3. Message Attack (ISD)

1. From Generic Decoding to Syndrome Decoding
2. Combinatorial Solutions: Exhaustive Search and Birthday Decoding
3. Information Set Decoding: the Power of Linear Algebra
4. Complexity Analysis
5. Lee and Brickell Algorithm
6. Stern/Dumer Algorithm
7. May, Meurer, and Thomae Algorithm
8. Becker, Joux, May, and Meurer Algorithm
9. Generalized Birthday Algorithm for Decoding
10. **Decoding One Out of Many**

Decoding One Out of Many (DOOM)

N-Syndrome Decoding

Instance: $S \subset \{0,1\}^{n-k}$, $|S| = N$, $H \in \{0,1\}^{(n-k)\times n}$, an integer $w > 0$
Answer: $e \in \{0,1\}^n$ such that $eH^T \in S$ and $\mathrm{wt}(e) \leq w$

We will denote $\mathrm{CSD}_N(H, S, w)$ the set of all solutions to the above problem

Decoding One Out of Many (DOOM)

N-Syndrome Decoding

Instance: $S \subset \{0,1\}^{n-k}$, $|S| = N$, $H \in \{0,1\}^{(n-k)\times n}$, an integer $w > 0$

Answer: $e \in \{0,1\}^n$ such that $eH^T \in S$ and $\mathrm{wt}(e) \leq w$

We will denote $\mathrm{CSD}_N(H,S,w)$ the set of all solutions to the above problem

As for CSD_1, we will consider solvable instances

Decoding One Out of Many (DOOM)

N-Syndrome Decoding

Instance:	$S \subset \{0,1\}^{n-k}$, $\lvert S \rvert = N$, $H \in \{0,1\}^{(n-k)\times n}$, an integer $w > 0$
Answer:	$e \in \{0,1\}^n$ such that $eH^T \in S$ and $\mathrm{wt}(e) \leq w$

We will denote $\mathrm{CSD}_N(H, S, w)$ the set of all solutions to the above problem

As for CSD_1, we will consider solvable instances

Meaning that $S \subset \{eH^T \mid \mathrm{wt}(e) = w\}$

Decoding One Out of Many (DOOM)

N-Syndrome Decoding

Instance: $S \subset \{0,1\}^{n-k}$, $|S| = N$, $H \in \{0,1\}^{(n-k)\times n}$, an integer $w > 0$
Answer: $e \in \{0,1\}^n$ such that $eH^T \in S$ and $\mathrm{wt}(e) \leq w$

We will denote $\mathrm{CSD}_N(H, S, w)$ the set of all solutions to the above problem

As for CSD_1, we will consider solvable instances

Meaning that $S \subset \{eH^T \mid \mathrm{wt}(e) = w\}$

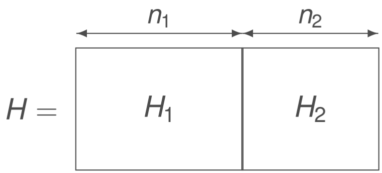
Improvement:

- we get the N solutions at the expense of a factor $\approx \sqrt{N}$
- or we get one solution with a gain of a factor $\approx \sqrt{N}$

Birthday Decoding With Multiple Instances

Solve $\mathrm{CSD}_N(H, S, w)$ with birthday decoding

$$\text{Let} \begin{cases} \mathcal{L}_1 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = w_1\} \\ \mathcal{L}_2 = \{s + e_2 H_2^T \mid s \in S, \mathrm{wt}(e_2) = w_2\} \end{cases}$$



$$n = n_1 + n_2,\ w = w_1 + w_2$$

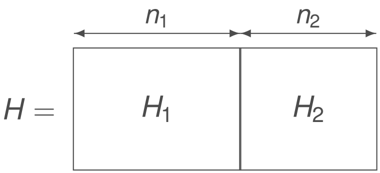
Birthday Decoding With Multiple Instances

Solve $\mathrm{CSD}_N(H, S, w)$ with birthday decoding

Let $\begin{cases} \mathcal{L}_1 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = w_1\} \\ \mathcal{L}_2 = \{s + e_2 H_2^T \mid s \in S, \mathrm{wt}(e_2) = w_2\} \end{cases}$

We choose w_1 and w_2 such that

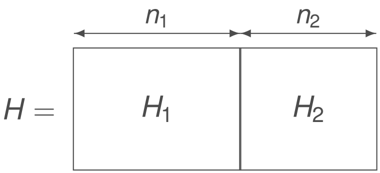
$$\frac{w_1}{n_1} = \frac{w_2}{n_2} \text{ and } |\mathcal{L}_1| = \binom{n_1}{w_1} = |\mathcal{L}_2| = N\binom{n_2}{w_2}$$



$$n = n_1 + n_2,\ w = w_1 + w_2$$

Birthday Decoding With Multiple Instances

Solve $\mathrm{CSD}_N(H, S, w)$ with birthday decoding



$n = n_1 + n_2,\ w = w_1 + w_2$

Let $\begin{cases} \mathcal{L}_1 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = w_1\} \\ \mathcal{L}_2 = \{s + e_2 H_2^T \mid s \in S, \mathrm{wt}(e_2) = w_2\} \end{cases}$

We choose w_1 and w_2 such that

$$\frac{w_1}{n_1} = \frac{w_2}{n_2} \text{ and } |\mathcal{L}_1| = \binom{n_1}{w_1} = |\mathcal{L}_2| = N\binom{n_2}{w_2}$$

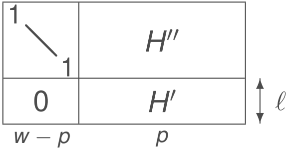
Claim: If $N \leq \binom{n}{w}$, we obtain all solutions of $\mathrm{CSD}_N(H, S, w)$

for a cost $\sqrt{N\binom{n}{w}} + \frac{N\binom{n}{w}}{2^{n-k}}$ (up to a polynomial factor)

DOOM-ISD

Solve $\mathrm{CSD}_N(H, S, w)$ when $S \subset \{eH^T \mid \mathrm{wt}(e) = w\}$ with Dumer Algorithm

The problem has N solutions and we only want one

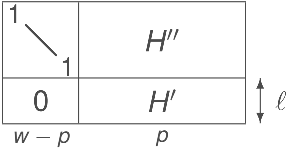


DOOM-ISD

Solve $\mathrm{CSD}_N(H, S, w)$ when $S \subset \{eH^T \mid \mathrm{wt}(e) = w\}$ with Dumer Algorithm

The problem has N solutions and we only want one

A specific solution requires $\mathcal{N}_\infty = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$ iterations

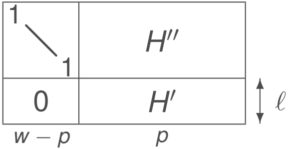


DOOM-ISD

Solve $\text{CSD}_N(H, S, w)$ when $S \subset \{eH^T \mid \text{wt}(e) = w\}$ with Dumer Algorithm

The problem has N solutions and we only want one

A specific solution requires $\mathcal{N}_\infty = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$ iterations

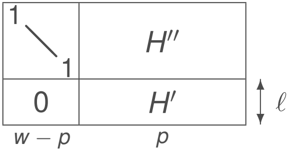


For one solution only, we expect $\mathcal{N}_1 = \mathcal{N}_\infty / N$ iterations as long as $N \leq \mathcal{N}_\infty$

DOOM-ISD

Solve $\mathrm{CSD}_N(H, S, w)$ when $S \subset \{eH^T \mid \mathrm{wt}(e) = w\}$ with Dumer Algorithm

The problem has N solutions and we only want one



A specific solution requires $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$ iterations

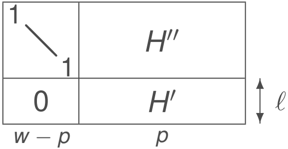
For one solution only, we expect $\mathcal{N}_1 = \mathcal{N}_\infty / N$ iterations as long as $N \leq \mathcal{N}_\infty$

Iteration cost: $\mathcal{K} = \sqrt{N\binom{k+\ell}{p}} + \dfrac{N\binom{k+\ell}{p}}{2^\ell}$ as long as $N \leq \binom{k+\ell}{p}$

DOOM-ISD

Solve $\text{CSD}_N(H, S, w)$ when $S \subset \{eH^T \mid \text{wt}(e) = w\}$ with Dumer Algorithm

The problem has N solutions and we only want one



A specific solution requires $\mathcal{N}_\infty = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$ iterations

For one solution only, we expect $\mathcal{N}_1 = \mathcal{N}_\infty / N$ iterations as long as $N \leq \mathcal{N}_\infty$

Iteration cost: $\mathcal{K} = \sqrt{N\binom{k+\ell}{p}} + \frac{N\binom{k+\ell}{p}}{2^\ell}$ as long as $N \leq \binom{k+\ell}{p}$

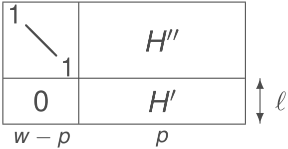
$$\rightarrow \text{WF}_{\text{DOOM}} = \min_{0 \leq p \leq w} \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\sqrt{N\binom{k+\ell}{p}}} \text{ with } \ell = \log_2 \sqrt{N\binom{k+\ell}{p}}$$

DOOM-ISD

Solve $\text{CSD}_N(H, S, w)$ when $S \subset \{eH^T \mid \text{wt}(e) = w\}$ with Dumer Algorithm

The problem has N solutions and we only want one

A specific solution requires $\mathcal{N}_\infty = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$ iterations



For one solution only, we expect $\mathcal{N}_1 = \mathcal{N}_\infty / N$ iterations as long as $N \leq \mathcal{N}_\infty$

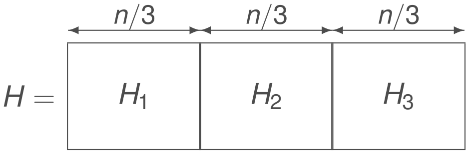
Iteration cost: $\mathcal{K} = \sqrt{N\binom{k+\ell}{p}} + \frac{N\binom{k+\ell}{p}}{2^\ell}$ as long as $N \leq \binom{k+\ell}{p}$

$\rightarrow$ $\text{WF}_{\text{DOOM}} = \min_{0 \leq p \leq w} \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\sqrt{N\binom{k+\ell}{p}}}$ with $\ell = \log_2 \sqrt{N\binom{k+\ell}{p}}$

$\rightarrow$ gain of a factor $\approx \sqrt{N}$ as long as $N \leq \min\left(\mathcal{N}_\infty, \binom{k+\ell}{p}\right)$

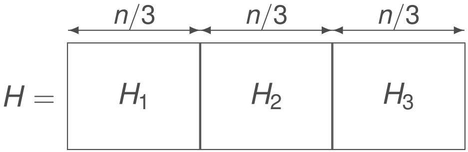
DOOM-GBA

A gain is also possible with an Order 2 GBA Decoding when $N = |S| = \binom{n/3}{w/3}$



DOOM-GBA

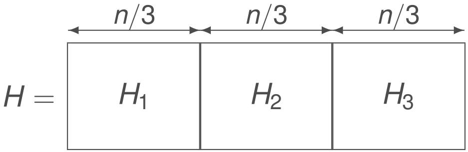
A gain is also possible with an Order 2 GBA Decoding when $N = |S| = \binom{n/3}{w/3}$



$\mathcal{L}_i \subset \{e_i H_i^T \mid \text{wt}(e_i) = w/3\}, i \in \{1, 2, 3\}$ and $\mathcal{L}_4 = S$

DOOM-GBA

A gain is also possible with an Order 2 GBA Decoding when $N = |S| = \binom{n/3}{w/3}$



$\mathcal{L}_i \subset \{e_i H_i^T \mid \mathrm{wt}(e_i) = w/3\}, i \in \{1, 2, 3\}$ and $\mathcal{L}_4 = S$

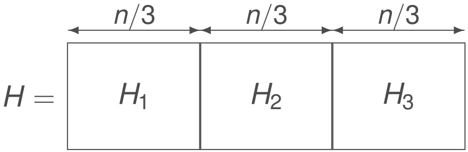
From $x_i \in \mathcal{L}_i, i \in \{1, 2, 3, 4\}$ such that $x_1 + x_2 + x_3 + x_4 = 0$ we obtain

$$e_1 H_1^T + e_2 H_2^T + e_3 H_3^T + s = 0, s \in S$$

and we have $e = (e_1, e_2, e_3) \in \mathrm{CSD}_N(H, S, w)$

DOOM-GBA

A gain is also possible with an Order 2 GBA Decoding when $N = |S| = \binom{n/3}{w/3}$



$\mathcal{L}_i \subset \{e_i H_i^T \mid \text{wt}(e_i) = w/3\}, i \in \{1, 2, 3\}$ and $\mathcal{L}_4 = S$

From $x_i \in \mathcal{L}_i, i \in \{1, 2, 3, 4\}$ such that $x_1 + x_2 + x_3 + x_4 = 0$ we obtain

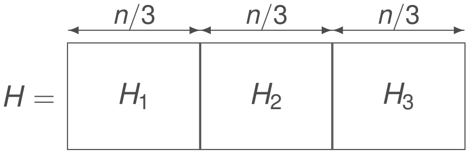
$$e_1 H_1^T + e_2 H_2^T + e_3 H_3^T + s = 0, s \in S$$

and we have $e = (e_1, e_2, e_3) \in \text{CSD}_N(H, S, w)$

Workfactor is $\binom{n/3}{w/3} \approx \sqrt[3]{\binom{n}{w}}$ up to a polynomial factor

DOOM-GBA

A gain is also possible with an Order 2 GBA Decoding when $N = |S| = \binom{n/3}{w/3}$



$\mathcal{L}_i \subset \{e_i H_i^T \mid \mathrm{wt}(e_i) = w/3\}, i \in \{1, 2, 3\}$ and $\mathcal{L}_4 = S$

From $x_i \in \mathcal{L}_i, i \in \{1, 2, 3, 4\}$ such that $x_1 + x_2 + x_3 + x_4 = 0$ we obtain

$$e_1 H_1^T + e_2 H_2^T + e_3 H_3^T + s = 0, s \in S$$

and we have $e = (e_1, e_2, e_3) \in \mathrm{CSD}_N(H, S, w)$

Workfactor is $\binom{n/3}{w/3} \approx \sqrt[3]{\binom{n}{w}}$ up to a polynomial factor

To be compared with $\sqrt{\binom{n}{w}}$ with the birthday decoding, gaining a factor $\approx \sqrt{N}$

3. Message Attack (ISD)

1. From Generic Decoding to Syndrome Decoding
2. Combinatorial Solutions: Exhaustive Search and Birthday Decoding
3. Information Set Decoding: the Power of Linear Algebra
4. Complexity Analysis
5. Lee and Brickell Algorithm
6. Stern/Dumer Algorithm
7. May, Meurer, and Thomae Algorithm
8. Becker, Joux, May, and Meurer Algorithm
9. Generalized Birthday Algorithm for Decoding
10. Decoding One Out of Many

Code-Based Cryptography