3. Message Attack (ISD)

Generalized Birthday Algorithm

Proposed by D. Wagner in 2002, in a more general context

The Generalized Birthday Algorithm (GBA) of order a solves the following problem:

Instance:	2^a lists of vectors $\mathcal{L}_i \subset \{0,1\}^\ell$, $i = 1, 2, \ldots, 2^a$
Answer:	$x_i \in \mathcal{L}_i$, $i = 1, 2, \ldots, 2^a$ such that $x_1 + x_2 + \ldots + x_{2^a} = 0$

If the lists are large enough, then GBA runs in time $O\left(2^{\ell/(a+1)}\right)$

(the case $a = 1$ corresponds to the usual birthday paradox)

Generalized Birthday Algorithm

Proposed by D. Wagner in 2002, in a more general context

The Generalized Birthday Algorithm (GBA) of order *a* solves the following problem:

Instance:	2^a lists of vectors $\mathcal{L}_i \subset \{0,1\}^\ell$, $i = 1, 2, \ldots, 2^a$
Answer:	$x_i \in \mathcal{L}_i$, $i = 1, 2, \ldots, 2^a$ such that $x_1 + x_2 + \ldots + x_{2^a} = 0$

If the lists are large enough, then GBA runs in time $O\left(2^{\ell/(a+1)}\right)$

(the case $a = 1$ corresponds to the usual birthday paradox)

GBA can be applied to decoding

- it applies to instances of CSD with many solutions
- it aims at finding one solution only

Birthday Decoding Again

Let $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, and $w > 0$, we consider CSD(H, s, w) where

- there are many solutions: exact condition to be determined
- we only want one solution

$$H = \begin{array}{|c|c|} \hline \quad H_1 \quad & \quad H_2 \quad \\ \hline \end{array}$$

$s = s_1 + s_2$ arbitrarily

Birthday Decoding Again

Let $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, and $w > 0$, we consider CSD(H, s, w) where

- there are many solutions: exact condition to be determined
- we only want one solution

We build two lists of size L

$$\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/2\}, i \in \{1,2\}$$

Any element of $\mathcal{L}_1 \cap \mathcal{L}_2$ provides a solution

$$H = \left[\begin{array}{c|c} \quad H_1 \quad & \quad H_2 \quad \end{array}\right]$$

$s = s_1 + s_2$ arbitrarily

Birthday Decoding Again

Let $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, and $w > 0$, we consider $\mathrm{CSD}(H, s, w)$ where

- there are many solutions: exact condition to be determined
- we only want one solution

$$H = \begin{array}{|c|c|}\hline \quad H_1 \quad & \quad H_2 \quad \\ \hline \end{array}$$

$s = s_1 + s_2$ arbitrarily

We build two lists of size L

$$\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/2\}, i \in \{1,2\}$$

Any element of $\mathcal{L}_1 \cap \mathcal{L}_2$ provides a solution

We must have $|\mathcal{L}_1 \cap \mathcal{L}_2| = \dfrac{L^2}{2^{n-k}} \geq 1$

Birthday Decoding Again

Let $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, and $w > 0$, we consider CSD(H, s, w) where

- there are many solutions: exact condition to be determined
- we only want one solution

$$H = \begin{array}{|c|c|}\hline \quad H_1 \quad & \quad H_2 \quad \\ \hline \end{array}$$

$s = s_1 + s_2$ arbitrarily

We build two lists of size L

$$\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/2\}, i \in \{1,2\}$$

Any element of $\mathcal{L}_1 \cap \mathcal{L}_2$ provides a solution

We must have $|\mathcal{L}_1 \cap \mathcal{L}_2| = \dfrac{L^2}{2^{n-k}} \geq 1$

Choosing $L = 2^{(n-k)/2}$ the workfactor is $O\left(2^{(n-k)/2}\right)$

Birthday Decoding Again

Let $H \in \{0,1\}^{(n-k)\times n}$, $s \in \{0,1\}^{n-k}$, and $w > 0$, we consider CSD(H, s, w) where

- there are many solutions: $\binom{n/2}{w/2}^2 \geq 2^{n-k}$
- we only want one solution

$$H = \begin{array}{|c|c|} \hline \quad H_1 \quad & \quad H_2 \quad \\ \hline \end{array}$$

$s = s_1 + s_2$ arbitrarily

We build two lists of size L

$$\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/2\}, i \in \{1, 2\}$$

Any element of $\mathcal{L}_1 \cap \mathcal{L}_2$ provides a solution

We must have $|\mathcal{L}_1 \cap \mathcal{L}_2| = \dfrac{L^2}{2^{n-k}} \geq 1$

Choosing $L = 2^{(n-k)/2}$ the workfactor is $O\left(2^{(n-k)/2}\right)$

L cannot exceed $\binom{n/2}{w/2}$, and thus we need $\binom{n/2}{w/2}^2 \geq 2^{n-k}$

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|}\hline \quad H_1 \quad & \quad H_2 \quad & \quad H_3 \quad & \quad H_4 \quad \\ \hline\end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline \quad H_1 \quad & \quad H_2 \quad & \quad H_3 \quad & \quad H_4 \quad \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1, 2, 3, 4\}$

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline \quad H_1 \quad & \quad H_2 \quad & \quad H_3 \quad & \quad H_4 \quad \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1, 2, 3, 4\}$ of size $L = 2^\ell$, $\ell = (n-k)/3$

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline H_1 & H_2 & H_3 & H_4 \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1, 2, 3, 4\}$ of size $L = 2^\ell$, $\ell = (n-k)/3$

Let $\mathcal{L}_{1,2} \subset \{x_1 + x_2 \mid x_1 \in \mathcal{L}_i, x_2 \in \mathcal{L}_2, \phi_\ell(x_1 + x_2) = 0\}$ ($\phi_\ell(x)$ the last ℓ bits of x)

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline H_1 & H_2 & H_3 & H_4 \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1, 2, 3, 4\}$ of size $L = 2^\ell$, $\ell = (n-k)/3$

Let $\mathcal{L}_{1,2} \subset \{x_1 + x_2 \mid x_1 \in \mathcal{L}_i, x_2 \in \mathcal{L}_2, \phi_\ell(x_1 + x_2) = 0\}$ ($\phi_\ell(x)$ the last ℓ bits of x)

We define $\mathcal{L}_{3,4}$ similarly, we expect $|\mathcal{L}_{1,2}| = |\mathcal{L}_{3,4}| = L^2/2^\ell = L$

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline H_1 & H_2 & H_3 & H_4 \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1, 2, 3, 4\}$ of size $L = 2^\ell$, $\ell = (n-k)/3$

Let $\mathcal{L}_{1,2} \subset \{x_1 + x_2 \mid x_1 \in \mathcal{L}_i, x_2 \in \mathcal{L}_2, \phi_\ell(x_1 + x_2) = 0\}$ ($\phi_\ell(x)$ the last ℓ bits of x)

We define $\mathcal{L}_{3,4}$ similarly, we expect $|\mathcal{L}_{1,2}| = |\mathcal{L}_{3,4}| = L^2/2^\ell = L$

We expect $|\mathcal{L}_{1,2} \cap \mathcal{L}_{3,4}| = \dfrac{|\mathcal{L}_{1,2}| \cdot |\mathcal{L}_{3,4}|}{2^{n-k-\ell}} = L^4/2^{n-k+\ell} = 1$

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline \quad H_1 \quad & \quad H_2 \quad & \quad H_3 \quad & \quad H_4 \quad \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1, 2, 3, 4\}$ of size $L = 2^\ell$, $\ell = (n-k)/3$

Let $\mathcal{L}_{1,2} \subset \{x_1 + x_2 \mid x_1 \in \mathcal{L}_i, x_2 \in \mathcal{L}_2, \phi_\ell(x_1 + x_2) = 0\}$ ($\phi_\ell(x)$ the last ℓ bits of x)

We define $\mathcal{L}_{3,4}$ similarly, we expect $|\mathcal{L}_{1,2}| = |\mathcal{L}_{3,4}| = L^2/2^\ell = L$

We expect $|\mathcal{L}_{1,2} \cap \mathcal{L}_{3,4}| = \dfrac{|\mathcal{L}_{1,2}| \cdot |\mathcal{L}_{3,4}|}{2^{n-k-\ell}} = L^4/2^{n-k+\ell} = 1$

After computing $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \mathcal{L}_4, \mathcal{L}_{1,2}, \mathcal{L}_{3,4}$ we expect to find an element in $\mathcal{L}_{1,2} \cap \mathcal{L}_{3,4}$ from which we derive a solution to CSD(H, s, w)

Order 2 GBA for Decoding

$$H = \begin{array}{|c|c|c|c|} \hline H_1 & H_2 & H_3 & H_4 \\ \hline \end{array} \qquad s = s_1 + s_2 + s_3 + s_4$$

Let $\mathcal{L}_i \subset \{s_i + e_i H_i^T \mid \mathrm{wt}(e_i) = w/4\}, i \in \{1,2,3,4\}$ of size $L = 2^\ell$, $\ell = (n-k)/3$

Let $\mathcal{L}_{1,2} \subset \{x_1 + x_2 \mid x_1 \in \mathcal{L}_i, x_2 \in \mathcal{L}_2, \phi_\ell(x_1 + x_2) = 0\}$ ($\phi_\ell(x)$ the last ℓ bits of x)

We define $\mathcal{L}_{3,4}$ similarly, we expect $|\mathcal{L}_{1,2}| = |\mathcal{L}_{3,4}| = L^2/2^\ell = L$

We expect $|\mathcal{L}_{1,2} \cap \mathcal{L}_{3,4}| = \dfrac{|\mathcal{L}_{1,2}| \cdot |\mathcal{L}_{3,4}|}{2^{n-k-\ell}} = L^4/2^{n-k+\ell} = 1$

After computing $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \mathcal{L}_4, \mathcal{L}_{1,2}, \mathcal{L}_{3,4}$ we expect to find an element in $\mathcal{L}_{1,2} \cap \mathcal{L}_{3,4}$ from which we derive a solution to $\mathrm{CSD}(H, s, w)$

The computing effort is $O\left(2^{(n-k)/3}\right)$ possible only if $\binom{n/4}{w/4} \geq 2^{(n-k)/3}$

Order a GBA for Decoding

In general the order *a* GBA decoding will have a cost $O\left(2^{\frac{n-k}{a+1}}\right)$

It is possible only if $\binom{n/2^a}{w/2^a} \geq 2^{\frac{n-k}{a+1}}$

Order a GBA for Decoding

In general the order *a* GBA decoding will have a cost $O\left(2^{\frac{n-k}{a+1}}\right)$

It is possible only if $\binom{n/2^a}{w/2^a} \geq 2^{\frac{n-k}{a+1}}$

Asymptotically, the condition becomes $\binom{n}{w} \geq 2^{\frac{2^a}{a+1}(n-k)}$ up to a polynomial factor

This reflects the fact that higher order GBA requires higher values of *w*

Order a GBA for Decoding

In general the order a GBA decoding will have a cost $O\left(2^{\frac{n-k}{a+1}}\right)$

It is possible only if $\binom{n/2^a}{w/2^a} \geq 2^{\frac{n-k}{a+1}}$

Asymptotically, the condition becomes $\binom{n}{w} \geq 2^{\frac{2^a}{a+1}(n-k)}$ up to a polynomial factor

This reflects the fact that higher order GBA requires higher values of w

Finally, note that improvements of birthday decoding apply

This allows to lower the complexity in some cases

Comparing GBA and ISD

Information Set Decoding (all variants) and its complexity analysis can easily be adapted to the case where we seek one solution among many

In practice ISD is almost always more efficient

GBA is more efficient only when the code rate k/n is close to 1 and even then, it is only better for a limited range of values of w

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**