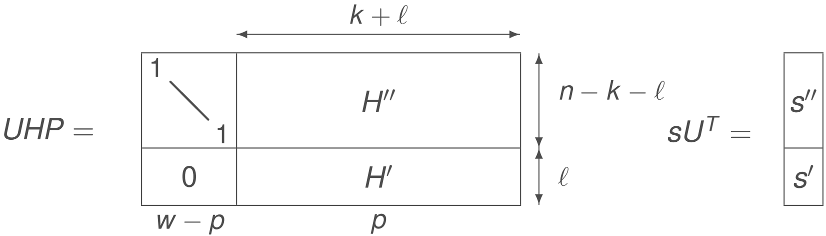
3. Message Attack (ISD)

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

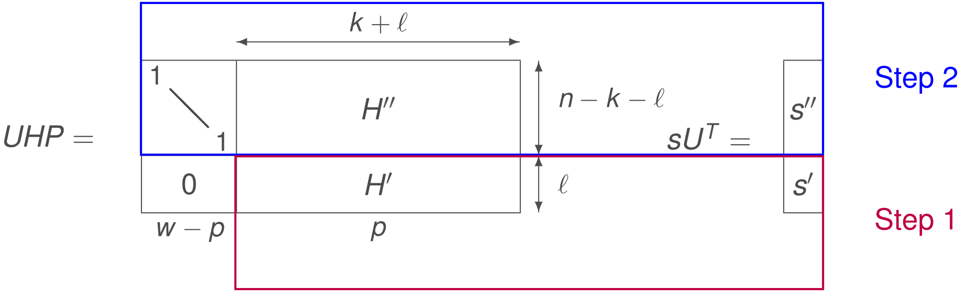
Stern Algorithm – Dumer Algorithm

Idea: combine Lee & Brickell algorithm and birthday decoding



Stern Algorithm – Dumer Algorithm

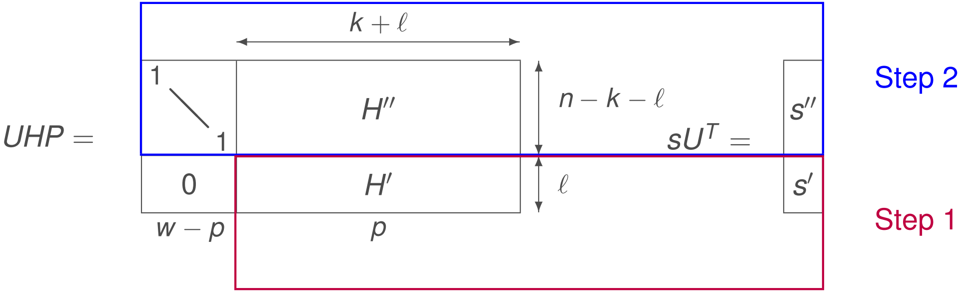
Idea: combine Lee & Brickell algorithm and birthday decoding



Step 1: Find all $e' \in \mathrm{CSD}(H', s', p)$
Step 2: Check $\mathrm{wt}(e' H''^T + s'') = w - p$

Stern Algorithm – Dumer Algorithm

Idea: combine Lee & Brickell algorithm and birthday decoding

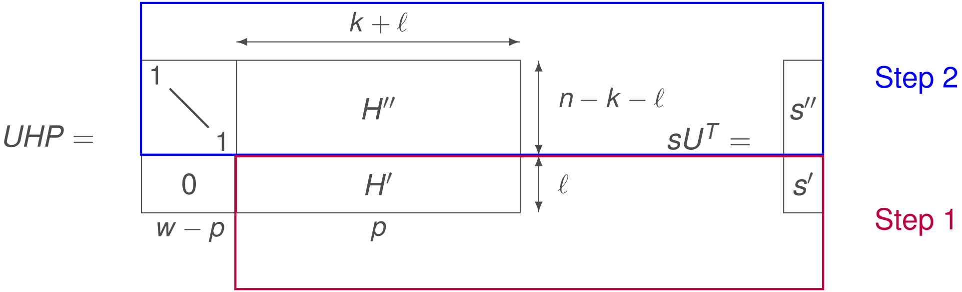


Step 1: Find all $e' \in \mathrm{CSD}(H', s', p)$
Step 2: Check $\mathrm{wt}(e'H''^T + s'') = w - p$

If step 1 is solved by enumeration $\rightarrow$ similar to Lee & Brickell

Stern Algorithm – Dumer Algorithm

Idea: combine Lee & Brickell algorithm and birthday decoding



Step 1: Find all $e' \in \mathrm{CSD}(H', s', p)$
Step 2: Check $\mathrm{wt}(e'H''^T + s'') = w - p$

If step 1 is solved by enumeration $\rightarrow$ similar to Lee & Brickell

If step 1 is solved by birthday decoding $\rightarrow$ Dumer Algorithm

Dumer Algorithm

input: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, integer $w > 0$, two parameters p and ℓ

output: $e \in \{0,1\}^n$ such that $eH^T = s$ and $\mathrm{wt}(e) = w$

Dumer Algorithm

input: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, integer $w > 0$, two parameters p and ℓ

output: $e \in \{0,1\}^n$ such that $eH^T = s$ and $\mathrm{wt}(e) = w$

repeat:

  pick a permutation matrix P

Dumer Algorithm

input: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, integer $w > 0$, two parameters p and ℓ
output: $e \in \{0,1\}^n$ such that $eH^T = s$ and $\mathrm{wt}(e) = w$

repeat:
    pick a permutation matrix P
    compute U, H', H'', s', s''

$$UHP = \left(\begin{array}{c|c} 1 \ddots 1 & H'' \\ \hline 0 & H' \end{array}\right) \updownarrow \ell$$

$$sU^T = \left(\begin{array}{c} s'' \\ \hline s' \end{array}\right)$$

Dumer Algorithm

input: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, integer $w > 0$, two parameters p and ℓ

output: $e \in \{0,1\}^n$ such that $eH^T = s$ and $\mathrm{wt}(e) = w$

repeat:

- pick a permutation matrix P
- compute U, H', H'', s', s''
- solve CSD(H', s', p) *(birthday decoding)*

$$UHP = \begin{pmatrix} \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} & H'' \\ 0 & H' \end{pmatrix} \quad \updownarrow \ell$$

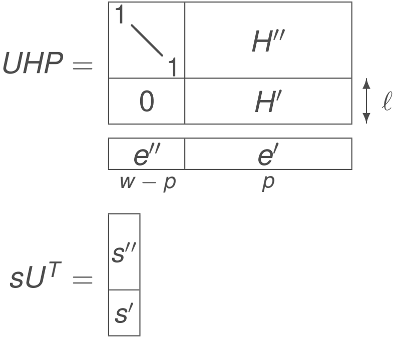
$$sU^T = \begin{pmatrix} s'' \\ s' \end{pmatrix}$$

Dumer Algorithm

input: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, integer $w > 0$, two parameters p and ℓ

output: $e \in \{0,1\}^n$ such that $eH^T = s$ and $\mathrm{wt}(e) = w$

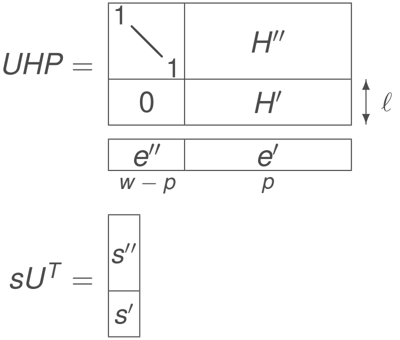
repeat:
    pick a permutation matrix P
    compute U, H', H'', s', s''
    solve $\mathrm{CSD}(H', s', p)$ *(birthday decoding)*
    for all $e' \in \mathrm{CSD}(H', s', p)$
        $e'' \leftarrow e' H''^T + s''$
        if $\mathrm{wt}(e'') = w - p$
            return $(e'', e')P$



Dumer Algorithm

input: $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, integer $w > 0$, two parameters p and ℓ
output: $e \in \{0,1\}^n$ such that $eH^T = s$ and $\mathrm{wt}(e) = w$

repeat:
- pick a permutation matrix P
- compute U, H', H'', s', s''
- solve $\mathrm{CSD}(H', s', p)$ *(birthday decoding)*
- for all $e' \in \mathrm{CSD}(H', s', p)$
  - $e'' \leftarrow e' H''^T + s''$
  - if $\mathrm{wt}(e'') = w - p$
    - return $(e'', e')P$



Note: Stern's algorithm (1989) was the first to use birthday decoding, Dumer's algorithm (1991) is only marginally better

We will refer now to the Stern/Dumer Algorithm

Stern/Dumer Algorithm – Complexity Analysis (1/2)

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

Stern/Dumer Algorithm – Complexity Analysis (1/2)

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

Gaussian elimination

Stern/Dumer Algorithm – Complexity Analysis (1/2)

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

Gaussian elimination

Birthday decoding

Stern/Dumer Algorithm – Complexity Analysis (1/2)

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

Gaussian elimination

Birthday decoding

Final check

Stern/Dumer Algorithm – Complexity Analysis (1/2)

In general, we can write

$$\mathcal{K} = K_0 \cdot n(n-k-\ell) + K_1 \cdot \sqrt{\binom{k+\ell}{p}} + K_2 \cdot \frac{\binom{k+\ell}{p}}{2^\ell}$$

where K_0, K_1, and K_2 are small (implementation dependent) constants

we will set $K_0 = K_1 = K_2 = 1$ to simplify the formula

Stern/Dumer Algorithm – Complexity Analysis (1/2)

We will simply write $\mathcal{K} = n(n-k-\ell) + \sqrt{\binom{k+\ell}{p}} + \frac{\binom{k+\ell}{p}}{2^\ell}$ up to a constant factor

Stern/Dumer Algorithm – Complexity Analysis (1/2)

We will simply write $\mathcal{K} = n(n-k-\ell) + \sqrt{\binom{k+\ell}{p}} + \frac{\binom{k+\ell}{p}}{2^\ell}$ up to a constant factor

Success probability: $\mathcal{P}_\infty = \frac{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}{\binom{n}{w}}$ and $\mathcal{N}_\infty = \frac{1}{\mathcal{P}_\infty} = \frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}$

Stern/Dumer Algorithm – Complexity Analysis (1/2)

We will simply write $\mathcal{K} = n(n-k-\ell) + \sqrt{\binom{k+\ell}{p}} + \frac{\binom{k+\ell}{p}}{2^\ell}$ up to a constant factor

Success probability: $\mathcal{P}_\infty = \frac{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}{\binom{n}{w}}$ and $\mathcal{N}_\infty = \frac{1}{\mathcal{P}_\infty} = \frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}$

Workfactor $\mathrm{WF}_{\mathrm{SD}}(p,\ell) = \mathcal{N}_\infty \cdot \mathcal{K} = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{n(n-k+\ell)}{\binom{k+\ell}{p}} + \frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^\ell} \right)$

Stern/Dumer Algorithm – Complexity Analysis (1/2)

We will simply write $\mathcal{K} = n(n-k-\ell) + \sqrt{\binom{k+\ell}{p}} + \frac{\binom{k+\ell}{p}}{2^\ell}$ up to a constant factor

Success probability: $\mathcal{P}_\infty = \frac{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}{\binom{n}{w}}$ and $\mathcal{N}_\infty = \frac{1}{\mathcal{P}_\infty} = \frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}$

Workfactor $\mathrm{WF}_{\mathrm{SD}}(p,\ell) = \mathcal{N}_\infty \cdot \mathcal{K} = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{n(n-k+\ell)}{\binom{k+\ell}{p}} + \frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^\ell} \right)$

(up to a constant factor)

Stern/Dumer Algorithm – Complexity Analysis (1/2)

We will simply write $\mathcal{K} = n(n-k-\ell) + \sqrt{\binom{k+\ell}{p}} + \frac{\binom{k+\ell}{p}}{2^\ell}$ up to a constant factor

Success probability: $\mathcal{P}_\infty = \frac{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}{\binom{n}{w}}$ and $\mathcal{N}_\infty = \frac{1}{\mathcal{P}_\infty} = \frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}$

$$\text{Workfactor } \mathrm{WF}_{\mathrm{SD}}(p,\ell) = \mathcal{N}_\infty \cdot \mathcal{K} = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{n(n-k+\ell)}{\binom{k+\ell}{p}} + \frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^\ell} \right)$$

(up to a constant factor)

To be minimized over p and ℓ (positive integers)

Stern/Dumer Algorithm – Complexity Analysis (2/2)

The optimization parameters p and ℓ grow with the problem parameters (n, k, w)

$$\mathrm{WF}_{\mathrm{SD}}(p, \ell) = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{n(n-k+\ell)}{\binom{k+\ell}{p}} + \frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^{\ell}} \right)$$

Stern/Dumer Algorithm – Complexity Analysis (2/2)

The optimization parameters p and ℓ grow with the problem parameters (n, k, w)

For cryptographic parameters, the Gaussian elimination will never dominate

$$\mathrm{WF}_{\mathrm{SD}}(p,\ell) = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\cancel{\frac{n(n-k+\ell)}{\binom{k+\ell}{p}}} + \frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^{\ell}} \right)$$

Stern/Dumer Algorithm – Complexity Analysis (2/2)

The optimization parameters p and ℓ grow with the problem parameters (n, k, w)

For cryptographic parameters, the Gaussian elimination will never dominate and we have a good estimate with

$$\mathrm{WF}_{\mathrm{SD}}(p, \ell) = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^{\ell}} \right)$$

Stern/Dumer Algorithm – Complexity Analysis (2/2)

The optimization parameters p and ℓ grow with the problem parameters (n, k, w)

For cryptographic parameters, the Gaussian elimination will never dominate and we have a good estimate with

$$\mathrm{WF}_{\mathrm{SD}}(p,\ell) = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^\ell} \right)$$

In most situations, the above formula is minimal when the addends are equal

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

Stern/Dumer Algorithm – Complexity Analysis (2/2)

The optimization parameters p and ℓ grow with the problem parameters (n, k, w)

For cryptographic parameters, the Gaussian elimination will never dominate and we have a good estimate with

$$\mathrm{WF}_{\mathrm{SD}}(p,\ell) = \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}} \left(\frac{1}{\sqrt{\binom{k+\ell}{p}}} + \frac{1}{2^\ell} \right)$$

In most situations, the above formula is minimal when the addends are equal

$$\mathrm{WF}_{\mathrm{SD}} = \min_{0 \le p \le w} \frac{\binom{n}{w}}{\binom{n-k-\ell}{w-p}\sqrt{\binom{k+\ell}{p}}} \text{ with } \ell = \log_2 \sqrt{\binom{k+\ell}{p}}$$

(up to a 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