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

ISD – Complexity Analysis

We will refer to Information Set Decoding (ISD) to designate is a family of algorithms similar to Prange algorithm

All variants of Information Set Decoding repeat a (large) number of times an independent iteration which has

- a constant (expected) cost $\mathcal{K}$
- a success probability $\mathcal{P}$
  $\rightarrow$ an expected number of iteration $\mathcal{N} = 1/\mathcal{P}$

The workfactor is $\mathcal{N} \cdot \mathcal{K}$

ISD – One Solution or All Solutions?

We consider the problem CSD(H, s, w) with $H \in \{0,1\}^{(n-k)\times n}$ and $s \in \{0,1\}^{n-k}$

ISD – One Solution or All Solutions?

We consider the problem CSD(H, s, w) with $H \in \{0,1\}^{(n-k)\times n}$ and $s \in \{0,1\}^{n-k}$

We assume that CSD$(H, s, w) \neq \emptyset$ (*i.e.* $s \in \{eH^T \mid \mathrm{wt}(e) = w\}$)

$\rightarrow$ **there is always at least one solution**

ISD – One Solution or All Solutions?

We consider the problem CSD(H, s, w) with $H \in \{0,1\}^{(n-k)\times n}$ and $s \in \{0,1\}^{n-k}$

We assume that CSD$(H, s, w) \neq \emptyset$ (*i.e.* $s \in \{eH^T \mid \mathrm{wt}(e) = w\}$)

$\rightarrow$ **there is always at least one solution**

1. If $\binom{n}{w} < 2^{n-k}$ (*i.e.* $w < \tau_{\mathrm{GV}}$) there is exactly one solution
2. If $\binom{n}{w} > 2^{n-k}$ (*i.e.* $w > \tau_{\mathrm{GV}}$) there are $\binom{n}{w}/2^{n-k}$ solutions (on average)

ISD – One Solution or All Solutions?

We consider the problem CSD(H, s, w) with $H \in \{0,1\}^{(n-k)\times n}$ and $s \in \{0,1\}^{n-k}$

We assume that CSD$(H, s, w) \neq \emptyset$ (*i.e.* $s \in \{eH^T \mid \mathrm{wt}(e) = w\}$)

$\rightarrow$ **there is always at least one solution**

1. If $\binom{n}{w} < 2^{n-k}$ (*i.e.* $w < \tau_{\mathrm{GV}}$) there is exactly one solution
2. If $\binom{n}{w} > 2^{n-k}$ (*i.e.* $w > \tau_{\mathrm{GV}}$) there are $\binom{n}{w}/2^{n-k}$ solutions (on average)

First case (the most common) $\rightarrow$ no difference

ISD – One Solution or All Solutions?

We consider the problem CSD(H, s, w) with $H \in \{0,1\}^{(n-k)\times n}$ and $s \in \{0,1\}^{n-k}$

We assume that CSD$(H, s, w) \neq \emptyset$ (*i.e.* $s \in \{eH^T \mid \mathrm{wt}(e) = w\}$)

$\rightarrow$ **there is always at least one solution**

1. If $\binom{n}{w} < 2^{n-k}$ (*i.e.* $w < \tau_{\mathrm{GV}}$) there is exactly one solution
2. If $\binom{n}{w} > 2^{n-k}$ (*i.e.* $w > \tau_{\mathrm{GV}}$) there are $\binom{n}{w}/2^{n-k}$ solutions (on average)

First case (the most common) $\rightarrow$ no difference

Second case $\rightarrow$ finding only one solution should be easier

(intuitively by a factor $\binom{n}{w}/2^{n-k}$)

ISD – Probabilities

ISD performs many independent iterations. For one iteration, we denote

- $\mathcal{P}_\infty$ the probability to find one specific element of $\mathrm{CSD}(H, s, w)$

ISD – Probabilities

ISD performs many independent iterations. For one iteration, we denote

- $\mathcal{P}_\infty$ the probability to find one specific element of $\mathrm{CSD}(H, s, w)$
- $\mathcal{P}_1$ the probability to find any one element of $\mathrm{CSD}(H, s, w)$

  If $N = |\mathrm{CSD}(H, s, w)|$, we have

  $$\mathcal{P}_1 = 1 - (1 - \mathcal{P}_\infty)^N \approx \min(1, N\mathcal{P}_\infty)$$ up to a small constant factor

  or simply $\mathcal{P}_1 = N\mathcal{P}_\infty$ if N is not too large (which corresponds to intuition)

ISD – Probabilities

ISD performs many independent iterations. For one iteration, we denote

- $\mathcal{P}_\infty$ the probability to find one specific element of CSD(H, s, w)
- $\mathcal{P}_1$ the probability to find any one element of CSD(H, s, w)

  If $N = |\text{CSD}(H, s, w)|$, we have

  $$\mathcal{P}_1 = 1 - (1 - \mathcal{P}_\infty)^N \approx \min(1, N\mathcal{P}_\infty)$$ up to a small constant factor

  or simply $\mathcal{P}_1 = N\mathcal{P}_\infty$ if N is not too large (which corresponds to intuition)

For the complexity analysis, there are two situations

- "$w < \tau_{\text{GV}}$" or "$w > \tau_{\text{GV}}$ and we want all solutions"
  $\rightarrow$ we expect to execute $\mathcal{N}_\infty = 1/\mathcal{P}_\infty$ iterations

ISD – Probabilities

ISD performs many independent iterations. For one iteration, we denote

- $\mathcal{P}_\infty$ the probability to find one specific element of CSD(H, s, w)
- $\mathcal{P}_1$ the probability to find any one element of CSD(H, s, w)

  If $N = |\text{CSD}(H, s, w)|$, we have

  $$\mathcal{P}_1 = 1 - (1 - \mathcal{P}_\infty)^N \approx \min(1, N\mathcal{P}_\infty)$$ up to a small constant factor

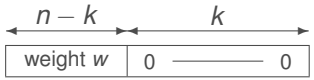
  or simply $\mathcal{P}_1 = N\mathcal{P}_\infty$ if N is not too large (which corresponds to intuition)

For the complexity analysis, there are two situations

- "$w < \tau_{\text{GV}}$" or "$w > \tau_{\text{GV}}$ and we want all solutions"
  $\rightarrow$ we expect to execute $\mathcal{N}_\infty = 1/\mathcal{P}_\infty$ iterations
- "$w > \tau_{\text{GV}}$ and we want only one solution"
  $\rightarrow$ we expect to execute $\mathcal{N}_1 = \mathcal{N}_\infty / N = \frac{2^{n-k}}{\binom{n}{w}\mathcal{P}_\infty}$ iterations

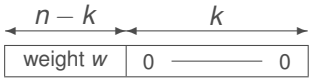
Prange Algorithm – Complexity Analysis

An error pattern is found if it has the following form $e =$



Prange Algorithm – Complexity Analysis

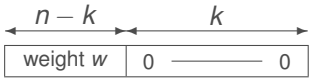
An error pattern is found if it has the following form $e =$



It follows that $\mathcal{P}_\infty = \frac{\binom{n-k}{w}}{\binom{n}{w}}$ and $\mathcal{P}_1 = \frac{\binom{n-k}{w}}{\min(2^{n-k}, \binom{n}{w})}$

Prange Algorithm – Complexity Analysis

An error pattern is found if it has the following form $e =$

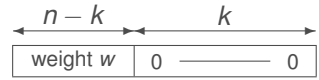


It follows that $\mathcal{P}_\infty = \frac{\binom{n-k}{w}}{\binom{n}{w}}$ and $\mathcal{P}_1 = \frac{\binom{n-k}{w}}{\min(2^{n-k}, \binom{n}{w})}$

$\mathcal{K} = n(n-k)$ column operations (the Gaussian elimination dominates)

Prange Algorithm – Complexity Analysis

An error pattern is found if it has the following form $e =$



It follows that $\mathcal{P}_\infty = \frac{\binom{n-k}{w}}{\binom{n}{w}}$ and $\mathcal{P}_1 = \frac{\binom{n-k}{w}}{\min(2^{n-k}, \binom{n}{w})}$

$\mathcal{K} = n(n-k)$ column operations (the Gaussian elimination dominates)

Total workfactor is

- for all solutions $\mathrm{WF}_{\mathrm{Prange}} = n(n-k)\frac{\binom{n}{w}}{\binom{n-k}{w}}$
- for one solution $n(n-k)\frac{\min(2^{n-k}, \binom{n}{w})}{\binom{n-k}{w}}$

indeed the values are identical when $\binom{n}{w} < 2^{n-k}$

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