How to distribute the multiplication of Secret Matrices?

Rafael G.L. D’Oliveira
Salim El Rouayheb
Daniel Heinlein
David Karpuk

Massachusetts Institute of Technology
Rutgers University
Aalto University
and
F-Secure
User has two matrices $A \in \mathbb{F}_q^{r \times s}$ and $B \in \mathbb{F}_q^{s \times t}$ and wants their product $AB$. 
User has two matrices $A \in \mathbb{F}^{r \times s}$ and $B \in \mathbb{F}^{s \times t}$ and wants their product $AB$.

$N$ helper servers. Honest but curious.
User has two matrices $A \in \mathbb{F}_{q}^{r \times s}$ and $B \in \mathbb{F}_{q}^{s \times t}$ and wants their product $AB$.

$N$ helper servers. Honest but curious.

Want information theoretic Privacy even if $T$ server collude.
User has two matrices $A \in \mathbb{F}_q^{r \times s}$ and $B \in \mathbb{F}_q^{s \times t}$ and wants their product $AB$.

$N$ helper servers. Honest but curious.

Want information theoretic Privacy even if $T$ server collude.

Figure of merit: communication cost.
User has two matrices $A \in \mathbb{F}_{q}^{r \times s}$ and $B \in \mathbb{F}_{q}^{s \times t}$ and wants their product $AB$.

- $N$ helper servers. Honest but curious.
- Want information theoretic Privacy even if $T$ server collude.
- Figure of merit: communication cost.
- Matrix Multiplication is everywhere!
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp.
- \[ h(x) := f(x)g(x) = AB + (AS + RB)x + RSx^2 \]
- \( f(i) \) and \( g(i) \) are sent to Server \( i \).
- User interpolates \( h(x) \) and decodes \( AB = h(0) \).

Communication cost: \( 3 \times (\text{upload } A + \text{upload } B + \text{download } AB) \).
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]

\[ h(x) = f(x)g(x) = (A + Rx)(B + Sx) = AB + (AS + RB)x + RSx^2 \]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp.
  and forms \( f(x) = A + Rx, g(x) = B + Sx \).
- User sends \( f(i) \) and \( g(i) \) to server \( i \).
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]

\[ h(1) = f(1)g(1) \quad h(2) = f(2)g(2) \quad h(3) = f(3)g(3) \]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp and forms \( f(x) = A + Rx, g(x) = B + Sx \).
- User sends \( f(i) \) and \( g(i) \) to server \( i \).
- \( h(x) := f(x)g(x) = AB + (AS + RB)x + RSx^2 \)
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp and forms \( f(x) = A + Rx, g(x) = B + Sx \).
- User sends \( f(i) \) and \( g(i) \) to server \( i \).
- \( h(x) := f(x)g(x) = AB + (AS + RB)x + RSx^2 \)
- User wants \( AB = h(0) \).
Simplest Example: Polynomial Codes/Secret Sharing

\[
f(x) = A + Rx \\
g(x) = B + Sx
\]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp and forms \( f(x) = A + Rx \), \( g(x) = B + Sx \).
- User sends \( f(i) \) and \( g(i) \) to server \( i \).
- \( h(x) := f(x)g(x) = AB + (AS + RB)x + RSx^2 \)
- User wants \( AB = h(0) \).
- Server \( i \) computes \( h(i) = f(i)g(i) \) and sends it to the user.
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]

\[ h(1) = f(1)g(1) \]
\[ h(2) = f(2)g(2) \]
\[ h(3) = f(3)g(3) \]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp and forms \( f(x) = A + Rx, g(x) = B + Sx \).
- User sends \( f(i) \) and \( g(i) \) to server \( i \).
- \( h(x) := f(x)g(x) = AB + (AS + RB)x + RSx^2 \)
- User wants \( AB = h(0) \).
- Server \( i \) computes \( h(i) = f(i)g(i) \) and sends it to the user.
- User interpolates \( h(x) \) and decodes \( AB = h(0) \).
Simplest Example: Polynomial Codes/Secret Sharing

\[ f(x) = A + Rx \]
\[ g(x) = B + Sx \]

- Generate random \( R \) and \( S \) same size as \( A \) and \( B \), resp.
- User sends \( f(i) \) and \( g(i) \) to server \( i \).
- \( h(x) := f(x)g(x) = AB + (AS + RB)x + RSx^2 \)
- User wants \( AB = h(0) \).
- Server \( i \) computes \( h(i) = f(i)g(i) \) and sends it to the user.
- User interpolates \( h(x) \) and decodes \( AB = h(0) \).
- Comm. cost = 3 \times (upload \( A \) + upload \( B \) + download \( AB \)).
Let $A \in \mathbb{F}^{r \times s}_q$ and $B \in \mathbb{F}^{s \times t}_q$.

We divide $A$ and $B$ as $A = \begin{bmatrix} A_1 \\ \vdots \\ A_K \end{bmatrix}$ and $B = \begin{bmatrix} B_1 & \cdots & B_L \end{bmatrix}$.
Divide & Parallelize

Let $A \in \mathbb{F}_{q}^{r \times s}$ and $B \in \mathbb{F}_{q}^{s \times t}$.

We divide $A$ and $B$ as $A = \begin{bmatrix} A_1 \\ \vdots \\ A_K \end{bmatrix}$ and $B = [B_1 \quad \cdots \quad B_L]$.

$AB = \begin{bmatrix} A_1 B_1 & \cdots & A_1 B_L \\ \vdots & \vdots & \vdots \\ A_K B_1 & \cdots & A_K B_L \end{bmatrix}$.
Divide & Parallelize

- Let $A \in \mathbb{F}_{q}^{r \times s}$ and $B \in \mathbb{F}_{q}^{s \times t}$

- We divide $A$ and $B$ as $A = \begin{bmatrix} A_1 \\ \vdots \\ A_K \end{bmatrix}$ and $B = \begin{bmatrix} B_1 & \cdots & B_L \end{bmatrix}$.

- $AB = \begin{bmatrix} A_1 B_1 & \cdots & A_1 B_L \\ \vdots & \ddots & \vdots \\ A_K B_1 & \cdots & A_K B_L \end{bmatrix}$

- Each server does $\frac{1}{KL}$ of the work.
Total Communication Cost

When using $N$ servers, the total Communication Cost is

$$N\left(\frac{rs}{K} + \frac{st}{L} + \frac{rt}{KL}\right)$$

Goal:
Given partition parameters $K$ and $L$, and security parameter $T$, minimize the number of servers $N$. 
When using $N$ servers, the total Communication Cost is

$$N\left(\frac{rs}{K} + \frac{st}{L} + \frac{rt}{KL}\right)$$

**Goal:** Given partition parameters $K$ and $L$, and security parameter $T$, minimize the number of servers $N$. 
Previous Work: Polynomial Codes for Stragglers

- Originally introduced in [Yu, Maddah-Ali, Avestimehr, ’17].
- Different Setting: mitigating stragglers
- Other Work: [Yu, Maddah-Ali, Avestimehr, ’18], [Dutta, Fahim, Haddadpour, Jeong, Cadambe, Grove, ’18], [Sheth, Dutta, Chaudhari, Jeong, Yang, Kohonen, Roos, Grove, ’18], [Li, Maddah-Ali, Yu, Avestimehr, ’18], etc.
Previous Work: Polynomial Codes for Security

- Distributed multiplication with information theoretic security.
- [Chang, Tandon, ’18], [Kakar, Ebadifar, Sezgin, ’18] and [Yang, Lee, ’19]
- Related work: [Yu et al. ’19], [Aliasgari et al. ’19]
Let $K = L = 3$ and $T = 2$.

\[
\begin{bmatrix}
A_1 \\
A_2 \\
A_3
\end{bmatrix}, \quad
\begin{bmatrix}
B_1 & B_2 & B_3
\end{bmatrix}, \quad
\begin{bmatrix}
A_1 B_1 & A_1 B_2 & A_1 B_3 \\
A_2 B_1 & A_2 B_2 & A_2 B_3 \\
A_3 B_1 & A_3 B_2 & A_3 B_3
\end{bmatrix}
\]

\[
f(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^3 + R_2 x^4
\]

\[
g(x) = B_1 + B_2 x + B_3 x^2 + S_1 x^3 + S_2 x^4
\]
Let $K = L = 3$ and $T = 2$.

$$A = \begin{bmatrix} A_1 \\ A_2 \\ A_3 \end{bmatrix}, \quad B = \begin{bmatrix} B_1 & B_2 & B_3 \end{bmatrix}, \quad AB = \begin{bmatrix} A_1B_1 & A_1B_2 & A_1B_3 \\ A_2B_1 & A_2B_2 & A_2B_3 \\ A_3B_1 & A_3B_2 & A_3B_3 \end{bmatrix}$$

$f(x) = A_1 + A_2x + A_3x^2 + R_1x^3 + R_2x^4$

g(x) = B_1 + B_2x + B_3x^2 + S_1x^3 + S_2x^4

Let $h(x) = f(x)g(x)$. Then,

$$h(x) = A_1B_1 + (A_1B_2 + A_2B_1)x + (A_1B_3 + A_2B_2 + A_3B_1)x^2 + \ldots$$
Let $K = L = 3$ and $T = 2$.

$$A = \begin{bmatrix} A_1 \\ A_2 \\ A_3 \end{bmatrix}, \quad B = \begin{bmatrix} B_1 & B_2 & B_3 \end{bmatrix}, \quad AB = \begin{bmatrix} A_1 B_1 & A_1 B_2 & A_1 B_3 \\ A_2 B_1 & A_2 B_2 & A_2 B_3 \\ A_3 B_1 & A_3 B_2 & A_3 B_3 \end{bmatrix}$$

- $f(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^3 + R_2 x^4$
- $g(x) = B_1 + B_2 x + B_3 x^2 + S_1 x^3 + S_2 x^4$
- Let $h(x) = f(x)g(x)$. Then,

$$h(x) = A_1 B_1 + (A_1 B_2 + A_2 B_1)x + (A_1 B_3 + A_2 B_2 + A_3 B_1)x^2 + \ldots$$

- Can’t retrieve $A_1 B_2$, for example.
It is not about the degree.

▶ **Scheme 1:**
  - \( f(x) = A_1 + A_2x + A_3x^2 + R_1x^3 + R_2x^4 \)
  - \( g(x) = B_1 + B_2x^5 + B_3x^{10} + S_1x^{13} + S_2x^{14} \)
  - \( N_h = \deg h + 1 = 19 \) servers.
It is not about the degree.

Scheme 1:
- \( f(x) = A_1 + A_2x + A_3x^2 + R_1x^3 + R_2x^4 \)
- \( g(x) = B_1 + B_2x^5 + B_3x^{10} + S_1x^{13} + S_2x^{14} \)
- \( N_h = \deg h + 1 = 19 \) servers.

Scheme 2:
- \( f^*(x) = A_1 + A_2x + A_3x^2 + R_1x^9 + R_2x^{12} \)
- \( g^*(x) = B_1 + B_2x^3 + B_3x^6 + S_1x^9 + S_2x^{10} \)
- \( \deg h^* = 22 \)
It is not about the degree.

- **Scheme 1:**
  - \( f(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^3 + R_2 x^4 \)
  - \( g(x) = B_1 + B_2 x^5 + B_3 x^{10} + S_1 x^{13} + S_2 x^{14} \)
  - \( N_h = \text{deg } h + 1 = 19 \text{ servers.} \)

- **Scheme 2:**
  - \( f^*(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^9 + R_2 x^{12} \)
  - \( g^*(x) = B_1 + B_2 x^3 + B_3 x^6 + S_1 x^9 + S_2 x^{10} \)
  - \( \text{deg } h^* = 22 > 18 = \text{deg } h \)
It is not about the degree.

**Scheme 1:**
- \( f(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^3 + R_2 x^4 \)
- \( g(x) = B_1 + B_2 x^5 + B_3 x^{10} + S_1 x^{13} + S_2 x^{14} \)
- \( N_h = \text{deg } h + 1 = 19 \) servers.

**Scheme 2:**
- \( f^*(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^9 + R_2 x^{12} \)
- \( g^*(x) = B_1 + B_2 x^3 + B_3 x^6 + S_1 x^9 + S_2 x^{10} \)
- \( \text{deg } h^* = 22 > 18 = \text{deg } h \)
- But \( h^* \) has gaps in the degrees.
- No term of degrees 13, 14, 16, 17 or 20.
It is not about the degree.

**Scheme 1:**
- \( f(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^3 + R_2 x^4 \)
- \( g(x) = B_1 + B_2 x^5 + B_3 x^{10} + S_1 x^{13} + S_2 x^{14} \)
- \( N_h = \text{deg } h + 1 = 19 \text{ servers.} \)

**Scheme 2:**
- \( f^*(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^9 + R_2 x^{12} \)
- \( g^*(x) = B_1 + B_2 x^3 + B_3 x^6 + S_1 x^9 + S_2 x^{10} \)
- \( \text{deg } h^* = 22 > 18 = \text{deg } h \)
- But \( h^* \) has gaps in the degrees.
- No term of degrees 13, 14, 16, 17 or 20.
- Thus, only 18 points needed to interpolate \( h^* \).
- \( N_{h^*} = 18 < 19 = N_h. \)
It is about the number of terms in the polynomial.
What is it about?

It is about the number of terms in the polynomial.

- Consider the polynomial \( f(x) = ax^6 + bx^5 + cx \).
- We need \( 3 < \deg f + 1 \) points to interpolate this polynomial.
What is it about?

It is about the number of terms in the polynomial.

- Consider the polynomial $f(x) = ax^6 + bx^5 + cx$.
- We need $3 < \deg f + 1$ points to interpolate this polynomial.
- **Not any points!** What does $f(0)$ tell you?
How many terms does $f(x)g(x)$ have?

- $f(x) = A_1 x^{\alpha_1} + A_2 x^{\alpha_2} + A_3 x^{\alpha_3} + R_1 x^{\alpha_4} + R_2 x^{\alpha_5}$
- $g(x) = B_1 x^{\beta_1} + B_2 x^{\beta_2} + B_3 x^{\beta_3} + S_1 x^{\beta_4} + S_2 x^{\beta_5}$

The terms in $h(x)$ appear in the following table.
How many terms does \( f(x)g(x) \) have?

\[
\begin{align*}
\bullet \quad f(x) &= A_1 x^{\alpha_1} + A_2 x^{\alpha_2} + A_3 x^{\alpha_3} + R_1 x^{\alpha_4} + R_2 x^{\alpha_5} \\
\bullet \quad g(x) &= B_1 x^{\beta_1} + B_2 x^{\beta_2} + B_3 x^{\beta_3} + S_1 x^{\beta_4} + S_2 x^{\beta_5}
\end{align*}
\]

The terms in \( h(x) \) appear in the following table.

<table>
<thead>
<tr>
<th></th>
<th>( \beta_1 )</th>
<th>( \beta_2 )</th>
<th>( \beta_3 )</th>
<th>( \beta_4 )</th>
<th>( \beta_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha_1 )</td>
<td>( \alpha_1 + \beta_1 )</td>
<td>( \alpha_2 + \beta_2 )</td>
<td>( \alpha_1 + \beta_3 )</td>
<td>( \alpha_1 + \beta_4 )</td>
<td>( \alpha_1 + \beta_5 )</td>
</tr>
<tr>
<td>( \alpha_2 )</td>
<td>( \alpha_2 + \beta_1 )</td>
<td>( \alpha_2 + \beta_2 )</td>
<td>( \alpha_2 + \beta_3 )</td>
<td>( \alpha_2 + \beta_4 )</td>
<td>( \alpha_2 + \beta_5 )</td>
</tr>
<tr>
<td>( \alpha_3 )</td>
<td>( \alpha_3 + \beta_1 )</td>
<td>( \alpha_3 + \beta_2 )</td>
<td>( \alpha_3 + \beta_3 )</td>
<td>( \alpha_3 + \beta_4 )</td>
<td>( \alpha_3 + \beta_5 )</td>
</tr>
<tr>
<td>( \alpha_4 )</td>
<td>( \alpha_4 + \beta_1 )</td>
<td>( \alpha_4 + \beta_2 )</td>
<td>( \alpha_4 + \beta_3 )</td>
<td>( \alpha_4 + \beta_4 )</td>
<td>( \alpha_4 + \beta_5 )</td>
</tr>
<tr>
<td>( \alpha_5 )</td>
<td>( \alpha_5 + \beta_1 )</td>
<td>( \alpha_5 + \beta_2 )</td>
<td>( \alpha_5 + \beta_3 )</td>
<td>( \alpha_5 + \beta_4 )</td>
<td>( \alpha_5 + \beta_5 )</td>
</tr>
</tbody>
</table>
How many terms does $f(x)g(x)$ have?

$\quad f(x) = A_1 x^{\alpha_1} + A_2 x^{\alpha_2} + A_3 x^{\alpha_3} + R_1 x^{\alpha_4} + R_2 x^{\alpha_5}$

$\quad g(x) = B_1 x^{\beta_1} + B_2 x^{\beta_2} + B_3 x^{\beta_3} + S_1 x^{\beta_4} + S_2 x^{\beta_5}$

The terms in $h(x)$ appear in the following table.

<table>
<thead>
<tr>
<th></th>
<th>$\beta_1$</th>
<th>$\beta_2$</th>
<th>$\beta_3$</th>
<th>$\beta_4$</th>
<th>$\beta_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_1$</td>
<td>$\alpha_1 + \beta_1$</td>
<td>$\alpha_1 + \beta_2$</td>
<td>$\alpha_1 + \beta_3$</td>
<td>$\alpha_1 + \beta_4$</td>
<td>$\alpha_1 + \beta_5$</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>$\alpha_2 + \beta_1$</td>
<td>$\alpha_2 + \beta_2$</td>
<td>$\alpha_2 + \beta_3$</td>
<td>$\alpha_2 + \beta_4$</td>
<td>$\alpha_2 + \beta_5$</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>$\alpha_3 + \beta_1$</td>
<td>$\alpha_3 + \beta_2$</td>
<td>$\alpha_3 + \beta_3$</td>
<td>$\alpha_3 + \beta_4$</td>
<td>$\alpha_3 + \beta_5$</td>
</tr>
<tr>
<td>$\alpha_4$</td>
<td>$\alpha_4 + \beta_1$</td>
<td>$\alpha_4 + \beta_2$</td>
<td>$\alpha_4 + \beta_3$</td>
<td>$\alpha_4 + \beta_4$</td>
<td>$\alpha_4 + \beta_5$</td>
</tr>
<tr>
<td>$\alpha_5$</td>
<td>$\alpha_5 + \beta_1$</td>
<td>$\alpha_5 + \beta_2$</td>
<td>$\alpha_5 + \beta_3$</td>
<td>$\alpha_5 + \beta_4$</td>
<td>$\alpha_5 + \beta_5$</td>
</tr>
</tbody>
</table>

$\quad$ We call this a degree table.
Properties of the Degree Table

- \( f^*(x) = A_1 + A_2x + A_3x^2 + R_1x^9 + R_2x^{12} \)
- \( g^*(x) = B_1 + B_2x^3 + B_3x^6 + S_1x^9 + S_2x^{10} \)

<table>
<thead>
<tr>
<th>( h^* )</th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>
Properties of the Degree Table

- \( f^*(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^9 + R_2 x^{12} \)
- \( g^*(x) = B_1 + B_2 x^3 + B_3 x^6 + S_1 x^9 + S_2 x^{10} \)

<table>
<thead>
<tr>
<th>( h^* )</th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

- Decodability: Red cells unique.
Properties of the Degree Table

- \( f^*(x) = A_1 + A_2x + A_3x^2 + R_1x^9 + R_2x^{12} \)
- \( g^*(x) = B_1 + B_2x^3 + B_3x^6 + S_1x^9 + S_2x^{10} \)

<table>
<thead>
<tr>
<th>( h^* )</th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

- Decodability: Red cells unique.
- Security A: Green cells distinct.
Properties of the Degree Table

- \( f^*(x) = A_1 + A_2x + A_3x^2 + R_1x^9 + R_2x^{12} \)
- \( g^*(x) = B_1 + B_2x^3 + B_3x^6 + S_1x^9 + S_2x^{10} \)

<table>
<thead>
<tr>
<th>( h^* )</th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

- Decodability: Red cells unique.
- Security A: Green cells distinct.
- Security B: Blue cells distinct.
Properties of the Degree Table

- \( f^*(x) = A_1 + A_2 x + A_3 x^2 + R_1 x^9 + R_2 x^{12} \)
- \( g^*(x) = B_1 + B_2 x^3 + B_3 x^6 + S_1 x^9 + S_2 x^{10} \)

<table>
<thead>
<tr>
<th>( h^* )</th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

- Decodability: Red cells unique.
- Security A: Green cells distinct.
- Security B: Blue cells distinct.

- **Goal:** Minimize distinct cells.
Problem Restatement: The Degree Table

<table>
<thead>
<tr>
<th></th>
<th>(\alpha_1)</th>
<th>(\beta_1)</th>
<th>(\cdots)</th>
<th>(\beta_L)</th>
<th>(\alpha_{K+1})</th>
<th>(\beta_{K+1})</th>
<th>(\cdots)</th>
<th>(\beta_{L+T})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\alpha_1)</td>
<td>(\alpha_1 + \beta_1)</td>
<td>(\alpha_1 + \beta_1)</td>
<td>(\cdots)</td>
<td>(\alpha_1 + \beta_L)</td>
<td>(\alpha_1 + \beta_{L+1})</td>
<td>(\cdots)</td>
<td>(\alpha_1 + \beta_{L+T})</td>
<td></td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>(\alpha_K)</td>
<td>(\alpha_K + \beta_1)</td>
<td>(\alpha_K + \beta_1)</td>
<td>(\cdots)</td>
<td>(\alpha_K + \beta_L)</td>
<td>(\alpha_K + \beta_{L+1})</td>
<td>(\cdots)</td>
<td>(\alpha_K + \beta_{L+T})</td>
<td></td>
</tr>
<tr>
<td>(\alpha_{K+1})</td>
<td>(\alpha_{K+1} + \beta_1)</td>
<td>(\alpha_{K+1} + \beta_1)</td>
<td>(\cdots)</td>
<td>(\alpha_{K+1} + \beta_L)</td>
<td>(\alpha_{K+1} + \beta_{L+1})</td>
<td>(\cdots)</td>
<td>(\alpha_{K+1} + \beta_{L+T})</td>
<td></td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>(\alpha_{K+T})</td>
<td>(\alpha_{K+T} + \beta_1)</td>
<td>(\alpha_{K+T} + \beta_1)</td>
<td>(\cdots)</td>
<td>(\alpha_{K+T} + \beta_L)</td>
<td>(\alpha_{K+T} + \beta_{L+1})</td>
<td>(\cdots)</td>
<td>(\alpha_{K+T} + \beta_{L+T})</td>
<td></td>
</tr>
</tbody>
</table>

**Goal:** Minimize number of distinct terms.

**Subject to:**

- **Decodability:** Numbers in the red region are all unique.
- **A-Security:** Numbers in the green region are all distinct.
- **B-Security:** Numbers in the blue region are all distinct.
GASP_{big} [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]
$K = L = T = 3$
GASP_{big} [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]

\[ \begin{array}{c}
\hline
K = L = T = 3 \\
\hline
0 \quad 1 \quad 2 \\
\hline
\end{array} \]
$K = L = T = 3$
$K = L = T = 3$
$K = L = T = 3$
$K = L = T = 3$
$K = L = T = 3$
$K = L = T = 3$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

\[ \text{GASP}_{\text{big}} [\text{D’Oliveira, SER, Karpuk, ISIT ’19}] \]
$K = L = T = 3$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>
GASP$_{\text{big}}$ [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]

\[
\begin{array}{c|ccc}
  & 0 & 3 & 6 \\
\hline
0 & 0 & 3 & 6 \\
1 & 1 & 4 & 7 \\
2 & 2 & 5 & 8 \\
9 & & & \\
\end{array}
\]
GASP\textsubscript{big} [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td>9</td>
</tr>
</tbody>
</table>
GASP\textsubscript{big} [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]

\begin{array}{|c|cccc|}
\hline
 & 0 & 3 & 6 & 9 \\
\hline
0 & 0 & 3 & 6 & 9 \\
1 & 1 & 4 & 7 & 10 \\
2 & 2 & 5 & 8 & 11 \\
9 & 9 & 12 & 15 & 18 \\
\hline
\end{array}
$K = L = T = 3$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\( K = L = T = 3 \)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th></th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>13</td>
<td>16</td>
<td>19</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>
$K = L = T = 3$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>13</td>
<td>16</td>
<td>19</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
$K = L = T = 3$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>13</td>
<td>16</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>14</td>
<td>17</td>
<td>20</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>
Number of Terms

Theorem [D'Oliveira, SER, Karpuk, ISIT '19]

The number of terms in GASP\textsubscript{big}, for $L \leq K$, is

$$N = \begin{cases} 
2K + 2T - 1 & \text{if } L = 1 \\
(K + T)(L + 1) - 1 & \text{if } L \geq 2, \ T < K \\
2KL + 2T - 1 & \text{if } L \geq 2, \ T \geq K 
\end{cases}$$
How good is $\text{GASP}_\text{big}$?
How good is $\text{GASP}_{\text{big}}$?

- Lagrange coding [Yu et al.,'19] achieves same rate for $T \geq \min\{K, L\}$. 
How good is $\text{GASP}_{\text{big}}$?

- Lagrange coding [Yu et al.,’19] achieves same rate for $T \geq \min\{K, L\}$.
- Can we do better?
GASP$_{\text{small}}$ [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]

\[
\begin{array}{cccc|ccc}
\hline
 & 0 & 3 & 6 & 9 & 10 & 11 \\
\hline
0 & 0 & 3 & 6 & 9 & 10 & 11 \\
1 & 1 & 4 & 7 & 10 & 11 & 12 \\
2 & 2 & 5 & 8 & 11 & 12 & 13 \\
\hline
\end{array}
\]
**GASP_{small} [D’Oliveira, SER, Karpuk, ISIT ’19]**

\[ K = L = T = 3 \]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
$K = L = T = 3$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**GASP**$_{\text{small}}$ [D’Oliveira, SER, Karpuk, ISIT ’19]

\[ K = L = T = 3 \]

\[ \begin{array}{cccccc}
0 & 0 & 3 & 6 & 9 & 10 & 11 \\
1 & 1 & 4 & 7 & 10 & 11 & 12 \\
2 & 2 & 5 & 8 & 11 & 12 & 13 \\
9 & & & & & & \\
12 & & & & & & \\
15 & & & & & & \\
\end{array} \]
$K = L = T = 3$

$$
\begin{array}{c|ccc|ccc}
& 0 & 3 & 6 & 9 & 10 & 11 \\
\hline
0 & 0 & 3 & 6 & 9 & 10 & 11 \\
1 & 1 & 4 & 7 & 10 & 11 & 12 \\
2 & 2 & 5 & 8 & 11 & 12 & 13 \\
9 & 9 & 12 & 15 & & & \\
12 & 12 & 15 & 18 & & & \\
15 & 15 & 18 & 21 & & & \\
\end{array}
$$
\( K = L = T = 3 \)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>3</th>
<th>6</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
</tbody>
</table>
The number of terms in $GASP_{\text{small}}$, for $K \leq L$, is

$$N = \begin{cases} 
2K + T^2 & \text{if } L = 1, T < K \\
KT + K + T & \text{if } L = 1, T \geq K \\
KL + K + L & \text{if } L \geq 2, 1 = T < K \\
KL + K + L + T^2 + T - 3 & \text{if } L \geq 2, 2 \leq T < K \\
KL + KT + L + 2T - 3 - \left\lfloor \frac{T-2}{K} \right\rfloor & \text{if } L \geq 2, K \leq T \leq K(L - 1) + 1 \\
2KL + KT - K + T & \text{if } L \geq 2, K(L - 1) + 1 \leq T 
\end{cases}$$
What is small $T$?

Theorem [D’Oliveira, SER, Karpuk, ISIT ’19]

$\text{GASP}_{\text{small}}$ outperforms $\text{GASP}_{\text{big}}$ for $T < \min\{K, L\}$.
What is small $T$?

Theorem [D’Oliveira, SER, Karpuk, ISIT ’19]

$\text{GASP}_{\text{small}}$ outperforms $\text{GASP}_{\text{big}}$ for $T < \min\{K, L\}$.

Can we do better?
# GASP$_r$: Gap Additive Secure Polynomial codes

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>4</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

$r = 1, S(r) = 14, N = 41$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>4</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

$r = 2, S(r) = 19, N = 36$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>4</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

$r = 3, S(r) = 18, N = 37$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>4</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td>15</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
</tr>
</tbody>
</table>

$r = 4, S(r) = 16, N = 39$
Theorem [D’Oliveira, SER, Heinlein, Karpuk, ITW ’19]

- Partitioning parameters: $K$ and $L$
- Security parameter: $T$
- Chain length: $r$

Then, the degree table constructed by GASP$_r$ has

$$N = KL + K + T - 1 + T \cdot (L + T) - S(r)$$
Theorem [D’Oliveira, SER, Heinlein, Karpuk, ITW ’19]

- Partitioning parameters: $K$ and $L$
- Security parameter: $T$
- Chain length: $r$

Then, the degree table constructed by $\text{GASP}_r$ has

$$N = KL + K + T - 1 + T \cdot (L + T) - S(r)$$

where

$$S(r) = \max\{0, \min\{r, \varphi\}\}L + 2 \max\{0, r - z + 1\} + \gamma + (T - r)L + \max\{0, K + T - KL - 1\} + \eta \max\{0, T - K + r - 1\} + (T - 1 - \eta)(T - 1)$$

$$\varphi = T - 1 - KL + 2K, \quad \eta = \lfloor (T - 1)/r \rfloor, \quad z = \max\{1, \varphi + 1\},$$

$$\gamma = \begin{cases} 0 & \text{if } r < z \\ K(x - a)(x + a - 1)/2 - ab + xy + x & \text{else} \end{cases}$$

with $a, b, x, y$ defined by

$$T - 1 - r = aK + b \text{ and } 0 \leq b \leq K - 1,$$

$$T - 1 - z = xK + y \text{ and } 0 \leq y \leq K - 1.$$
Theorem [D’Oliveira, SER, Heinlein, Karpuk, ITW ’19]

- Partitioning parameters: $K$ and $L$
- Security parameter: $T$
- Number of distinct terms: $N$

Then the following three inequalities hold.

1. $KL + \max\{K, L\} + 2T - 1 \leq N.$
Theorem [D’Oliveira, SER, Heinlein, Karpuk, ITW ’19]

- Partitioning parameters: \( K \) and \( L \)
- Security parameter: \( T \)
- Number of distinct terms: \( N \)

Then the following three inequalities hold.

1. \( KL + \max\{K, L\} + 2T - 1 \leq N \).

2. If \( 3\max\{K, L\} + 3T - 2 < KL \) or \( 2 \leq K = L \), then
   \( KL + \max\{K, L\} + 2T \leq N \).
Theorem [D’Oliveira, SER, Heinlein, Karpuk, ITW ’19]

- Partitioning parameters: $K$ and $L$
- Security parameter: $T$
- Number of distinct terms: $N$

Then the following three inequalities hold.

1. $KL + \max\{K, L\} + 2T - 1 \leq N$.

2. If $3\max\{K, L\} + 3T - 2 < KL$ or $2 \leq K = L$, then $KL + \max\{K, L\} + 2T \leq N$.

3. $KL + K + L + 2T - 1 - T \min\{K, L, T\} \leq N$. 
Main Idea Behind Lower Bound

- Result from additive combinatorics on the minimal size of sum sets.
Main Idea Behind Lower Bound

- Result from additive combinatorics on the minimal size of sum sets.

**Lemma [Tao, Vu, “Additive Combinatorics”]**

Let $A$ and $B$ be sets of integers. Then $|A| + |B| - 1 \leq |A + B|$ and if $2 \leq |A|, |B|$, then equality holds iff $A$ and $B$ are arithmetic progressions with the same common difference.
Main Idea Behind Lower Bound

- Result from additive combinatorics on the minimal size of sum sets.

**Lemma [Tao, Vu, “Additive Combinatorics”]**

Let $A$ and $B$ be sets of integers. Then $|A| + |B| - 1 \leq |A + B|$ and if $2 \leq |A|, |B|$, then equality holds iff $A$ and $B$ are arithmetic progressions with the same common difference.
Current Situation

- $K = L = 4$
- $\text{GASP}_r$ for $r = 1, \ldots, K$. 

![Graph showing the relationship between the number of servers ($N$) and security level ($T$). The graph includes lines for $\text{GASP}_1$, $\text{GASP}_2$, $\text{GASP}_3$, $\text{GASP}_4$, and a lower bound line.](image-url)
Corollary

If either $K = 1$, $L = 1$, or $T = 1$, then $\text{GASP}_r$ is optimal.
### Corollary

If either $K = 1$, $L = 1$, or $T = 1$, then $\text{GASP}_r$ is optimal.

### Corollary

If $K = L = T = n^2 \geq 4$, then $\text{GASP}_n$ is asymptotically optimal.
Corollary

If either $K = 1$, $L = 1$, or $T = 1$, then GASP$_r$ is optimal.

Corollary

If $K = L = T = n^2 \geq 4$, then GASP$_n$ is asymptotically optimal.
Is it all worth it?

- $r = s = t = n$ (square matrices).
Is it all worth it?

- $r = s = t = n$ (square matrices).
- Security parameter $T$ is constant.
Is it all worth it?

- $r = s = t = n$ (square matrices).
- Security parameter $T$ is constant.
- Servers multiply two $n \times n$ in time $\mathcal{O}(n^\omega)$. 
Is it all worth it?

- \( r = s = t = n \) (square matrices).
- Security parameter \( T \) is constant.
- Servers multiply two \( n \times n \) in time \( \mathcal{O}(n^\omega) \).
- Partitioning parameters \( K = L = n^\varepsilon \).
Is it all worth it?

- \( r = s = t = n \) (square matrices).
- Security parameter \( T \) is constant.
- Servers multiply two \( n \times n \) in time \( \mathcal{O}(n^\omega) \).
- Partitioning parameters \( K = L = n^\varepsilon \).

Theorem [D’Oliveira, SER, Heinlein, Karpuk ’20]

By using GASP, the user can perform the matrix multiplication in time \( \mathcal{O}(n^{4-\frac{6}{\omega+1}} \log(n)^2) \) as opposed to the \( \mathcal{O}(n^\omega) \) time it would take to do locally.
Is it all worth it?
Is it all worth it?

\[ 4 - \frac{6}{\omega + 1} \]

called conjectured

- Standard
- Strassen
- Le Gall

Total Time Complexity Exponent

Matrix Multiplication Complexity Exponent
Open Problems

- Are there better schemes for the degree table?
- Are there better bounds?
- What about information theoretical bounds?
- Are polynomial codes optimal?
Thanks!