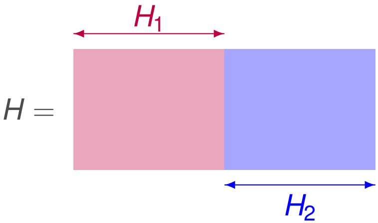
3. Message Attack (ISD)

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

Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

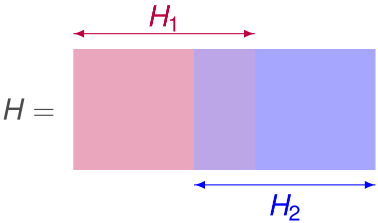
Let $\mathcal{L}_1 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\}$ and $\mathcal{L}_2 = \{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}$



Improved Birthday Decoding

Idea: Use the "representation technique" (Howgrave-Graham and Joux, 2010)

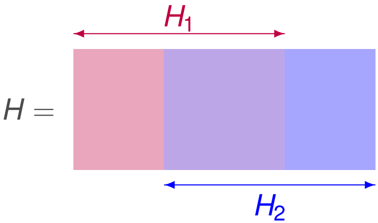
Let $\mathcal{L}_1 = \{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\}$ and $\mathcal{L}_2 = \{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}$



Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

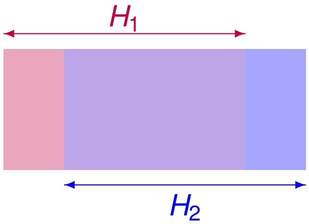
Let $\mathcal{L}_1 = \left\{e_1 H_1^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\right\}$ and $\mathcal{L}_2 = \left\{s + e_2 H_2^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\right\}$



Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

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

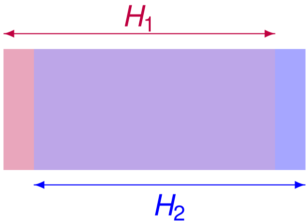
$H =$ 

Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

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

$H =$

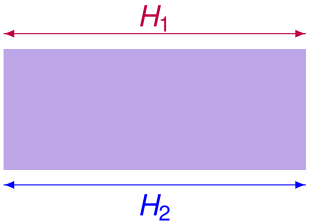


Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

Let $\mathcal{L}_1 = \{e_1 H^T \mid \mathrm{wt}(e_1) = \frac{w}{2}\}$ and $\mathcal{L}_2 = \{s + e_2 H^T \mid \mathrm{wt}(e_2) = \frac{w}{2}\}$

$H =$



Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

$$\text{Let } \mathcal{L}_1 = \{e_1 H^T \mid \mathrm{wt}(e_1) = \tfrac{w}{2}\} \text{ and } \mathcal{L}_2 = \{s + e_2 H^T \mid \mathrm{wt}(e_2) = \tfrac{w}{2}\}$$

Each $e \in \mathrm{CSD}(H, s, w)$ “represented” $\binom{w}{w/2}$ times as $e = e_1 + e_2$ with $e_1 H^T = s + e_2 H^T \in \mathcal{L}_1 \cap \mathcal{L}_2$

Improved Birthday Decoding

Idea: Use the "representation technique" (Howgrave-Graham and Joux, 2010)

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

Each $e \in \mathrm{CSD}(H, s, w)$ "represented" $\binom{w}{w/2}$ times as $e = e_1 + e_2$ with $e_1 H^T = s + e_2 H^T \in \mathcal{L}_1 \cap \mathcal{L}_2$

We may decimate $\mathcal{L}_1$ and $\mathcal{L}_2$ while keeping the solutions in $\mathcal{L}_1 \cap \mathcal{L}_2$

Improved Birthday Decoding

Idea: Use the “representation technique” (Howgrave-Graham and Joux, 2010)

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

Each $e \in \mathrm{CSD}(H, s, w)$ “represented” $\binom{w}{w/2}$ times as $e = e_1 + e_2$ with $e_1 H^T = s + e_2 H^T \in \mathcal{L}_1 \cap \mathcal{L}_2$

We may decimate $\mathcal{L}_1$ and $\mathcal{L}_2$ while keeping the solutions in $\mathcal{L}_1 \cap \mathcal{L}_2$

For any binary vector, let $\phi_r(x)$ denote the last r bits of x, we define

$$\mathcal{L}_1(r) = \left\{e_1 H^T \mid \mathrm{wt}(e_1) = \tfrac{w}{2}, \phi_r(e_1 H^T) = 0\right\}$$

$$\mathcal{L}_2(r) = \left\{s + e_2 H^T \mid \mathrm{wt}(e_2) = \tfrac{w}{2}, \phi_r(s + e_2 H^T) = 0\right\}$$

Improved Birthday Decoding

Idea: Use the "representation technique" (Howgrave-Graham and Joux, 2010)

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

Each $e \in \mathrm{CSD}(H, s, w)$ "represented" $\binom{w}{w/2}$ times as $e = e_1 + e_2$ with $e_1 H^T = s + e_2 H^T \in \mathcal{L}_1 \cap \mathcal{L}_2$

We may decimate $\mathcal{L}_1$ and $\mathcal{L}_2$ while keeping the solutions in $\mathcal{L}_1 \cap \mathcal{L}_2$

For any binary vector, let $\phi_r(x)$ denote the last r bits of x, we define

$$\mathcal{L}_1(r) = \left\{ e_1 H^T \mid \mathrm{wt}(e_1) = \tfrac{w}{2}, \phi_r(e_1 H^T) = 0 \right\}$$

$$\mathcal{L}_2(r) = \left\{ s + e_2 H^T \mid \mathrm{wt}(e_2) = \tfrac{w}{2}, \phi_r(s + e_2 H^T) = 0 \right\}$$

Claim: if $2^r = \binom{w}{w/2}$ then any $e \in \mathrm{CSD}(H, s, w)$ is "represented in $\mathcal{L}_1(r) \cap \mathcal{L}_2(r)$" with probability $> 1/2$

Improved Birthday Decoding – Algorithm

$$H = \begin{array}{c} \\ r \end{array} \left[\begin{array}{c} H'' \\ \hline H' \end{array}\right] \qquad s = \left[\begin{array}{c} s'' \\ \hline s' \end{array}\right]$$

Improved Birthday Decoding – Algorithm

$\texttt{for all } e_1 \in \boxed{\mathrm{CSD}(H', 0, w/2)}$

$\quad x \leftarrow e_1 H''^T \; ; \; T[x] \leftarrow T[x] \cup \{e_1\}$

$$H = \begin{array}{c} \\ r \updownarrow \end{array} \begin{bmatrix} H'' \\ \hline H' \end{bmatrix} \qquad s = \begin{bmatrix} s'' \\ \hline s' \end{bmatrix}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r}$$

first recursive call to CSD

solved by birthday decoding with complexity $\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r}$

Improved Birthday Decoding – Algorithm

$\texttt{for all } e_1 \in \mathrm{CSD}(H', 0, w/2)$

$\quad x \leftarrow e_1 H''^T \; ; \; T[x] \leftarrow T[x] \cup \{e_1\}$

$\texttt{for all } e_2 \in \boxed{\mathrm{CSD}(H', s', w/2)}$

$\quad x \leftarrow s + e_2 H''^T$

$$H = \begin{array}{c} \\ r \updownarrow \end{array} \begin{bmatrix} H'' \\ H' \end{bmatrix} \qquad s = \begin{bmatrix} s'' \\ s' \end{bmatrix}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r}$$

second recursive call to CSD

solved with birthday decoding with complexity $\sqrt{\binom{n}{w/2}} + \dfrac{\binom{n}{w/2}}{2^r}$

Improved Birthday Decoding – Algorithm

$\texttt{for all } e_1 \in \mathrm{CSD}(H', 0, w/2)$
$\quad x \leftarrow e_1 H''^T \; ; \; T[x] \leftarrow T[x] \cup \{e_1\}$
$\texttt{for all } e_2 \in \mathrm{CSD}(H', s', w/2)$
$\quad x \leftarrow s + e_2 H''^T$
$\quad \texttt{for all } e_1 \in T[x]$
$\quad\quad \mathcal{I} \leftarrow \mathcal{I} \cup \{(e_1, e_2)\}$

$$H = \begin{array}{l} \boxed{\quad H'' \quad} \\ \boxed{\quad H' \quad} \end{array} \quad \updownarrow r \qquad s = \begin{array}{l} \boxed{s''} \\ \boxed{s'} \end{array}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \frac{\binom{n}{w/2}^2}{2^{n-k+r}}$$

Keep the syndromes matching on the first $n-k-r$ bits

There are $\left(\frac{\binom{n}{w/2}}{2^r}\right)^2 \frac{1}{2^{n-k-r}}$ such syndromes and as many solutions

Improved Birthday Decoding – Algorithm

for all $e_1 \in \mathrm{CSD}(H', 0, w/2)$
  $x \leftarrow e_1 H''^T$; $T[x] \leftarrow T[x] \cup \{e_1\}$
for all $e_2 \in \mathrm{CSD}(H', s', w/2)$
  $x \leftarrow s + e_2 H''^T$
  for all $e_1 \in T[x]$
    $\mathcal{I} \leftarrow \mathcal{I} \cup \{(e_1, e_2)\}$
return $\mathcal{I}$

$$H = \begin{array}{c} \\ r\updownarrow \end{array} \begin{bmatrix} H'' \\ \hline H' \end{bmatrix} \qquad s = \begin{bmatrix} s'' \\ \hline s' \end{bmatrix}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \frac{\binom{n}{w/2}^2}{2^{n-k+r}} \text{ column operations}$$

Improved Birthday Decoding – Algorithm

$\texttt{for all } e_1 \in \mathrm{CSD}(H', 0, w/2)$
$\quad x \leftarrow e_1 H''^T \; ; \; T[x] \leftarrow T[x] \cup \{e_1\}$
$\texttt{for all } e_2 \in \mathrm{CSD}(H', s', w/2)$
$\quad x \leftarrow s + e_2 H''^T$
$\quad \texttt{for all } e_1 \in T[x]$
$\quad\quad \mathcal{I} \leftarrow \mathcal{I} \cup \{(e_1, e_2)\}$
$\texttt{return } \mathcal{I}$

$$H = \begin{array}{r} \\ r \updownarrow \end{array} \begin{bmatrix} H'' \\ \hline H' \end{bmatrix} \qquad s = \begin{bmatrix} s'' \\ \hline s' \end{bmatrix}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \frac{\binom{n}{w/2}^2}{2^{n-k+r}} \text{ column operations}$$

Replacing $2^r = \binom{w}{w/2}$ and using the identity $\dfrac{\binom{n}{w/2}}{\binom{w}{w/2}} = \dfrac{\binom{n}{w}}{\binom{n-w/2}{w/2}}$

Improved Birthday Decoding – Algorithm

$$
\begin{array}{l}
\texttt{for all } e_1 \in \mathrm{CSD}(H', 0, w/2) \\
\quad x \leftarrow e_1 H''^T \ ;\ T[x] \leftarrow T[x] \cup \{e_1\} \\
\texttt{for all } e_2 \in \mathrm{CSD}(H', s', w/2) \\
\quad x \leftarrow s + e_2 H''^T \\
\quad \texttt{for all } e_1 \in T[x] \\
\qquad \mathcal{I} \leftarrow \mathcal{I} \cup \{(e_1, e_2)\} \\
\texttt{return } \mathcal{I}
\end{array}
$$

$$H = \begin{array}{c} \\ r \updownarrow \end{array} \begin{array}{|c|} \hline H'' \\ \hline H' \\ \hline \end{array} \qquad s = \begin{array}{|c|} \hline s'' \\ \hline s' \\ \hline \end{array}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \frac{\binom{n}{w/2}^2}{2^{n-k+r}} \text{ column operations}$$

Replacing $2^r = \binom{w}{w/2}$ and using the identity $\frac{\binom{n}{w/2}}{\binom{w}{w/2}} = \frac{\binom{n}{w}}{\binom{n-w/2}{w/2}}$

$$\sqrt{\binom{n}{w/2}} + \boxed{\frac{\binom{n}{w}}{\binom{n-w/2}{w/2}}} + \frac{\binom{n}{w}}{2^{n-k}} \frac{\binom{n}{w/2}}{\binom{n-w/2}{w/2}}$$

Improved Birthday Decoding – Algorithm

```
for all e_1 ∈ CSD(H', 0, w/2)
    x ← e_1 H''^T ; T[x] ← T[x] ∪ {e_1}
for all e_2 ∈ CSD(H', s', w/2)
    x ← s + e_2 H''^T
    for all e_1 ∈ T[x]
        I ← I ∪ {(e_1, e_2)}
return I
```

$$H = \begin{array}{c} \\ r\updownarrow \end{array}\begin{bmatrix} H'' \\ \hline H' \end{bmatrix} \qquad s = \begin{bmatrix} s'' \\ \hline s' \end{bmatrix}$$

$$\sqrt{\binom{n}{w/2}} + \frac{\binom{n}{w/2}}{2^r} + \frac{\binom{n}{w/2}^2}{2^{n-k+r}} \text{ column operations}$$

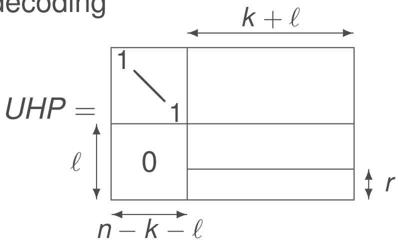
Replacing $2^r = \binom{w}{w/2}$ and using the identity $\frac{\binom{n}{w/2}}{\binom{w}{w/2}} = \frac{\binom{n}{w}}{\binom{n-w/2}{w/2}}$

$$\sqrt{\binom{n}{w/2}} + \boxed{\frac{\binom{n}{w}}{\binom{n-w/2}{w/2}}} + \frac{\binom{n}{w}}{2^{n-k}} \frac{\binom{n}{w/2}}{\binom{n-w/2}{w/2}}$$

Asymptotically, we have $\sqrt{\frac{\binom{n}{w}}{2^w}} \cdot 2^{o(w)}$ and we essentially gain a factor $2^{w/2}$

May, Meurer, and Thomae Algorithm

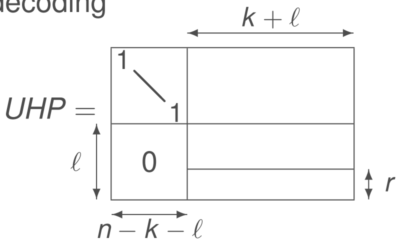
Idea: Dumer Algorithm with the improved birthday decoding



May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding

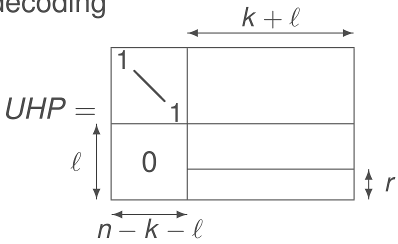
Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$



May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding

Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$



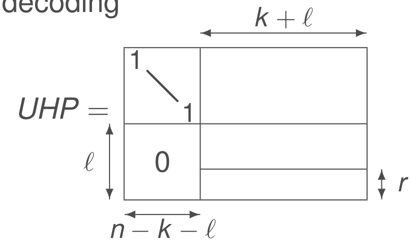
Iteration cost

$$\mathcal{K} = n(n-k-\ell) + \sqrt{\binom{k+\ell}{p/2}} + \frac{\binom{k+\ell}{p}}{\binom{k+\ell-p/2}{p/2}} + \frac{\binom{k+\ell}{p}}{2^\ell}\frac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}$$

May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding

Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$



Iteration cost

$$\mathcal{K} = \cancel{n(n-k-\ell)} + \cancel{\sqrt{\binom{k+\ell}{p/2}}} + \frac{\binom{k+\ell}{p}}{\binom{k+\ell-p/2}{p/2}} + \frac{\binom{k+\ell}{p}}{2^\ell}\frac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}$$

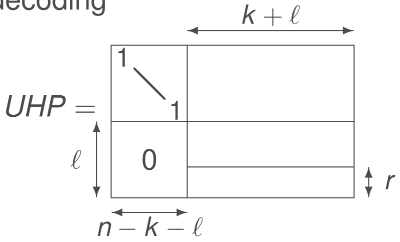
First two terms can be neglected (to be checked *a posteriori*)

May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding

Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$

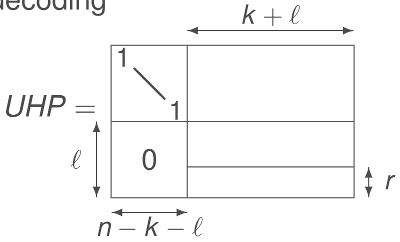
Iteration cost $\mathcal{K} = \dfrac{\binom{k+\ell}{p}}{\binom{k+\ell-p/2}{p/2}} + \dfrac{\binom{k+\ell}{p}}{2^\ell}\dfrac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}$



May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding

Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$



Iteration cost $\mathcal{K} = \dfrac{\binom{k+\ell}{p}}{\binom{k+\ell-p/2}{p/2}} + \dfrac{\binom{k+\ell}{p}}{2^\ell}\dfrac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}$

Workfactor is $\mathcal{N}_\infty \cdot \mathcal{K} = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}}\left(\dfrac{1}{\binom{k+\ell-p/2}{p/2}} + \dfrac{1}{2^\ell}\dfrac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}\right)$

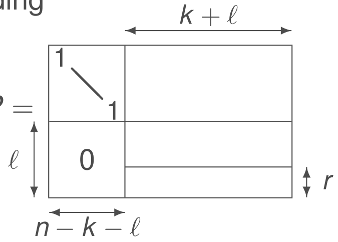
minimal when the two terms are equal, *i.e.* $2^\ell = \binom{k+\ell}{p/2}$

May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding

Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$

$UHP =$

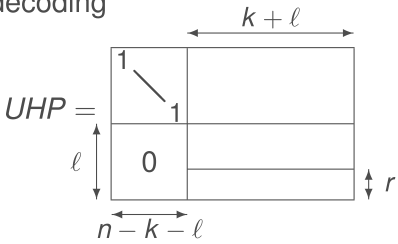


Iteration cost $\mathcal{K} = \dfrac{\binom{k+\ell}{p}}{\binom{k+\ell-p/2}{p/2}} + \dfrac{\binom{k+\ell}{p}}{2^\ell}\dfrac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}$

$$\mathrm{WF}_{\mathrm{MMT}} = \min_p \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell-p/2}{p/2}} \text{ with } \ell = \log_2 \binom{k+\ell}{p/2}$$

May, Meurer, and Thomae Algorithm

Idea: Dumer Algorithm with the improved birthday decoding



Number of iterations $\mathcal{N}_\infty = \dfrac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell}{p}}$

Iteration cost $\mathcal{K} = \dfrac{\binom{k+\ell}{p}}{\binom{k+\ell-p/2}{p/2}} + \dfrac{\binom{k+\ell}{p}}{2^\ell}\dfrac{\binom{k+\ell}{p/2}}{\binom{k+\ell-p/2}{p/2}}$

$$\mathrm{WF}_{\mathrm{MMT}} = \min_p \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\binom{k+\ell-p/2}{p/2}} \text{ with } \ell = \log_2 \binom{k+\ell}{p/2}$$

Asymptotic gain $\approx 2^{p/2}$ compared with Dumer's algorithm

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