qquad \boldsymbol{e}^* = \boldsymbol{Pe}$
3. Retreive $\boldsymbol{m}$ from $\boldsymbol{P}^{-1}\boldsymbol{e}^*$

Message recovery using fault injection

- Attack the message at the encryption level

Message recovery using fault injection

- Attack the message at the encryption level
- Bit-swapping by laser injection changes the **XOR** into **ADD**

Message recovery using fault injection

- Attack the message at the encryption level
- Bit-swapping by laser injection changes the **XOR** into **ADD**
- The rezulting syndrome gives larger quantity of information

Message recovery using fault injection

- Attack the message at the encryption level
- Bit-swapping by laser injection changes the **XOR** into **ADD**
- The rezulting syndrome gives larger quantity of information
- Solve the problem using ILP

Syndrome decoding over $\mathbb{Z}$

Definition 2 ($\mathbb{Z}$-SDP)

Instance : $\boldsymbol{H} \in \mathcal{M}_{n-k,n}(\mathbb{Z})$ with $h_{i,j} \in \{0,1\}$ for all i, j
a vector $\boldsymbol{s} \in \mathbb{Z}^{n-k}$ and an integer $t > 0$.

Question : Is there a vector $\boldsymbol{x} \in \{0,1\}^n$ with $\mathrm{wt}(\boldsymbol{x}) \leq t$, s.t. $\boldsymbol{Hx} = \boldsymbol{s}$?

Optimized exhaustive search for $\mathbb{Z}$-SDP

1. Exhaustive search

$$\binom{n}{t} \tag{3}$$

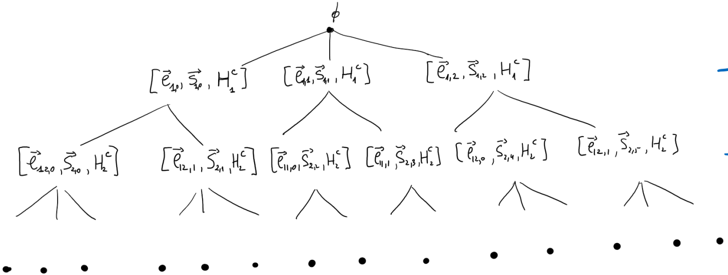
2. Divide and conquer techniques (VanDerMonde type inequality)

$$\binom{n}{t} > \binom{i}{j}\binom{n-i}{t-j} \tag{4}$$

Divide and conquer

$$
\boldsymbol{P}^* \boldsymbol{H} \boldsymbol{P} = \left[\begin{array}{ccc:ccc:ccc:ccccc}
1 & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 \\
\hdashline
 & & & 1 & \dots & 1 & 0 & 0 & \dots & \dots & \dots & 0 & 0 \\
\hdashline
 & & & & & & 1 & \dots & 1 & 0 & \dots & 0 & 0 \\
\hdashline
 & \boldsymbol{H}_1 & & & & & & & & & & & \\
 & & & & \boldsymbol{H}_2 & & & & & & \ddots & & \\
 & & & & & & & \boldsymbol{H}_3 & & & & & \\
 & & & & & & & & & & & & \boldsymbol{H}_l
\end{array}\right]
$$

Complexity



$$\binom{m_1}{s_1}$$

$$\binom{m_1}{s_1}\cdot\binom{m_2}{s_2}$$

$$\vdots$$

$$\binom{m_1}{s_1}\cdots\binom{m_e}{s_e}\cdot\binom{n-\sum_1^e m_i}{t-\sum_1^e s_i}$$

Complexity

- Estimate the value of l

Proposition 1

Let j be a strictly positive integer. Then $X_j \sim Bin(n, 1/2^j)$.

- $E(X_{\log_2 n}) = 1$ hence, typical break of the decomposition at $\log_2(n)$.
- Sorting the syndrome given smaller values of the binomials at the begining
- As $s_i \sim Bin(t, 1/2)$ - tail bounds on the binomial distribution determines the minimum

Complexity

Tacking $t = \sqrt{n}$

1. One step sorting + exhaustive search (at average)

$$\binom{n}{t} \sim \left(\frac{2^{5/3}}{3}\right)^{\sqrt{n}} n^{1/4} \binom{n/2}{t/3} \binom{n/2}{2t/3} \tag{5}$$

2. Three steps +exhaustive search

$$\binom{n}{t} \sim 2^{\sqrt{n}/4} n^{3/4} \binom{n/2}{t/4} \binom{n/4}{t/4} \binom{n/8}{t/4} \binom{n/8}{t/4} \tag{6}$$

Simulations

Open questions

- What is the worst case/average complexity of the $\mathbb{Z}$-SDP ?
- Are there other post-quantum proposals subject to our approach ?
- Probabilistic polynomial time algorithms.