3. Message Attack (ISD)

Exhaustive Search

Problem: find w columns of H adding to s (modulo 2)

$$H = \overbrace{\boxed{\; h_1 \quad h_2 \quad \cdots \quad h_n \;}}^{n} \; n-k \qquad s = \boxed{\;}$$

Exhaustive Search

Problem: find w columns of H adding to s (modulo 2)

$$H = \overbrace{\boxed{h_1 \quad h_2 \quad \cdots \quad h_n}}^{n} \; n-k \qquad s = \boxed{}$$

Answer: enumerate all w-tuples $(j_1, j_2, \cdots, j_w)$ such that $1 \leq j_1 < j_2 < \ldots < j_w \leq n$ and check whether $s + h_{j_1} + h_{j_2} \cdots + h_{j_w} = 0$

How to enumerate nicely

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \leq j_1 < \ldots < j_w \leq n\}}$$

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \begin{bmatrix} s \end{bmatrix} \; n-k$$

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \leq j_1 < \ldots < j_w \leq n\}}$$

`for` j_1 `from` 1 `to` n

$$H = \overbrace{\begin{array}{|cccc|}\hline & & & \\ h_1 & h_2 & \cdots & h_n \\ & & & \\ \hline\end{array}}^{n} \; \begin{array}{|c|}\hline \\ s \\ \\ \hline\end{array} \; \Big\updownarrow n-k$$

$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \leq j_1 < \ldots < j_w \leq n\}}$

for j_1 from 1 to n

  for j_2 from $j_1 + 1$ to n

$$H = \overbrace{\boxed{\; h_1 \quad h_2 \quad \cdots \quad h_n \;}}^{n}\ \boxed{s}\ \Big\updownarrow\, n-k$$

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$$

1: for j_1 from 1 to n

2: for j_2 from $j_1 + 1$ to n

$\ddots$

w: for j_w from $j_{w-1} + 1$ to n

$$H = \begin{array}{c} \overset{n}{\longleftrightarrow} \\ \boxed{\; h_1 \quad h_2 \quad \cdots \quad h_n \;} \end{array} \boxed{s} \; \updownarrow n - k$$

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$$

1: for j_1 from 1 to n

2: for j_2 from $j_1 + 1$ to n

$\ddots$

w: for j_w from $j_{w-1} + 1$ to n

$s_w \leftarrow s + h_{j_1} + h_{j_2} + \cdots + h_{j_w}$

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \quad \begin{bmatrix} s \end{bmatrix} \; \Big\updownarrow \, n-k$$

$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \leq j_1 < \ldots < j_w \leq n\}}$

1: `for` j_1 `from` 1 `to` n

2: `for` j_2 `from` $j_1 + 1$ `to` n

$\ddots$

w: `for` j_w `from` $j_{w-1} + 1$ `to` n

$s_w \leftarrow s + h_{j_1} + h_{j_2} + \cdots + h_{j_w}$

[`if` $s_w = 0$ `then return` $(j_1, j_2, \ldots, j_w)$] or [`store`$(s_w, (j_1, j_2, \ldots, j_w))$]

$$H = \begin{array}{c} \overset{n}{\longleftrightarrow} \\ \begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix} \end{array} \begin{bmatrix} s \end{bmatrix} \Big\updownarrow n - k$$

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$$

1: `for` j_1 `from` 1 `to` n

2: `for` j_2 `from` $j_1 + 1$ `to` n

$\ddots$

w: `for` j_w `from` $j_{w-1} + 1$ `to` n

$s_w \leftarrow s + h_{j_1} + h_{j_2} + \cdots + h_{j_w}$

[`if` $s_w = 0$ `then return` $(j_1, j_2, \ldots, j_w)$] or [`store`$(s_w, (j_1, j_2, \ldots, j_w))$]

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \quad \begin{bmatrix} s \end{bmatrix} \; \updownarrow n-k$$

Total cost is at most $w\binom{n}{w}$ column additions and $\binom{n}{w}$ tests

$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$

1: for j_1 from 1 to n

2: for j_2 from $j_1 + 1$ to n

$\ddots$

w: for j_w from $j_{w-1} + 1$ to n

$s_w \leftarrow s + h_{j_1} + h_{j_2} + \cdots + h_{j_w}$

[if $s_w = 0$ then return $(j_1, j_2, \ldots, j_w)$] or [store$(s_w, (j_1, j_2, \ldots, j_w))$]

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \begin{bmatrix} s \end{bmatrix} \; \Big\updownarrow \, n-k$$

Total cost is at most $w\binom{n}{w}$ column additions ~~and $\binom{n}{w}$ tests~~

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$$

1: `for` j_1 `from` 1 `to` n

2: `for` j_2 `from` $j_1 + 1$ `to` n

$\ddots$

w: `for` j_w `from` $j_{w-1} + 1$ `to` n

$s_w \leftarrow s + h_{j_1} + h_{j_2} + \cdots + h_{j_w}$

[`if` $s_w = 0$ `then return` $(j_1, j_2, \ldots, j_w)$] or [`store`$(s_w, (j_1, j_2, \ldots, j_w))$]

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \quad \begin{bmatrix} s \end{bmatrix} \Big\updownarrow n-k$$

Total cost is about $w\binom{n}{w}$ column operations

$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$

`for` j_1 `from` 1 `to` n

1: $s_1 \leftarrow s + h_{j_1}$

`for` j_2 `from` $j_1 + 1$ `to` n

2:

$\ddots$

`for` j_w `from` $j_{w-1} + 1$ `to` n

w:

[`if` $s_w = 0$ `then return` $(j_1, j_2, \ldots, j_w)$] or [`store`$(s_w, (j_1, j_2, \ldots, j_w))$]

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \quad \begin{bmatrix} s \end{bmatrix} \quad n-k$$

Instead, we may keep track of partial sums

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$$

```
    for j_1 from 1 to n
1:      s_1 ← s + h_{j_1}
        for j_2 from j_1 + 1 to n
2:          s_2 ← s_1 + h_{j_2}   (= s + h_{j_1} + h_{j_2})
                  ⋱
                for j_w from j_{w-1} + 1 to n
w:
                    [if s_w = 0 then return (j_1, j_2, ..., j_w)] or [store(s_w, (j_1, j_2, ..., j_w))]
```

$$H = \underbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}_{n} \; \begin{bmatrix} s \end{bmatrix} \quad n - k$$

Instead, we may keep track of partial sums

$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$

$$H = \Big[\, \overbrace{h_1 \quad h_2 \quad \cdots \quad h_n}^{n} \;\Big|\; s \,\Big] \quad n-k$$

for j_1 from 1 to n

1: $s_1 \leftarrow s + h_{j_1}$

for j_2 from $j_1 + 1$ to n

2: $s_2 \leftarrow s_1 + h_{j_2}$

$\ddots$

for j_w from $j_{w-1} + 1$ to n

w: $s_w \leftarrow s_{w-1} + h_{j_w}$ $\quad (= s + h_{j_1} + h_{j_2} + \cdots + h_{j_w})$

[if $s_w = 0$ then return $(j_1, j_2, \ldots, j_w)$] or [store$(s_w, (j_1, j_2, \ldots, j_w))$]

Instead, we may keep track of partial sums

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \leq j_1 < \ldots < j_w \leq n\}}$$

$\texttt{for } j_1 \texttt{ from } 1 \texttt{ to } n$

1: $\quad s_1 \leftarrow s + h_{j_1}$

$\quad\quad \texttt{for } j_2 \texttt{ from } j_1 + 1 \texttt{ to } n$

2: $\quad\quad s_2 \leftarrow s_1 + h_{j_2}$

$\quad\quad\quad \ddots$

$\quad\quad\quad \texttt{for } j_w \texttt{ from } j_{w-1} + 1 \texttt{ to } n$

w: $\quad\quad\quad s_w \leftarrow s_{w-1} + h_{j_w}$

$\quad\quad\quad [\texttt{if } s_w = 0 \texttt{ then return } (j_1, j_2, \ldots, j_w)]$ or $[\texttt{store}(s_w, (j_1, j_2, \ldots, j_w))]$

$$H = \overbrace{\boxed{h_1 \quad h_2 \quad \cdots \quad h_n}}^{n} \; \boxed{s} \; \updownarrow n - k$$

Line i is executed about $\binom{n}{i}$ times

$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$

```
    for j_1 from 1 to n
1:      s_1 ← s + h_{j_1}
        for j_2 from j_1 + 1 to n
2:          s_2 ← s_1 + h_{j_2}
                ⋱
                    for j_w from j_{w-1} + 1 to n
w:                      s_w ← s_{w-1} + h_{j_w}
                        [if s_w = 0 then return (j_1, j_2, ..., j_w)] or [store(s_w, (j_1, j_2, ..., j_w))]
```

$$H = \overbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \; \begin{bmatrix} s \end{bmatrix} \; \Big\updownarrow\, n-k$$

Line i is executed about $\binom{n}{i}$ times

$\rightarrow$ total of about $\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{w}$ column additions

$$\boxed{\text{Enumerate } \{s + eH^T \mid \mathrm{wt}(e) = w\} = \{s + h_{j_1} + \cdots + h_{j_w} \mid 1 \le j_1 < \ldots < j_w \le n\}}$$

for j_1 from 1 to n

1: $\quad s_1 \leftarrow s + h_{j_1}$

for j_2 from $j_1 + 1$ to n

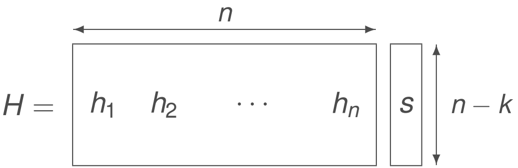
2: $\quad s_2 \leftarrow s_1 + h_{j_2}$

$\ddots$

for j_w from $j_{w-1} + 1$ to n

w: $\quad s_w \leftarrow s_{w-1} + h_{j_w}$

[if $s_w = 0$ then return $(j_1, j_2, \ldots, j_w)$] or [store$(s_w, (j_1, j_2, \ldots, j_w))$]



Line i is executed about $\binom{n}{i}$ times

$\rightarrow$ total of about $\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{w}$ column additions

dominated by $\binom{n}{w}$ when w is not too large

Back

Exhaustive Search

Problem: find w columns of H adding to s (modulo 2)

$$H = \underbrace{\begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}_{n} \; \Big\updownarrow n-k \qquad s = \begin{bmatrix} \; \end{bmatrix}$$

Answer: enumerate all w-tuples $(j_1, j_2, \cdots, j_w)$ such that $1 \leq j_1 < j_2 < \ldots < j_w \leq n$ and check whether $s + h_{j_1} + h_{j_2} \cdots + h_{j_w} = 0$

▸ How to enumerate nicely

Requires *about* $\binom{n}{w}$ column operations

Exhaustive Search

Problem: find w columns of H adding to s (modulo 2)

$$\overbrace{H = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix}}^{n} \; \updownarrow n-k \qquad s = \begin{bmatrix} \\ \\ \end{bmatrix}$$

Answer: enumerate all w-tuples $(j_1, j_2, \cdots, j_w)$ such that $1 \leq j_1 < j_2 < \ldots < j_w \leq n$ and check whether $s + h_{j_1} + h_{j_2} \cdots + h_{j_w} = 0$

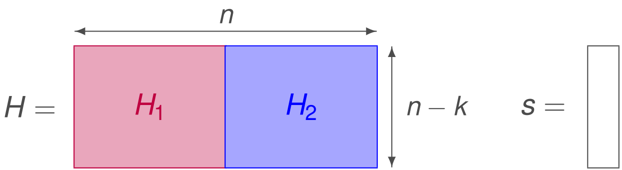
▸ How to enumerate nicely

Requires *about* $\binom{n}{w}$ column operations

Note that we obtain all solutions

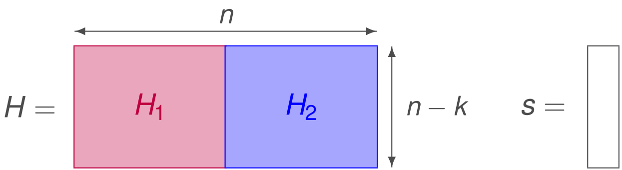
Birthday Decoding

Problem: find w columns of H adding to s (modulo 2)



Birthday Decoding

Problem: find w columns of H adding to s (modulo 2)



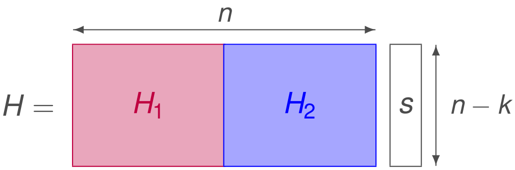
Answer: Split H into two equal parts and enumerate the two following sets

$$\mathcal{L}_1 = \left\{ e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2} \right\} \text{ and } \mathcal{L}_2 = \left\{ s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2} \right\}$$

If $\mathcal{L}_1 \cap \mathcal{L}_2 \neq \emptyset$, we have solution(s): $s + e_1 H_1^T + e_2 H_2^T = 0$

▸ Algorithm

$$\boxed{\text{Compute } \mathcal{L}_1 \cap \mathcal{L}_2 = \left\{ e_1 H_1^T \mid \mathrm{wt}(e_1) = \tfrac{w}{2} \right\} \cap \left\{ s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \tfrac{w}{2} \right\}}$$



$\boxed{\text{Compute } \mathcal{L}_1 \cap \mathcal{L}_2 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\} \cap \{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}}$

`for all` e_1 of weight $w/2$

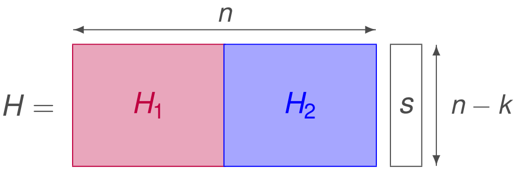
$x \leftarrow e_1 H_1^T \; ; \; T[x] \leftarrow T[x] \cup \{e_1\}$

$$H = \overbrace{\begin{bmatrix} H_1 & H_2 \end{bmatrix}}^{n} \quad \begin{bmatrix} s \end{bmatrix} \; \Big\updownarrow \; n-k$$

Total cost: $\binom{n/2}{w/2}$

$|\mathcal{L}_1|$

$\boxed{\text{Compute } \mathcal{L}_1 \cap \mathcal{L}_2 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\} \cap \{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}}$



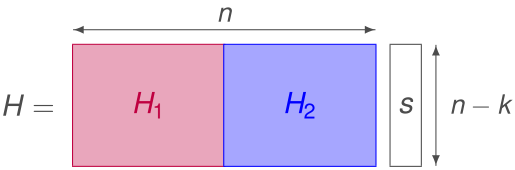
`for all` e_1 of weight $w/2$
  $x \leftarrow e_1 H_1^T$; $T[x] \leftarrow T[x] \cup \{e_1\}$
`for all` e_2 of weight $w/2$
  $x \leftarrow s + e_2 H_2^T$

Total cost: $\binom{n/2}{w/2} + \binom{n/2}{w/2}$

$|\mathcal{L}_1| \qquad |\mathcal{L}_2|$

Compute $\mathcal{L}_1 \cap \mathcal{L}_2 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\} \cap \{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}$

for all e_1 of weight $w/2$
  $x \leftarrow e_1 H_1^T$; $T[x] \leftarrow T[x] \cup \{e_1\}$
for all e_2 of weight $w/2$
  $x \leftarrow s + e_2 H_2^T$
  for all $e_1 \in T[x]$
    $\mathcal{I} \leftarrow \mathcal{I} \cup \{(e_1, e_2)\}$

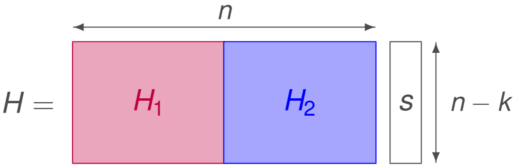


Total cost: $\binom{n/2}{w/2} + \binom{n/2}{w/2} + \frac{\binom{n/2}{w/2}^2}{2^{n-k}}$

$|\mathcal{L}_1|$ $|\mathcal{L}_2|$ $\frac{|\mathcal{L}_1| \cdot |\mathcal{L}_2|}{2^{n-k}}$

Compute $\mathcal{L}_1 \cap \mathcal{L}_2 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\} \cap \{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}$

for all e_1 of weight $w/2$
  $x \leftarrow e_1 H_1^T$; $T[x] \leftarrow T[x] \cup \{e_1\}$
for all e_2 of weight $w/2$
  $x \leftarrow s + e_2 H_2^T$
  for all $e_1 \in T[x]$
    $\mathcal{I} \leftarrow \mathcal{I} \cup \{(e_1, e_2)\}$
return $\mathcal{I}$



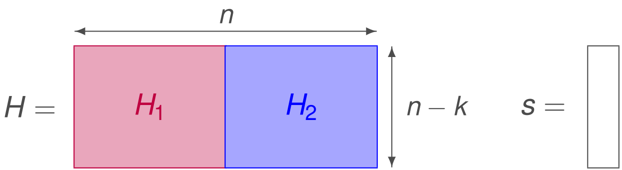
Total cost: $\binom{n/2}{w/2} + \binom{n/2}{w/2} + \frac{\binom{n/2}{w/2}^2}{2^{n-k}}$

$|\mathcal{L}_1|$ $\quad |\mathcal{L}_2|$ $\quad \frac{|\mathcal{L}_1| \cdot |\mathcal{L}_2|}{2^{n-k}}$

Back

Birthday Decoding

Problem: find w columns of H adding to s (modulo 2)



Answer: Split H into two equal parts and enumerate the two following sets

$$\mathcal{L}_1 = \left\{ e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2} \right\} \text{ and } \mathcal{L}_2 = \left\{ s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2} \right\}$$

If $\mathcal{L}_1 \cap \mathcal{L}_2 \neq \emptyset$, we have solution(s): $s + e_1 H_1^T + e_2 H_2^T = 0$

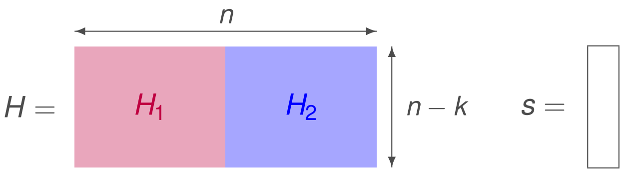
▸ Algorithm

Requires *about* $2\binom{n/2}{w/2} + \frac{\binom{n/2}{w/2}^2}{2^{n-k}}$ column operations

Can also be written $2L + L^2/2^{n-k}$ where $L = |\mathcal{L}_1| = |\mathcal{L}_2|$

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)



Birthday Decoding – Complexity

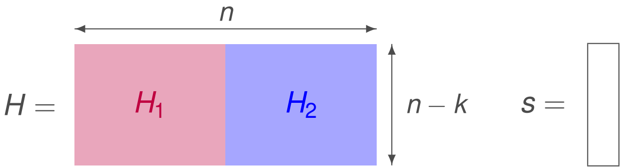
Problem: find w columns of H adding to s (modulo 2)

$$H = \begin{array}{c} \overset{n}{\longleftrightarrow} \\ \boxed{\;H_1\; \mid \;H_2\;} \end{array} \updownarrow n-k \qquad s = \boxed{}$$

One particular error of Hamming weight w splits evenly with probability $\mathcal{P} = \dfrac{\binom{n/2}{w/2}^2}{\binom{n}{w}}$

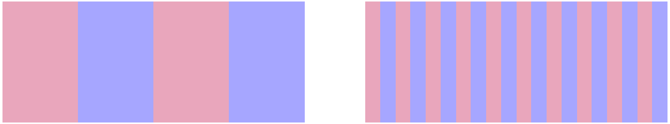
Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)



One particular error of Hamming weight w splits evenly with probability $\mathcal{P} = \frac{\binom{n/2}{w/2}^2}{\binom{n}{w}}$

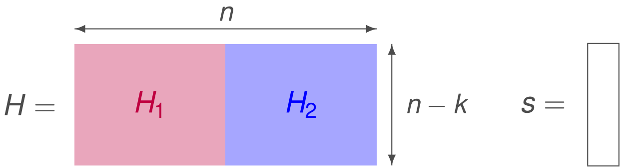
We may have to repeat with H divided in several different ways



or more generally by picking the two halves randomly

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)

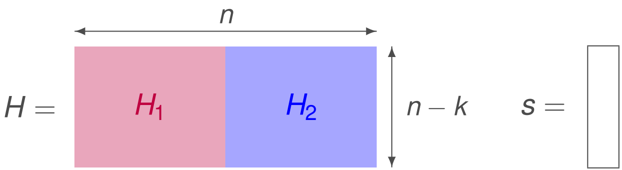


To obtain all solutions:

$$\mathcal{P} = \frac{\binom{n/2}{w/2}^2}{\binom{n}{w}}$$

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)



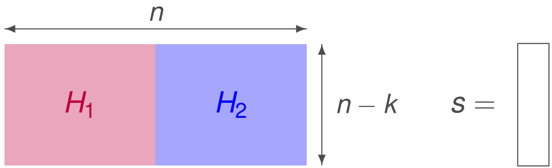
To obtain ~~all~~ most solutions:

repeat with $\approx \frac{1}{\mathcal{P}}$ different splitting: $\begin{cases} \text{1. compute } \mathcal{L}_1 \text{ and } \mathcal{L}_2 \\ \text{2. compute } \mathcal{L}_1 \cap \mathcal{L}_2 \end{cases}$

$$\mathcal{P} = \frac{\binom{n/2}{w/2}^2}{\binom{n}{w}}$$

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)

$H =$ 

To obtain ~~all~~ most solutions:

repeat with $\approx \frac{1}{\mathcal{P}}$ different splitting: $\begin{cases} \text{1. compute } \mathcal{L}_1 \text{ and } \mathcal{L}_2 \\ \text{2. compute } \mathcal{L}_1 \cap \mathcal{L}_2 \end{cases}$

$$\mathcal{P} = \frac{\binom{n/2}{w/2}^2}{\binom{n}{w}}$$

Total cost $\dfrac{2\binom{n/2}{w/2} + \binom{n/2}{w/2}^2 / 2^{n-k}}{\mathcal{P}} = \dfrac{2\binom{n}{w}}{\binom{n/2}{w/2}} + \dfrac{\binom{n}{w}}{2^{n-k}}$ operations

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)

$$H = \overbrace{\begin{bmatrix} H_1 & H_2 \end{bmatrix}}^{n} \Big\} n-k \qquad s = \begin{bmatrix} \; \end{bmatrix}$$

To obtain ~~all~~ most solutions:

repeat with $\approx \frac{1}{\mathcal{P}}$ different splitting: $\begin{cases} \text{1. compute } \mathcal{L}_1 \text{ and } \mathcal{L}_2 \\ \text{2. compute } \mathcal{L}_1 \cap \mathcal{L}_2 \end{cases}$

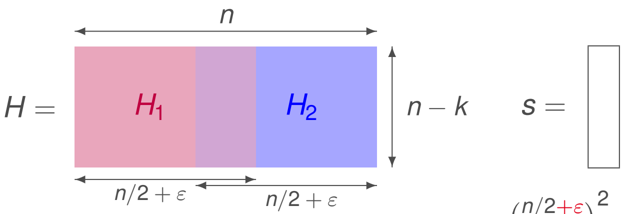
$$\mathcal{P} = \frac{\binom{n/2}{w/2}^2}{\binom{n}{w}}$$

Total cost $\dfrac{2\binom{n/2}{w/2} + \binom{n/2}{w/2}^2 / 2^{n-k}}{\mathcal{P}} = \dfrac{2\binom{n}{w}}{\binom{n/2}{w/2}} + \dfrac{\binom{n}{w}}{2^{n-k}}$ operations

$$\approx \sqrt[4]{8\pi w}\sqrt{\binom{n}{w}} + \#Solutions$$

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)



$$\mathcal{P} = \frac{\binom{n/2+\varepsilon}{w/2}^2}{\binom{n}{w}}$$

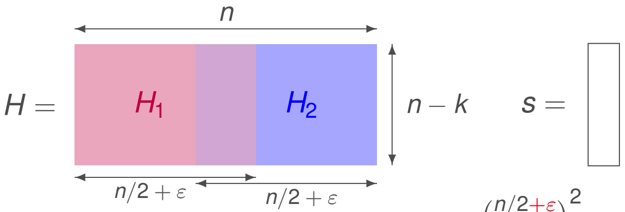
To obtain ~~all~~ most solutions:

repeat with $\approx \frac{1}{\mathcal{P}}$ different splitting: $\begin{cases} \text{1. compute } \mathcal{L}_1 \text{ and } \mathcal{L}_2 \\ \text{2. compute } \mathcal{L}_1 \cap \mathcal{L}_2 \end{cases}$

Relaxation: allow overlapping $\rightarrow$ H_1 and H_2 are wider by ε

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)



To obtain ~~all~~ most solutions:

repeat with $\approx \frac{1}{\mathcal{P}}$ different splitting: $\begin{cases} \text{1. compute } \mathcal{L}_1 \text{ and } \mathcal{L}_2 \\ \text{2. compute } \mathcal{L}_1 \cap \mathcal{L}_2 \end{cases}$

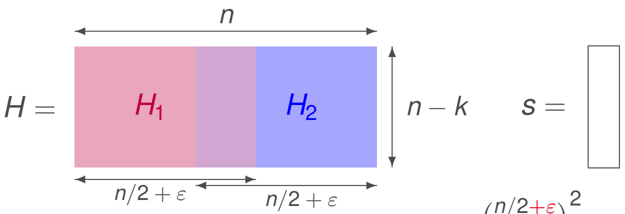
$$\mathcal{P} = \frac{\binom{n/2+\varepsilon}{w/2}^2}{\binom{n}{w}} \approx 1$$

Relaxation: allow overlapping $\rightarrow$ H_1 and H_2 are wider by ε

We choose ε such that $\binom{n/2+\varepsilon}{w/2} \approx \sqrt{\binom{n}{w}}$ $\rightarrow$ single repetition

Birthday Decoding – Complexity

Problem: find w columns of H adding to s (modulo 2)



To obtain ~~all~~ most solutions:

repeat with $\approx \frac{1}{\mathcal{P}}$ different splitting: $\begin{cases} 1.\ \text{compute } \mathcal{L}_1 \text{ and } \mathcal{L}_2 \\ 2.\ \text{compute } \mathcal{L}_1 \cap \mathcal{L}_2 \end{cases}$

$$\mathcal{P} = \frac{\binom{n/2+\varepsilon}{w/2}^2}{\binom{n}{w}} \approx 1$$

Relaxation: allow overlapping $\to$ H_1 and H_2 are wider by ε

We choose ε such that $\binom{n/2+\varepsilon}{w/2} \approx \sqrt{\binom{n}{w}}$ $\to$ single repetition

Total cost: $2\sqrt{\binom{n}{w}} + \binom{n}{w}/2^{n-k} = 2L + L^2/2^{n-k}$ with $L = \sqrt{\binom{n}{w}}$

(up to a small constant factor)

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