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

Further Improvement of Birthday Decoding

$$\mathcal{L}_1(r,\varepsilon) = \{e_1 H^T \mid \mathrm{wt}(e_1) = \tfrac{w}{2} + \varepsilon, \phi_r(e_1 H^T) = 0\}$$
$$\mathcal{L}_2(r,\varepsilon) = \{s + e_2 H^T \mid \mathrm{wt}(e_2) = \tfrac{w}{2} + \varepsilon, \phi_r(s + e_2 H^T) = 0\}$$

Further Improvement of Birthday Decoding

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

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

Idea: two words of weight $\frac{w}{2}$ and length n are expected to have

$$\begin{cases} \frac{w^2}{4n} \text{ non-zero positions in common} \\ \text{a sum of weight } w - \frac{w^2}{2n} \end{cases}$$

Further Improvement of Birthday Decoding

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

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

Idea: if $\varepsilon = \frac{(w/2+\varepsilon)^2}{n}$, two words of weight $\frac{w}{2} + \varepsilon$ and length n are expected to have

$$\begin{cases} \varepsilon \quad \text{non-zero positions in common} \\ \text{a sum of weight } w \end{cases}$$

Further Improvement of Birthday Decoding

$$\mathcal{L}_1(r,\varepsilon) = \{e_1 H^T \mid \mathrm{wt}(e_1) = \tfrac{w}{2} + \varepsilon, \phi_r(e_1 H^T) = 0\}$$
$$\mathcal{L}_2(r,\varepsilon) = \{s + e_2 H^T \mid \mathrm{wt}(e_2) = \tfrac{w}{2} + \varepsilon, \phi_r(s + e_2 H^T) = 0\}$$

Idea: if $\varepsilon = \frac{(w/2+\varepsilon)^2}{n}$, two words of weight $\frac{w}{2} + \varepsilon$ and length n are expected to have

$$\begin{cases} \varepsilon \ \text{ non-zero positions in common} \\ \text{a sum of weight } w \end{cases}$$

Note also that there are $\binom{w}{w/2}\binom{n-w}{\varepsilon}$ different ways to write $e = e_1 + e_2$ with $\mathrm{wt}(e) = w$ and $\mathrm{wt}(e_1) = \mathrm{wt}(e_2) = \frac{w}{2} + \varepsilon$

Further Improvement of Birthday Decoding

$$\mathcal{L}_1(r,\varepsilon) = \{e_1 H^T \mid \mathrm{wt}(e_1) = \frac{w}{2} + \varepsilon, \phi_r(e_1 H^T) = 0\}$$

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

Claim: Let $2^r = \binom{w}{w/2}\binom{n-w}{\varepsilon}$ and $\varepsilon = \frac{(w/2+\varepsilon)^2}{n}$
Any $e \in \mathrm{CSD}(H, s, w)$ is "represented in $\mathcal{L}_1(r,\varepsilon) \cap \mathcal{L}_2(r,\varepsilon)$" with probability $> 1/2$

Further Improvement of Birthday Decoding

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

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

Claim: Let $2^r = \binom{w}{w/2}\binom{n-w}{\varepsilon}$ and $\varepsilon = \frac{(w/2+\varepsilon)^2}{n}$
Any $e \in \mathrm{CSD}(H,s,w)$ is "represented in $\mathcal{L}_1(r,\varepsilon) \cap \mathcal{L}_2(r,\varepsilon)$" with probability $> 1/2$

Workfactor "simplifies" to

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

(up to a polynomial factor)

Impact on MMT Algorithm Complexity

Instead of

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

(up to a constant factor)

Impact on MMT Algorithm Complexity

Instead of

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

(up to a constant factor)

We set $\varepsilon = \frac{(w/2+\varepsilon)^2}{n}$, and the workfactor reduces to

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

(up to a polynomial factor)

Impact on MMT Algorithm Complexity

Instead of

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

(up to a constant factor)

We set $\varepsilon = \frac{(w/2+\varepsilon)^2}{n}$, and the workfactor reduces to

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

(up to a polynomial factor)

This is the embryo of the next improvement of ISD

Becker, Joux, May, and Meurer Algorithm (1/2)

Idea: what happens if we let ε grows (much) beyond $w^2/4n$?

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

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

Becker, Joux, May, and Meurer Algorithm (1/2)

Idea: what happens if we let ε grows (much) beyond $w^2/4n$?

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

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

The workfactor becomes $\sqrt{L} + \frac{L}{2^r} + \frac{L^2}{2^{n-k+r}}$ with $L = \binom{n}{w/2+\varepsilon}$ and $2^r = \binom{w}{w/2}\binom{n-w}{\varepsilon}$

Becker, Joux, May, and Meurer Algorithm (1/2)

Idea: what happens if we let ε grows (much) beyond $w^2/4n$?

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

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

The workfactor becomes $\sqrt{L} + \dfrac{L}{2^r} + \dfrac{L^2}{2^{n-k+r}}$ with $L = \binom{n}{w/2+\varepsilon}$ and $2^r = \binom{w}{w/2}\binom{n-w}{\varepsilon}$

We may also write $\sqrt{L} + \dfrac{1}{\mu}\dfrac{\binom{n}{w}}{L} + \dfrac{1}{\mu}\dfrac{\binom{n}{w}}{2^{n-k}}$

where $\mu = \dfrac{\binom{w/2+\varepsilon}{\varepsilon}\binom{n-w/2-\varepsilon}{w/2}}{\binom{n}{w/2+\varepsilon}}$ is the probability that two words of weight $w/2+\varepsilon$ and length n have a sum of weight w

BJMM Algorithm (2/2)

BJMM Algorithm, key features:

- increase ε leading to FIBD (Further Improved Birthday Decoding)
- make an additional level of recursive call to FIBD
  (improved birthday decoding makes two calls to smaller CSD problems)
- embed all this into Information Set Decoding framework

BJMM Algorithm (2/2)

BJMM Algorithm, key features:

- increase ε leading to FIBD (Further Improved Birthday Decoding)
- make an additional level of recursive call to FIBD
  (improved birthday decoding makes two calls to smaller CSD problems)
- embed all this into Information Set Decoding framework

Improves the workfactor

Algorithm and analysis are very elaborated

Comparison of the Various ISD Variants

$$\mathrm{WF} = 2^{c \cdot n(1+o(1))}$$

c a constant
(asymptotic exponent)

Comparison of the Various ISD Variants

	$c = \lim_{n\to\infty} \frac{\log_2 \mathrm{WF}}{n}$	
	$k = 0.5n$ $w = 0.11n$	
Enumeration	0.5	
Birthday Decoding	0.25	
Prange	0.1198	
Stern	0.1154	
Dumer	0.1151	
MMT	0.1101	
BJMM	0.1000	

$\mathrm{WF} = 2^{c \cdot n(1+o(1))}$

c a constant
(asymptotic exponent)

Comparison of the Various ISD Variants

	$c = \lim_{n\to\infty} \frac{\log_2 \text{WF}}{n}$	
	$k = 0.5n$ $w = 0.11n$	$k = 0.8n$ $w = 0.03n$
Enumeration	0.5	0.2
Birthday Decoding	0.25	0.1
Prange	0.1198	0.0724
Stern	0.1154	0.0680
Dumer	0.1151	0.0679
MMT	0.1101	0.0638
BJMM	0.1000	0.0562

$\text{WF} = 2^{c \cdot n(1+o(1))}$

c a constant
(asymptotic exponent)

Comparison of the Various ISD Variants

	$c = \lim_{n\to\infty} \frac{\log_2 \mathrm{WF}}{n}$	
	$k = 0.5n$ $w = 0.11n$	$k = 0.8n$ $w = 0.03n$
Enumeration	0.5	0.2
Birthday Decoding	0.25	0.1
Prange	0.1198	0.0724
Stern	0.1154	0.0680
Dumer	0.1151	0.0679
MMT	0.1101	0.0638
BJMM	0.1000	0.0562

$\mathrm{WF} = 2^{c \cdot n(1+o(1))}$

c a constant
(asymptotic exponent)

Remark that Birthday Decoding is comparatively better when k/n grows

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