Simultaneous Diagonalization of Incomplete Matrices and Applications

Jean-Sébastien Coron[1], **Luca Notarnicola**[2] and Gabor Wiese[3]

ANTS-XIV 2020

July 4, 2020

[1,2,3]University of Luxembourg, Luxembourg

I • Summary

Notation and Problem Statement

- Consider matrices

$$\begin{aligned} W_0 &= P \cdot Q \in \mathbb{Q}^{p \times q} \\ W_a &= P \cdot U_a \cdot Q \in \mathbb{Q}^{p \times q}, \quad a \in I \end{aligned}$$

  where
  - $P \in \mathbb{Q}^{p \times n}$ of rank $p \leq n$
  - $Q \in \mathbb{Q}^{n \times q}$ of rank $q \leq n$
  - $\{U_a\}_{a \in I} \subseteq \mathbb{Q}^{n \times n}$ diagonal , $I := \{1, \ldots, t\}$
- **Problem:** Given W_0, $\{W_a\}_a$, and assume W_0 is of full rank p compute diagonal entries of $\{U_a\}_a$

Notation and Problem Statement

- Consider matrices

$$\begin{aligned} W_0 &= P \cdot Q \in \mathbb{Q}^{p \times q} \\ W_a &= P \cdot U_a \cdot Q \in \mathbb{Q}^{p \times q}, \quad a \in I \end{aligned}$$

  where
  - $P \in \mathbb{Q}^{p \times n}$ of rank $p \leq n$
  - $Q \in \mathbb{Q}^{n \times q}$ of rank $q \leq n$
  - $\{U_a\}_{a \in I} \subseteq \mathbb{Q}^{n \times n}$ diagonal , $I := \{1, \ldots, t\}$
- **Problem:** Given $W_0, \{W_a\}_a$, and assume W_0 is of full rank p compute diagonal entries of $\{U_a\}_a$
- Easy case ($p, q = n, t = 1$) [we call this Problem $\mathbb{A}$]
  Solution: Return the eigenvalues of

$$W_0^{-1} \cdot W_1 = Q^{-1} U_1 Q$$

Notation and Problem Statement

- Consider matrices

$$\begin{aligned} W_0 &= P \cdot Q \in \mathbb{Q}^{p\times q} \\ W_a &= P \cdot U_a \cdot Q \in \mathbb{Q}^{p\times q}, \quad a \in I \end{aligned}$$

  where
  - $P \in \mathbb{Q}^{p\times n}$ of rank $p \leq n$
  - $Q \in \mathbb{Q}^{n\times q}$ of rank $q \leq n$
  - $\{U_a\}_{a\in I} \subseteq \mathbb{Q}^{n\times n}$ diagonal , $I := \{1, \ldots, t\}$
- **Problem:** Given W_0, $\{W_a\}_a$, and assume W_0 is of full rank p compute diagonal entries of $\{U_a\}_a$
- Easy case ($p, q = n, t = 1$) [we call this Problem $\mathbb{A}$]
  Solution: Return the eigenvalues of

$$W_0^{-1} \cdot W_1 = Q^{-1} U_1 Q$$

- Goal: Minimize p, q, t w.r.t. n

Notation and Problem Statement

- Consider matrices

$$\begin{aligned} W_0 &= P \cdot Q \in \mathbb{Q}^{p \times q} \\ W_a &= P \cdot U_a \cdot Q \in \mathbb{Q}^{p \times q}, \quad a \in I \end{aligned}$$

  where
  - $P \in \mathbb{Q}^{p \times n}$ of rank $p \leq n$
  - $Q \in \mathbb{Q}^{n \times q}$ of rank $q \leq n$
  - $\{U_a\}_{a \in I} \subseteq \mathbb{Q}^{n \times n}$ diagonal , $I := \{1, \ldots, t\}$
- **Problem:** Given W_0, $\{W_a\}_a$, and assume W_0 is of full rank p compute diagonal entries of $\{U_a\}_a$
- Easy case ($p, q = n, t = 1$) [we call this Problem $\mathbb{A}$]
  Solution: Return the eigenvalues of

$$W_0^{-1} \cdot W_1 = Q^{-1} U_1 Q$$

- Goal: Minimize p, q, t w.r.t. n
- Motivation for improved cryptanalysis

Summary of our work

1. We solve the mentioned problem by heuristic algorithms in the following cases:
   - (Problem $\mathbb{C}$) P of rank $p < n$, Q of rank $q = n$
   - (Problem $\mathbb{D}$) P, Q of rank $p = q < n$

   Parameters:
   - Solve $\mathbb{C}$ for $p \geq \sqrt{2n} = \mathcal{O}(\sqrt{n})$; $t \geq \sqrt{2n} - 1 = \mathcal{O}(\sqrt{n})$
   - Solve $\mathbb{D}$ for $p \geq \frac{2}{3}n + \frac{\sqrt{n}}{3\sqrt{2}} = \frac{2}{3}n + \mathcal{O}(\sqrt{n})$; $t \geq \frac{\sqrt{2n}}{3} + \frac{5}{3} = \mathcal{O}(\sqrt{n})$

2. Applications
   - CRT-Approximate-Common Divisor Problem
     - improvement of the Coron-Pereira algorithm (Asiacrypt'19)
     - By solving a certain instance of this problem, we obtain a quadratic improvement in the number of input samples
   - Cryptanalysis of CLT13 Multilinear Maps
     - improvement of the Cheon et al. attack (Eurocrypt'15)
     - By solving a certain instance of this problem, we obtain a quadratic improvement in the number of encodings needed for the attack

II • Our Algorithms

Problem $\mathbb{C}$: $Q \in \mathbf{GL}_n(\mathbb{Q})$

- Write $W_a = (PQ)(Q^{-1}U_aQ) =: W_0 Z_a$ (Z_a unknown)

Problem $\mathbb{C}$: $Q \in \mathbf{GL}_n(\mathbb{Q})$

- Write $W_a = (PQ)(Q^{-1}U_aQ) =: W_0 Z_a$ (Z_a unknown)
- Properties of $\{Z_a\}_a$:
  (a) General solution: $Z_a = Y_a + EX_a$, where
    - $Y_a \in \mathbb{Q}^{n\times n}$ s.t. $W_0 Y_a = W_a$ (let $Y_a = W_0^\dagger W_a$)
    - $E \in \mathbb{Q}^{n\times p}$ s.t. $\langle E\rangle = \ker(W_0)$
    - $\{X_a\}_a \subseteq \mathbb{Q}^{p\times n}$ variables

  (b) Matrices $\{Z_a\}_a$ commute

Problem $\mathbb{C}$: $Q \in \mathbf{GL}_n(\mathbb{Q})$

- Write $W_a = (PQ)(Q^{-1}U_aQ) =: W_0 Z_a$ (Z_a unknown)
- Properties of $\{Z_a\}_a$:
  (a) General solution: $Z_a = Y_a + EX_a$, where
  - $Y_a \in \mathbb{Q}^{n\times n}$ s.t. $W_0 Y_a = W_a$ (let $Y_a = W_0^\dagger W_a$)
  - $E \in \mathbb{Q}^{n\times p}$ s.t. $\langle E\rangle = \ker(W_0)$
  - $\{X_a\}_a \subseteq \mathbb{Q}^{p\times n}$ variables

  (b) Matrices $\{Z_a\}_a$ commute
- $[Z_a, Z_b] = 0$ for all $a < b$ gives an explicit system of linear equations in the variables $\{X_a\}_a$
- Heuristic unicity of solution $\{X_a\}_a$ if the system has sufficiently many equations
- working condition: $p(t+1) \leq 2n$

Problem $\mathbb{C}$: $Q \in \mathbf{GL}_n(\mathbb{Q})$

- Write $W_a = (PQ)(Q^{-1}U_aQ) =: W_0 Z_a$ (Z_a unknown)
- Properties of $\{Z_a\}_a$:
  (a) General solution: $Z_a = Y_a + EX_a$, where
    - $Y_a \in \mathbb{Q}^{n\times n}$ s.t. $W_0 Y_a = W_a$ (let $Y_a = W_0^{\dagger} W_a$)
    - $E \in \mathbb{Q}^{n\times p}$ s.t. $\langle E \rangle = \ker(W_0)$
    - $\{X_a\}_a \subseteq \mathbb{Q}^{p\times n}$ variables

  (b) Matrices $\{Z_a\}_a$ commute
- $[Z_a, Z_b] = 0$ for all $a < b$ gives an explicit system of linear equations in the variables $\{X_a\}_a$
- Heuristic unicity of solution $\{X_a\}_a$ if the system has sufficiently many equations
- working condition: $p(t+1) \leq 2n$
- e.g. choose $p = \lceil \sqrt{2n} \rceil$, $t = \lceil \sqrt{2n} \rceil - 1$

Algorithm for Pb. $\mathbb{C}$ - P of low-rank, Q of full rank

Algorithm for Pb. $\mathbb{C}$ - P of low-rank, Q of full rank

Note that for $a, b \in I$:

$$[Z_a, Z_b] = 0 \implies W_a W_0^\dagger W_b - W_b W_0^\dagger W_a + W_a E X_b - W_b E X_a = 0$$

Algorithm for Pb. $\mathbb{C}$ - P of low-rank, Q of full rank

Note that for $a, b \in I$:

$$[Z_a, Z_b] = 0 \implies W_a W_0^\dagger W_b - W_b W_0^\dagger W_a + W_a E X_b - W_b E X_a = 0$$

Algorithm

1. For $a, b \in I$, $a < b$ compute $\Delta_{ab} = W_a W_0^\dagger W_b - W_b W_0^\dagger W_a$
2. Solve a linear system of equations

   $$\Delta_{ab} = W_b E X_a - W_a E X_b \ , \quad a, b \in I,\ a < b$$

   for the matrices $\{X_a\}_a$
3. If success, run simultaneous diagonalization of $\{Z_a\}_a$ with

   $$Z_a = W_0^\dagger W_a + E X_a, \quad a \in I$$

Problem $\mathbb{D}$: P, Q of low-rank p

- Main idea: reduce to Problem $\mathbb{C}$
- We compute $\{V_a\}_a \subseteq \mathbb{Q}^{p\times(n-p)}$ s.t. there exists $\tilde{Q} \in \mathbb{Q}^{p\times(n-p)}$ s.t. $[Q|\tilde{Q}] \in \mathrm{GL}_n(\mathbb{Q})$ and

$$\begin{aligned} P\tilde{Q} &= 0 \\ PU_a\tilde{Q} &= V_a, \quad a \in I \end{aligned}$$

Problem $\mathbb{D}$: P, Q of low-rank p

- Main idea: reduce to Problem $\mathbb{C}$
- We compute $\{V_a\}_a \subseteq \mathbb{Q}^{p\times(n-p)}$ s.t. there exists $\tilde{Q} \in \mathbb{Q}^{p\times(n-p)}$ s.t. $[Q|\tilde{Q}] \in \mathsf{GL}_n(\mathbb{Q})$ and

$$\begin{aligned} P\tilde{Q} &= 0 \\ PU_a\tilde{Q} &= V_a, \quad a \in I \end{aligned}$$

- This gives public augmented matrices $\{W'_a\}_{a\in I\cup\{0\}}$:

$$\begin{aligned} W'_0 := [W_0|0] &= P[Q|\tilde{Q}] \in \mathbb{Q}^{p\times n} \text{ of full rank} \\ W'_a := [W_a|V_a] &= PU_a[Q|\tilde{Q}] \in \mathbb{Q}^{p\times n}, \quad a \in I \end{aligned}$$

- Use previous Algorithm on augmented input W'_0, $\{W'_a\}_a$

Algorithm for Pb. $\mathbb{D}$ - symmetrically low ranks in P, Q

- For $a, b \in I$ define $\Delta_{ab} = W_a W_0^{-1} W_b - W_b W_0^{-1} W_a \in \mathbb{Q}^{p \times p}$
- Rewrite as

$$\Delta_{ab} = V_a G_b - V_b G_a$$

  for some $V_a \in \mathbb{Q}^{p \times (n-p)}$, $G_a \in \mathbb{Q}^{(n-p) \times n}$ (explicit construction)
- Heuristically, if $p > \frac{2}{3}n$ and $t = \#I \geq 3$:

$$\bigcap_{b \in I \setminus \{a\}} \mathrm{Im}(\Delta_{ab}) = \mathrm{Im}(V_a) \ , \ a \in I$$

Algorithm

1. Compute $\Delta_{ab} = W_a W_0^{-1} W_b - W_b W_0^{-1} W_a$ for $a, b \in I$
2. Compute basis matrices $\{V_a'\}$ of $\bigcap_{b \in I \setminus \{a\}} \mathrm{Im}(\Delta_{ab})$ for every $a \in I$
3. Compute $\{V_a\}$ by solving a system of linear equations
4. Run first algorithm on $W_0' = [W_0 | 0]$ and $W_a' = [W_a | V_a]$ for $a \in I$

III • Applications

Motivation : Applications in Cryptography

1. The CRT-ACD Approximate Common Divisor Problem

   - improvement of the Coron-Pereira [CP19] algorithm
   - By solving a certain instance of this problem, we obtain a quadratic improvement in the number of input samples

2. CLT13 Multilinear Maps

   - improvement of the Cheon et al. attack [CHL$^+$15]
   - By solving a certain instance of this problem, we obtain a quadratic improvement in the number of encodings (of zero) needed for the attack

The CLT13 multilinear maps over the integers [CLT13]

- integers $n \geq 2$ (dimension of CLT13), $\kappa \geq 2$ multilinearity degree
- Instance generation: secret ”large” primes $p_1, \ldots, p_n$ and secret ”small” primes $g_1, \ldots, g_n$
  - $x_0 = \prod_{1 \leq i \leq n} p_i$ public

The CLT13 multilinear maps over the integers [CLT13]

- integers $n \geq 2$ (dimension of CLT13), $\kappa \geq 2$ multilinearity degree
- Instance generation: secret ”large” primes $p_1, \ldots, p_n$ and secret ”small” primes $g_1, \ldots, g_n$
    - $x_0 = \prod_{1 \leq i \leq n} p_i$ public
- Messages are elements $m = (m_1, \ldots, m_n) \in \mathbb{F}_{g_1} \times \cdots \times \mathbb{F}_{g_n}$

The CLT13 multilinear maps over the integers [CLT13]

- integers $n \geq 2$ (dimension of CLT13), $\kappa \geq 2$ multilinearity degree
- Instance generation: secret "large" primes $p_1, \ldots, p_n$ and secret "small" primes $g_1, \ldots, g_n$
  - $x_0 = \prod_{1 \leq i \leq n} p_i$ public
- Messages are elements $m = (m_1, \ldots, m_n) \in \mathbb{F}_{g_1} \times \cdots \times \mathbb{F}_{g_n}$
- Encoding space $\mathcal{E} = \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_n} \simeq \mathbb{Z}/x_0\mathbb{Z}$
  - graded structure: encode at levels $j \in \{1, \ldots, \kappa\}$
  - supports homomorphic addition and multiplication

The CLT13 multilinear maps over the integers [CLT13]

- integers $n \geq 2$ (dimension of CLT13), $\kappa \geq 2$ multilinearity degree
- Instance generation: secret "large" primes $p_1, \ldots, p_n$ and secret "small" primes $g_1, \ldots, g_n$
  - $x_0 = \prod_{1 \leq i \leq n} p_i$ public
- Messages are elements $m = (m_1, \ldots, m_n) \in \mathbb{F}_{g_1} \times \cdots \times \mathbb{F}_{g_n}$
- Encoding space $\mathcal{E} = \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_n} \simeq \mathbb{Z}/x_0\mathbb{Z}$
  - graded structure: encode at levels $j \in \{1, \ldots, \kappa\}$
  - supports homomorphic addition and multiplication
- A public zero-testing procedure $\mathcal{P} : \mathcal{E}_\kappa \to \{0, 1\}$ defined by public zero-test parameter $p_{zt} \in \mathbb{Z}/x_0\mathbb{Z}$

Application to the cryptanalysis of the CLT13 Mmap

Cheon *et al.* attack against CLT13, [CHL+15]

Application to the cryptanalysis of the CLT13 Mmap

Cheon *et al.* attack against CLT13, [CHL+15]

- Sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ of low-level encodings s.t
  $\forall\ (a, b, c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C} : abc = enc_{\kappa}(0)$
- $\#\mathcal{A} = n, \#\mathcal{B} = 2, \#\mathcal{C} = n$

Application to the cryptanalysis of the CLT13 Mmap

Cheon *et al.* attack against CLT13, [CHL$^+$15]

- Sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ of low-level encodings s.t
  $\forall\ (a, b, c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C} : abc = enc_\kappa(0)$
- $\#\mathcal{A} = n, \#\mathcal{B} = 2, \#\mathcal{C} = n$
- Using zero-test function, derive matrix equalities
  $W_a = P \cdot U_a \cdot Q$, $a = 1, 2$ with secret
    - P – $n \times n$ matrix of rank n (whp)
    - U_a – diagonal $n \times n$
    - Q – $n \times n$ matrix of rank n (whp)
- Find prime factorization of x_0 from W_1, W_2 by solving Problem $\mathbb{A}$

Application to the cryptanalysis of the CLT13 Mmap

Cheon *et al.* **attack against CLT13, [CHL$^+$15]**

- Sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ of low-level encodings s.t
  $\forall\ (a, b, c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C} : abc = enc_\kappa(0)$
- $\#\mathcal{A} = n, \#\mathcal{B} = 2, \#\mathcal{C} = n$
- Using zero-test function, derive matrix equalities
  $W_a = P \cdot U_a \cdot Q$, $a = 1, 2$ with secret
  - P – $n \times n$ matrix of rank n (whp)
  - U_a – diagonal $n \times n$
  - Q – $n \times n$ matrix of rank n (whp)
- Find prime factorization of x_0 from W_1, W_2 by solving Problem $\mathbb{A}$

Cryptanalysis with fewer encodings

Rearrange sets $\mathcal{A}, \mathcal{B}, \mathcal{C}$ and solve Pb. $\mathbb{C}/\mathbb{D}$ instead of $\mathbb{A}$:

- $\mathcal{O}(\sqrt{n})$ encodings of zero vs. n
- $4n/3 + \mathcal{O}(\sqrt{n})$ total encodings vs. $2n + 2$

Conclusion

This work

- generalizes a computational problem based on simultaneous matrix diagonalization
- provides heuristic algorithms to solve this problem
- offers quadratic improvement in input size for two problems with interest in computational number theory and cryptanalysis
- open: other applications possibly to find

Thank you for your attention

- Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé, Cryptanalysis of the Multilinear Map over the Integers, EUROCRYPT 2015, Part I, LNCS, vol. 9056, Springer, 2015, pp. 3–12.
- Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi, Practical multilinear Maps over the Integers, CRYPTO, Springer, 2013, pp. 476–493.
- Jean-Sébastien Coron and Hilder V. L. Pereira, On Kilian's Randomization of Multilinear Map Encodings, Advances in Cryptology - ASIACRYPT 2019 - Proceedings, Part II, 2019, pp. 325–355.