

SIMULTANEOUS DIAGONALIZATION OF INCOMPLETE MATRICES AND APPLICATIONS

Jean-Sebastien Coron¹

Luca Notarnicola²

Gabor Wiese³

^{1,2,3} University of Luxembourg

14th Algorithmic Number Theory
Symposium • July 2020



UNIVERSITÉ DU
LUXEMBOURG

Introduction

Introduction

- Let
- $n \in \mathbb{N}_{\geq 2}$
 - $P, Q \in \mathbb{Q}^{n \times n}$ of full rank (then PQ of full rank)
 - $U_1 \in \mathbb{Q}^{n \times n}$ diagonal matrix

Introduction

- Let
- $n \in \mathbb{N}_{\geq 2}$
 - $P, Q \in \mathbb{Q}^{n \times n}$ of full rank (then PQ of full rank)
 - $U_1 \in \mathbb{Q}^{n \times n}$ diagonal matrix

$$\begin{array}{cc} \boxed{P} & \boxed{Q} \\ \boxed{P} & \boxed{U_1} & \boxed{Q} \end{array} = \begin{array}{c} \boxed{W_0} \\ \boxed{W_1} \end{array} \in \mathbb{Q}^{n \times n}$$

The diagram illustrates the decomposition of the product of two matrices P and Q . The top row shows P and Q as separate boxes, which are equal to a single box W_0 . The bottom row shows P , U_1 (a box with a diagonal line), and Q as separate boxes, which are equal to a single box W_1 . Both W_0 and W_1 are labeled as $\mathbb{Q}^{n \times n}$ matrices.

Introduction

- Let
- $n \in \mathbb{N}_{\geq 2}$
 - $P, Q \in \mathbb{Q}^{n \times n}$ of full rank (then PQ of full rank)
 - $U_1 \in \mathbb{Q}^{n \times n}$ diagonal matrix

$$\begin{array}{cc} \boxed{P} & \boxed{Q} \\ \boxed{P} & \boxed{U_1} & \boxed{Q} \end{array} = \begin{array}{c} \boxed{W_0} \\ \boxed{W_1} \end{array} \in \mathbb{Q}^{n \times n}$$

Problem: given the product matrices $W_0, W_1 \in \mathbb{Q}^{n \times n}$
reveal the diagonal entries of $U_1 \in \mathbb{Q}^{n \times n}$

Introduction

- Let
- $n \in \mathbb{N}_{\geq 2}$
 - $P, Q \in \mathbb{Q}^{n \times n}$ of full rank (then PQ of full rank)
 - $U_1 \in \mathbb{Q}^{n \times n}$ diagonal matrix

$$\begin{array}{cc} \boxed{P} & \boxed{Q} \\ \boxed{P} & \boxed{U_1} & \boxed{Q} \end{array} = \begin{array}{c} \boxed{W_0} \\ \boxed{W_1} \end{array} \in \mathbb{Q}^{n \times n}$$

The diagram illustrates the relationship between matrices P , Q , U_1 , W_0 , and W_1 . The first row shows P and Q as white boxes, followed by an equals sign and a green box labeled W_0 , with the text $\in \mathbb{Q}^{n \times n}$ to its right. The second row shows P , U_1 (a white box with a red diagonal line), and Q as white boxes, followed by an equals sign and a green box labeled W_1 , with the text $\in \mathbb{Q}^{n \times n}$ to its right.

Problem: given the product matrices $W_0, W_1 \in \mathbb{Q}^{n \times n}$
reveal the diagonal entries of $U_1 \in \mathbb{Q}^{n \times n}$

Introduction

- Let
- $n \in \mathbb{N}_{\geq 2}$
 - $P, Q \in \mathbb{Q}^{n \times n}$ of full rank (then PQ of full rank)
 - $U_1 \in \mathbb{Q}^{n \times n}$ diagonal matrix

$$\begin{array}{cc} \boxed{P} & \boxed{Q} \\ \boxed{P} & \boxed{U_1} & \boxed{Q} \end{array} = \begin{array}{c} \boxed{W_0} \\ \boxed{W_1} \end{array} \in \mathbb{Q}^{n \times n}$$

The diagram shows two equations. The first equation shows two boxes labeled P and Q followed by an equals sign and a green box labeled W_0, with the text "in Q^{n x n}" to the right. The second equation shows three boxes: P, U_1 (with a red diagonal line), and Q, followed by an equals sign and a green box labeled W_1, with the text "in Q^{n x n}" to the right.

Problem: given the product matrices $W_0, W_1 \in \mathbb{Q}^{n \times n}$
reveal the diagonal entries of $U_1 \in \mathbb{Q}^{n \times n}$

Solution: compute the eigenvalues of $W_0^{-1} W_1 = Q^{-1} U_1 Q$

Problem Statement

- We now lower the ranks of P and Q

$$\boxed{P} \boxed{U_1} \boxed{Q} = \boxed{W_1}$$

Problem Statement

- We now lower the ranks of P and Q

The diagram shows the following sequence of operations:

- Matrix $P \in \mathbb{Q}^{p \times n}$ with $\text{rank } p \leq n$. A blue shaded region of size $p \times p$ is shown in the top-left corner, with a dashed blue line indicating the boundary.
- Matrix U_1 is shown as a square with a diagonal orange band.
- Matrix $Q \in \mathbb{Q}^{h \times q}$ with $\text{rank } q \leq n$. A blue shaded region of size $h \times q$ is shown in the top-left corner, with a dashed blue line indicating the boundary.
- An equals sign follows.
- Matrix W_1 is shown as a square with a blue shaded region of size $p \times q$ in the top-left corner, with a dashed blue line indicating the boundary.
- The final result is a matrix in $\mathbb{Q}^{p \times q}$.

Problem Statement

- We now **lower** the ranks of P and Q

The diagram shows the product of three matrices: P , U_1 , and Q , resulting in matrix W_1 .

$P \in \mathbb{Q}^{p \times n}$
rank $p \leq n$

U_1

$Q \in \mathbb{Q}^{h \times q}$
rank $q \leq n$

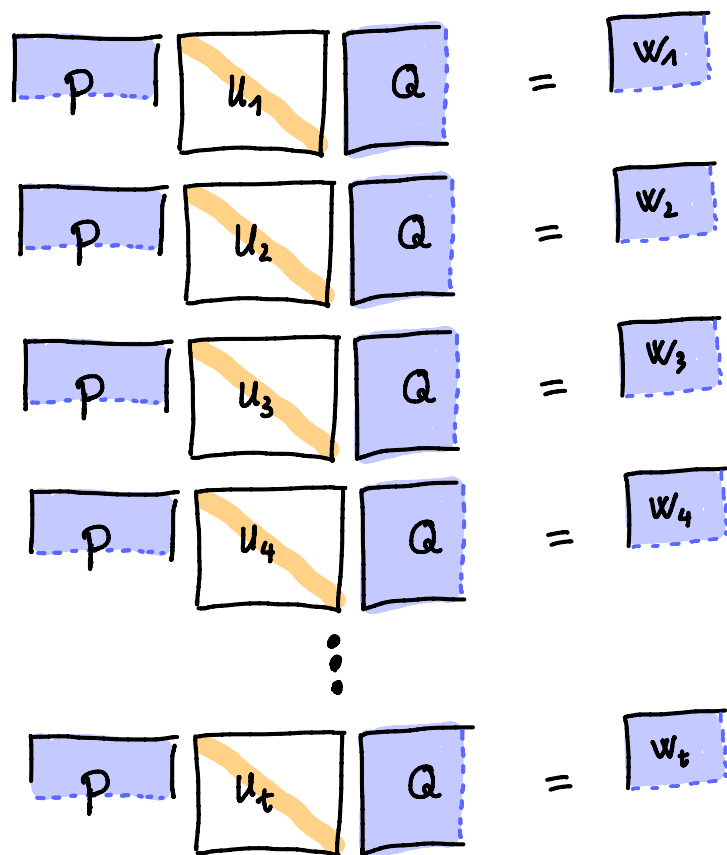
$= W_1 \in \mathbb{Q}^{p \times q}$

product matrix is "incomplete"

Detailed description: The diagram consists of four square boxes representing matrices. The first box is labeled 'P' and has a blue shaded top portion with a dashed blue line below it. Below it is the text 'P in Q^{p x n} rank p <= n'. The second box is labeled 'U_1' and has a diagonal orange shaded band. The third box is labeled 'Q' and has a blue shaded left portion with a dashed blue line to its right. Below it is the text 'Q in Q^{h x q} rank q <= n'. An equals sign follows. The fourth box is labeled 'W_1' and has a blue shaded top-left corner with dashed blue lines extending to the right and down. Below it is the text 'W_1 in Q^{p x q}'. A purple arrow points from the text 'product matrix is "incomplete"' to the 'W_1' box.

Problem Statement


- We now lower the ranks of P and Q
- In compensation we consider more samples ($i \in I := \{1, \dots, t\}$, $t \geq 2$)



Problem Statement

- We now lower the ranks of P and Q
- In compensation we consider more samples ($i \in I := \{1, \dots, t\}$, $t \geq 2$)

$$\begin{array}{l} \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_1 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_1 \\ \hline \end{array} \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_2 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_2 \\ \hline \end{array} \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_3 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_3 \\ \hline \end{array} \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_4 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_4 \\ \hline \end{array} \\ \vdots \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_t \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_t \\ \hline \end{array} \end{array}$$



Problem Statement
given the matrices
 $\{W_i\}_{i \in I \cup \{0\}} \subset \mathbb{Q}^{p \times q}$
compute the diagonal
entries of the matrices
 $\{U_i\}_{i \in I} \subset \mathbb{Q}^{n \times n}$

Problem Statement

- We now lower the ranks of P and Q
- In compensation we consider more samples ($i \in I := \{1, \dots, t\}$, $t \geq 2$)

$$\begin{array}{l} \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_1 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_1 \\ \hline \end{array} \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_2 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_2 \\ \hline \end{array} \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_3 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_3 \\ \hline \end{array} \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_4 \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_4 \\ \hline \end{array} \\ \vdots \\ \begin{array}{|c|} \hline P \\ \hline \end{array} \begin{array}{|c|} \hline U_t \\ \hline \end{array} \begin{array}{|c|} \hline Q \\ \hline \end{array} = \begin{array}{|c|} \hline W_t \\ \hline \end{array} \end{array}$$

Problem Statement
given the matrices
 $\{W_i\}_{i \in I \cup \{0\}} \subset \mathbb{Q}^{p \times q}$
compute the diagonal
entries of the matrices
 $\{U_i\}_{i \in I} \subset \mathbb{Q}^{n \times n}$

Algorithms

- We study 2 cases :

$(p \leq n, q = n)$ and $(p \leq n, q = p)$, $t \in \mathbb{N}$

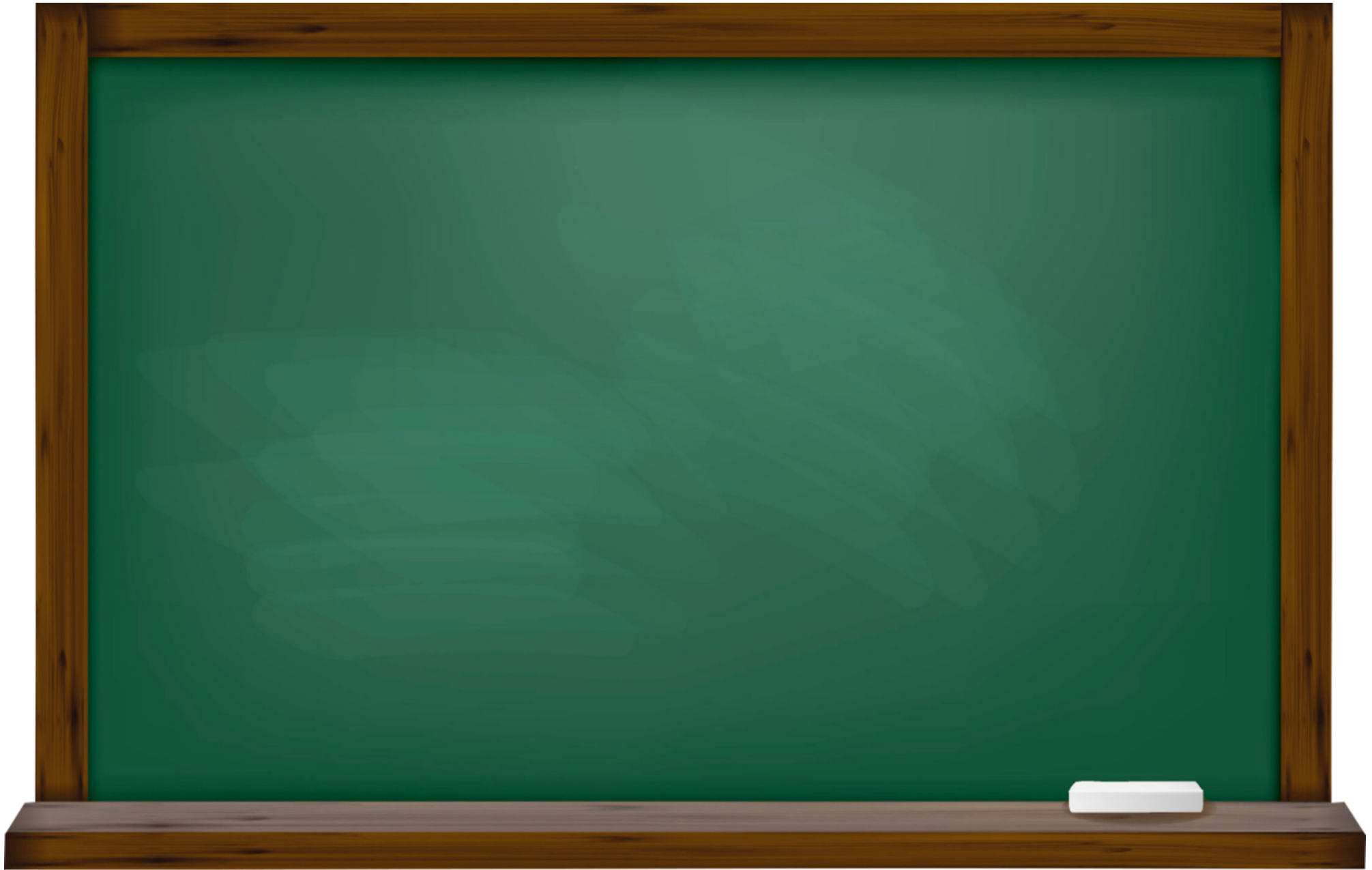
- Find range of parameters minimizing p, q, t for fixed n

Algorithms

- We study 2 cases :
 $(p \leq n, q = n)$ and $(p \leq n, q = p)$, $t \in \mathbb{N}$
- Find range of parameters minimizing p, q, t for fixed n
- We obtain heuristic algorithms

$p \leq n, q = n$	$p \leq n, q = p$
$p = O(\sqrt{n})$	$p = O(\frac{2}{3}n)$
$q = n$	$q = p$
$t = O(\sqrt{n})$	$t = O(\sqrt{n})$

Case ($p \leq n, q = n$) - main tools



Case $(p \leq n, q = n)$ - main tools

Step 1: given $W_0 = PQ$, $W_i = PU_iQ$, $i \in \bar{I}$

write $W_i = (PQ)(Q^{-1}U_iQ) =: W_0Z_i$, $i \in \bar{I}$

Case ($p \leq n, q = n$) - main tools

Step 1: given $W_0 = PQ$, $W_i = PU_iQ$, $i \in I$

write $W_i = (PQ)(Q^{-1}U_iQ) =: W_0Z_i$, $i \in I$

GOAL: Recover $\{Z_i\}_i$

Case ($p \leq n, q = n$) - main tools

Step 1: given $W_0 = PQ$, $W_i = PU_iQ$, $i \in I$

write $W_i = (PQ)(Q^{-1}U_iQ) =: W_0Z_i$, $i \in I$

GOAL: Recover $\{Z_i\}_i$



The matrices $\{Z_i\}_i$ commute

Case ($p \leq n, q = n$) - main tools

Step 1: given $W_0 = PQ$, $W_i = PU_iQ$, $i \in I$

write $W_i = (PQ)(Q^{-1}U_iQ) =: W_0 Z_i$, $i \in I$

GOAL: Recover $\{Z_i\}_i$



The matrices $\{Z_i\}_i$ commute

general solution: $Z_i = Y_i + SX_i$, $i \in I$

$W_0 Y_i = W_i$, $\langle S \rangle = \ker(W_0)$

Case ($p \leq n, q = n$) - main tools

Step 1: given $W_0 = PQ$, $W_i = PU_iQ$, $i \in I$

write $W_i = (PQ)(Q^{-1}U_iQ) =: W_0 Z_i$, $i \in I$

GOAL: Recover $\{Z_i\}_i$



The matrices $\{Z_i\}_i$ commute

general solution: $Z_i = Y_i + S(X_i)$, $i \in I$

$$W_0 Y_i = W_i, \quad \langle S \rangle = \ker(W_0)$$

known

unknown!

Case ($p \leq n, q = n$) - main tools

Step 2: • The commutation of $\{z_i\}_i$
allows us to write down explicit systems
of linear equations in the variables $\{x_i\}_i$

Case ($p \leq n, q = n$) - main tools

- Step 2: • The commutation of $\{z_i\}_i$
allows us to write down explicit systems
of linear equations in the variables $\{x_i\}_i$
- $E = \#(\text{Equations}), v = \#(\text{variables})$
are explicit in parameters p, q, t, n

Case ($p \leq n, q = n$) - main tools

- Step 2: • The commutation of $\{z_i\}_i$ allows us to write down explicit systems of linear equations in the variables $\{x_i\}_i$
- $E = \#(\text{Equations}), V = \#(\text{variables})$ are explicit in parameters p, q, t, n
 - if $E \geq V \Rightarrow$ unique solution to "our" system of equations

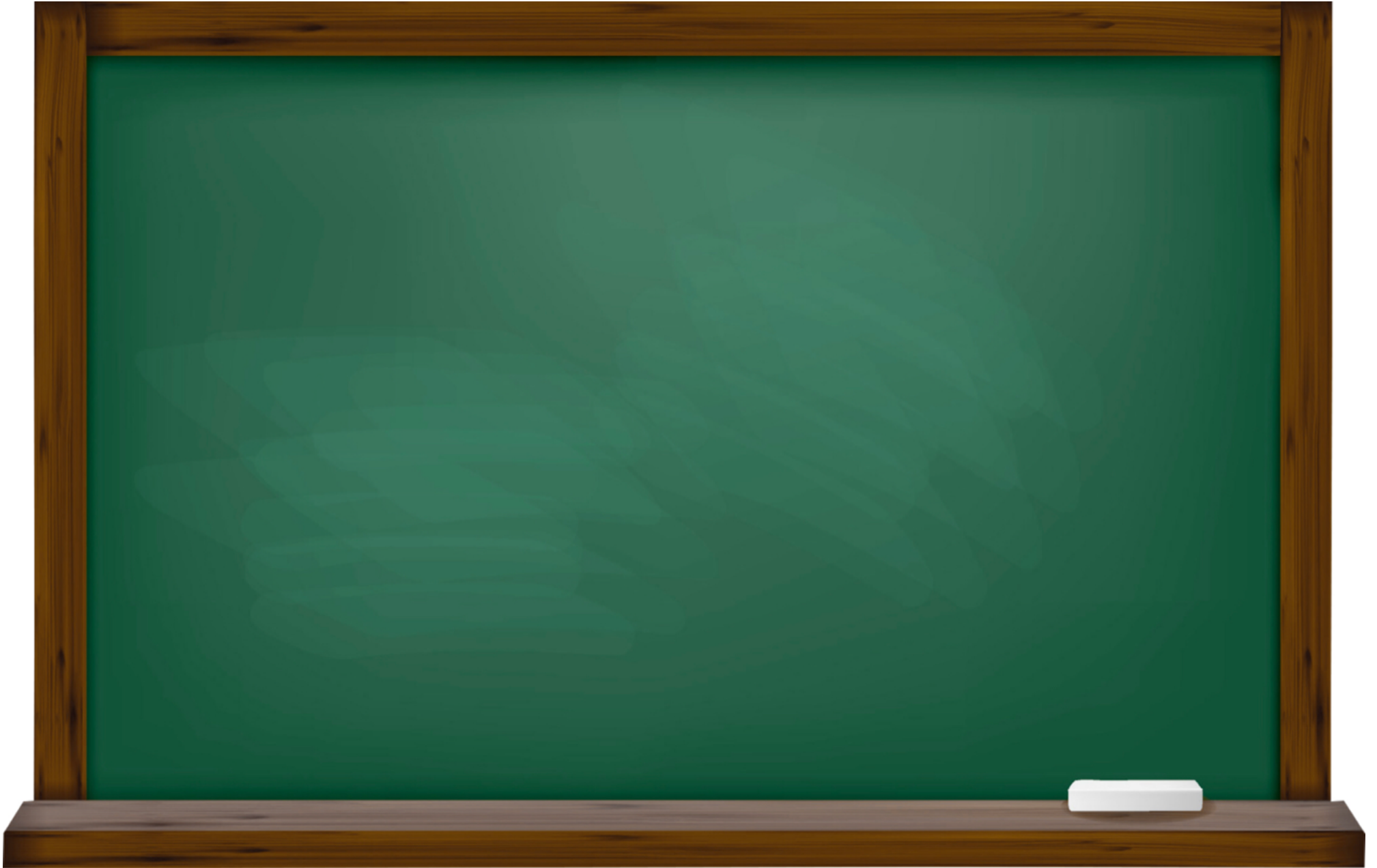
Case ($p \leq n, q = n$) - main tools

- Step 2: • The commutation of $\{z_i\}_i$ allows us to write down explicit systems of linear equations in the variables $\{x_i\}_i$
- $E = \#(\text{Equations}), V = \#(\text{variables})$ are explicit in parameters p, q, t, n
 - if $E \geq V$ \Rightarrow unique solution to "our" system of equations
HEURISTIC

Case ($p \leq n, q = n$) - main tools

- Step 2: • The commutation of $\{z_i\}_i$ allows us to write down explicit systems of linear equations in the variables $\{x_i\}_i$
- $E = \#(\text{Equations}), V = \#(\text{variables})$ are explicit in parameters p, q, t, n
 - if $E \geq V$ \Rightarrow unique solution to "our" system of equations
 - explicit parameter selection
 - HEURISTIC
 - minimization
 - $p, t = O(\sqrt{n})$

Case ($p = q \leq n$) - main tools



Case ($p = q \leq n$) - main tools

$$\begin{array}{ccc} p \times n & n \times n & n \times p \\ \boxed{P} & \boxed{U_i} & \boxed{Q} \\ & & = \end{array} \quad \begin{array}{c} p \times p \\ \boxed{W_i} \end{array}$$

Case ($p = q \leq n$) - main tools

$$\begin{array}{ccc} p \times n & n \times n & n \times p \\ \boxed{P} & \boxed{U_i} & \boxed{Q} \end{array} = \boxed{W_i} \begin{array}{c} p \times p \end{array}$$

Idea: reduce to the previous case by augmenting $\{W_i\}_i$ suitably

Case ($p = q \leq n$) - main tools

$$\begin{array}{c} p \times n \\ \boxed{P} \end{array} \quad \begin{array}{c} n \times n \\ \boxed{U_i} \end{array} \quad \begin{array}{c} n \times p \rightarrow n \times n \\ \text{full rank} \\ \boxed{Q} \end{array} \quad \begin{array}{c} p \times p \rightarrow p \times n \\ \boxed{W_i} \end{array} \quad \begin{array}{c} \boxed{\text{Z}} \end{array} = \begin{array}{c} \boxed{W_i} \end{array} \quad \begin{array}{c} \boxed{\text{Z}} \end{array}$$

Idea: reduce to the previous case by augmenting $\{W_i\}_i$ suitably

Case ($p = q \leq n$) - main tools

$$\begin{array}{c} p \times n \\ \boxed{P} \end{array} \quad \begin{array}{c} n \times n \\ \boxed{U_i} \end{array} \quad \begin{array}{c} n \times p \rightarrow n \times n \\ \text{full rank} \\ \boxed{Q} \quad \boxed{Q'} \end{array} = \begin{array}{c} p \times p \rightarrow p \times n \\ \boxed{W_i} \quad \boxed{V_i} \end{array}$$

Idea: reduce to the previous case by augmenting $\{W_i\}_i$ suitably

- augmentation process:
compute matrices $\{V_i\}_i$ s.t. $V_i = P U_i Q'$
($i \in I$)
and $(Q | Q') \in GL_n(\mathbb{Q})$

Case ($p = q \leq n$) - main tools

$$\begin{array}{c} p \times n \\ \boxed{P} \end{array} \quad \begin{array}{c} n \times n \\ \boxed{U_i} \end{array} \quad \begin{array}{c} n \times p \rightarrow n \times n \\ \text{full rank} \\ \boxed{Q} \quad \boxed{Q'} \end{array} = \begin{array}{c} p \times p \rightarrow p \times n \\ \boxed{W_i} \quad \boxed{V_i} \end{array}$$

Idea: reduce to the previous case by augmenting $\{W_i\}_i$ suitably

- computation of $\{V_i\}_i$ needs some extra information

parameters: $p = \mathcal{O}\left(\frac{2}{3}n\right)$
 $t = \mathcal{O}(\sqrt{n})$

Applications

Applications

- our algorithms apply to

Applications

- our algorithms apply to



APPROXIMATE COMMON DIVISOR PROBLEM

- CRT - multiprime version:
reveal prime factorisation
of $N = p_1 \cdots p_n$ from
many CRT - residues
- quadratic improvement
of an algorithm of
Coron - Pereira [CP19]

[CP19] J.S. Coron and H.V.L. Pereira. On Kilian's randomization of multilinear map encodings. ASIACRYPT 2019

Applications

- our algorithms apply to

APPROXIMATE COMMON DIVISOR PROBLEM

- CRT - multiprime version: reveal prime factorisation of $N = p_1 \cdots p_n$ from many CRT - residues
- quadratic improvement of an algorithm of Coron - Pereira [CP19]

CRYPTOGRAPHIC MULTILINEAR MAPS

- [CLT13] graded encoding schemes over the integers
- total break given many low-level encodings of zero (Cheon et al. attack [CHL⁺15])
- quadratic improvement of [CHL⁺15] - cryptanalysis

[CP19] J.S. Coron and H.V.L. Pereira. On Kilian's randomization of multilinear map encodings. ASIACRYPT 2019

[CLT13] J.S. Coron, T. Lepoint, M. Tibouchi. Practical multilinear maps over the integers. CRYPTO 2013

[CHL⁺15] J.H. Cheon, K. Han, C. Lee, H. Ryu, D. Stehlé. Cryptanalysis of the multilinear map over the integers. EUROCRYPT 2015

CRT-ACD Problem - Main ideas

Problem Statement

- $N = \prod_{i=1}^n p_i$, p_i large secret primes
↑
public modulus

- a finite set

$$S = \{x_1, \dots, x_{|S|}\} \subset \mathbb{Z}$$

with "small" residues mod $\{p_i\}$:

$$\text{i.e. } x_j \equiv x_j^{(i)} \pmod{p_i} \quad j=1, \dots, |S|$$

and $|x_j^{(i)}|$ "small"
compared to size
of p_i

CRT-ACD Problem - Main ideas

Problem Statement

- $N = \prod_{i=1}^n p_i$, p_i large secret primes
↑
public modulus

- a finite set

$$S = \{x_1, \dots, x_{|S|}\} \subset \mathbb{Z}$$

with "small" residues mod $\{p_i\}$:

$$\text{i.e. } x_j \equiv x_j^{(i)} \pmod{p_i} \\ j=1, \dots, |S|$$

and $|x_j^{(i)}|$ "small"
compared to size
of p_i

→ given N and S
factor N completely

CRT-ACD Problem - Main ideas

Problem Statement

- $N = \prod_{i=1}^n p_i$, p_i large secret primes
↑
public modulus

- a finite set

$$S = \{x_1, \dots, x_{|S|}\} \subset \mathbb{Z}$$

with "small" residues mod $\{p_i\}$:

$$\text{i.e. } x_j \equiv x_j^{(i)} \pmod{p_i} \quad j=1, \dots, |S|$$

and $|x_j^{(i)}|$ "small"
compared to size
of p_i

→ given N and S
factor N completely

[CP19]:

$$|S| = n+1$$

this work:

$$|S| = 2 \lceil \sqrt{2n} \rceil$$

CRT-ACD Problem - Main ideas

Problem Statement

- $N = \prod_{i=1}^n p_i$, p_i large secret primes
↑
public modulus

- a finite set

$$S = \{x_1, \dots, x_{|S|}\} \subset \mathbb{Z}$$

with "small" residues mod $\{p_i\}$:

$$\text{i.e. } x_j \equiv x_j^{(i)} \pmod{p_i} \quad j=1, \dots, |S|$$

and $|x_j^{(i)}|$ "small"
compared to size
of p_i

→ given N and S
factor N completely

[CP19]:

$$|S| = n+1$$

this work:

$$|S| = 2 \lceil \sqrt{2n} \rceil$$

quadratic improvement
in input length

CRT-ACD Problem - Main ideas

Problem Statement

- $N = \prod_{i=1}^n p_i$, p_i large secret primes
↑
public modulus

- a finite set

$$S = \{x_1, \dots, x_{|S|}\} \subset \mathbb{Z}$$

with "small" residues mod $\{p_i\}$:

$$\text{i.e. } x_j \equiv x_j^{(i)} \pmod{p_i} \quad j=1, \dots, |S|$$

and $|x_j^{(i)}|$ "small"
compared to size
of p_i

→ given N and S
factor N completely

[CP19]:

$$|S| = n+1$$

this work:

$$|S| = 2 \lceil \sqrt{2n} \rceil$$

quadratic improvement
in input length

In practice:

e.g. $n=50$

$$\text{size}\{p_i\} \sim 2^{800}$$

$$\text{residue size} \sim 2^{100}$$

$|S|$

[CP19] : 51

this work : 19

CRT-ACD Problem - Main ideas

[CP19]

- $|S| = n + 1$

this work

CRT-ACD Problem - Main ideas

[CP19]

- $|S| = n + 1$

- $S = \{x_1, \dots, x_n, y\}$
construct (public) vector

$$\underline{b} = \begin{pmatrix} \underline{x} \\ y \cdot \underline{x} \end{pmatrix} \in \mathbb{Z}^{2n}$$

$$\underline{x} = (x_1, \dots, x_n)^T \in \mathbb{Z}^n$$

this work

CRT-ACD Problem - Main ideas

[CP19]

- $|S| = n + 1$
- $S = \{x_1, \dots, x_n, y\}$
construct (public) vector

$$\underline{b} = \begin{pmatrix} \underline{x} \\ y \cdot \underline{x} \end{pmatrix} \in \mathbb{Z}^{2n}$$

$$\underline{x} = (x_1, \dots, x_n)^T \in \mathbb{Z}^n$$

this work

- $|S| = p + t$
 $p, t \in \mathbb{N}, p + t \leq n$

CRT-ACD Problem - Main ideas

[CP19]

- $|S| = n + 1$
- $S = \{x_1, \dots, x_n, y\}$
construct (public) vector

$$\underline{b} = \begin{pmatrix} \underline{x} \\ y \cdot \underline{x} \end{pmatrix} \in \mathbb{Z}^{2n}$$

$$\underline{x} = (x_1, \dots, x_n)^T \in \mathbb{Z}^n$$

this work

- $|S| = p + t$
 $p, t \in \mathbb{N}, p + t \leq n$
- $S = \{x_1, \dots, x_p, y_1, \dots, y_t\}$
construct (public) vector

$$\underline{b} = \begin{pmatrix} \underline{x} \\ y_1 \cdot \underline{x} \\ \vdots \\ y_t \cdot \underline{x} \end{pmatrix} \in \mathbb{Z}^{p(t+1)}$$

$$\underline{x} = (x_1, \dots, x_p) \in \mathbb{Z}^p$$

CRT-ACD Problem - Main ideas

[CP19]

- $|S| = n + 1$
- $S = \{x_1, \dots, x_n, y\}$
construct (public) vector

$$\underline{b} = \begin{pmatrix} \underline{x} \\ y \cdot \underline{x} \end{pmatrix} \in \mathbb{Z}^{2n}$$

$$\underline{x} = (x_1, \dots, x_n)^T \in \mathbb{Z}^n$$

"fixed" dimension

this work

- $|S| = p + t$
 $p, t \in \mathbb{N}, p + t \leq n$
- $S = \{x_1, \dots, x_p, y_1, \dots, y_t\}$
construct (public) vector

$$\underline{b} = \begin{pmatrix} \underline{x} \\ y_1 \cdot \underline{x} \\ \vdots \\ y_t \cdot \underline{x} \end{pmatrix} \in \mathbb{Z}^{p(t+1)}$$

$$\underline{x} = (x_1, \dots, x_p) \in \mathbb{Z}^p$$

"variable" dimension

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

By CRT:

$$\underline{b} = \sum_i \alpha_i \underline{b}^i \pmod{N}$$

$$\alpha_i \in \mathbb{Z}$$

$$\underline{b}^i \in \mathbb{Z}^{p^{(t+1)}} \text{ "short"}$$

$$\underline{b} \equiv \underline{b}^i \pmod{p_i}$$

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

By CRT:

$$\underline{b} = \sum_i \alpha_i \underline{b}^i \pmod{N}$$

$$\alpha_i \in \mathbb{Z}$$

$$\underline{b}^i \in \mathbb{Z}^{p^{(t+1)}} \text{ "short"}$$

$$\underline{b} \equiv \underline{b}^i \pmod{p_i}$$

• Step 1: Lattice reduction

from \underline{b} and N compute

with $\underline{x} \equiv \underline{x}^i$, $y_j \equiv y_j^i \pmod{p_i}$

$$\begin{aligned} & \left[\underline{b}^1 \mid \dots \mid \underline{b}^n \right] \cdot Q \\ &= \left[\begin{array}{c|c|c} \underline{x}^1 & & \underline{x}^n \\ y_1^1 \underline{x}^1 & \dots & y_1^n \underline{x}^n \\ \vdots & & \vdots \\ y_t^1 \underline{x}^1 & & y_t^n \underline{x}^n \end{array} \right] \cdot Q \end{aligned}$$

for $Q \in GL_n(\mathbb{Q})$

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

By CRT:

$$\underline{b} = \sum_i \alpha_i \underline{b}^i \pmod{N}$$

$$\alpha_i \in \mathbb{Z}$$

$$\underline{b}^i \in \mathbb{Z}^{p^{(t+1)}} \text{ "short"}$$

$$\underline{b} \equiv \underline{b}^i \pmod{p_i}$$

• Step 1: Lattice reduction

from \underline{b} and N compute

with $\underline{x} \equiv \underline{x}^i$, $y_j \equiv y_j^i \pmod{p_i}$

$$\begin{aligned} & \left[\underline{b}^1 \mid \dots \mid \underline{b}^n \right] \cdot Q \\ &= \left[\begin{array}{c|c|c} \underline{x}^1 & & \\ y_1^1 \underline{x}^1 & \dots & y_1^n \underline{x}^n \\ \vdots & & \vdots \\ y_t^1 \underline{x}^1 & & y_t^n \underline{x}^n \end{array} \right] \cdot Q \end{aligned}$$

for $Q \in GL_n(\mathbb{Q})$

• Step 2: Diagonalization

writing out components with

$$P := [\underline{x}^1 \mid \dots \mid \underline{x}^n] \in \mathbb{Z}^{p \times n}$$

$$U_i := \text{diag}(y_1^i, \dots, y_n^i) \in \mathbb{Z}^{n \times n}$$

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

By CRT:

$$\underline{b} = \sum_i \alpha_i \underline{b}^i \pmod{N}$$

$$\alpha_i \in \mathbb{Z}$$

$$\underline{b}^i \in \mathbb{Z}^{p^{(t+1)}} \text{ "short"}$$

$$\underline{b} \equiv \underline{b}^i \pmod{p_i}$$

• Step 1: Lattice reduction

from \underline{b} and N compute

with $\underline{x} \equiv \underline{x}^i$, $y_j \equiv y_j^i \pmod{p_i}$

$$\begin{aligned} & \left[\underline{b}^1 \mid \dots \mid \underline{b}^n \right] \cdot Q \\ &= \left[\begin{array}{c|c|c} \underline{x}^1 & & \\ y_1^1 \underline{x}^1 & \dots & y_1^n \underline{x}^n \\ \vdots & & \vdots \\ y_t^1 \underline{x}^1 & & y_t^n \underline{x}^n \end{array} \right] \cdot Q \end{aligned}$$

for $Q \in GL_n(\mathbb{Q})$

• Step 2: Diagonalization

writing out components with

$$P := [\underline{x}^1 \mid \dots \mid \underline{x}^n] \in \mathbb{Z}^{p \times n}$$

$$U_i := \text{diag}(y_1^i, \dots, y_n^i) \in \mathbb{Z}^{n \times n}$$

this gives public matrices

$$W_0 := P \cdot Q$$

$$W_i := P U_i Q, \quad i \in \{1, \dots, t\}$$

our algorithm reveals

diagonal entries of $\{U_i\}$

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

By CRT:

$$\underline{b} = \sum_i \alpha_i \underline{b}^i \pmod{N}$$

$$\alpha_i \in \mathbb{Z}$$

$$\underline{b}^i \in \mathbb{Z}^{p^{(t+1)}} \text{ "short"}$$

$$\underline{b} \equiv \underline{b}^i \pmod{p_i}$$

• Step 1: Lattice reduction

from \underline{b} and N compute

with $\underline{x} \equiv \underline{x}^i$, $y_j \equiv y_j^i \pmod{p_i}$

$$\begin{aligned} & \left[\underline{b}^1 \mid \dots \mid \underline{b}^n \right] \cdot Q \\ &= \left[\begin{array}{c|c|c} \underline{x}^1 & & \\ y_1^1 \underline{x}^1 & \dots & y_1^n \underline{x}^n \\ \vdots & & \vdots \\ y_t^1 \underline{x}^1 & & y_t^n \underline{x}^n \end{array} \right] \cdot Q \end{aligned}$$

for $Q \in GL_n(\mathbb{Q})$

• Step 2: Diagonalization

writing out components with

$$P := [\underline{x}^1 \mid \dots \mid \underline{x}^n] \in \mathbb{Z}^{p \times n}$$

$$U_i := \text{diag}(y_1^i, \dots, y_n^i) \in \mathbb{Z}^{n \times n}$$

this gives public matrices

$$W_0 := P \cdot Q$$

$$W_i := P U_i Q, \quad i \in \{1, \dots, t\}$$

our algorithm reveals

diagonal entries of $\{U_i\}_i$

• Step 3: gcd computation

gcd computation reveals
prime factors $\{p_i\}_i$ of N

CRT-ACD Problem - Main ideas

Algorithm in 3 steps:

By CRT:

$$\underline{b} = \sum_i \alpha_i \underline{b}^i \pmod{N}$$

$$\alpha_i \in \mathbb{Z}$$

$$\underline{b}^i \in \mathbb{Z}^{p^{(t+1)}} \text{ "short"}$$

$$\underline{b} \equiv \underline{b}^i \pmod{p_i}$$

• Step 1: Lattice reduction

from \underline{b} and N compute

with $\underline{x} \equiv \underline{x}^i$, $y_j \equiv y_j^i \pmod{p_i}$

$$\begin{aligned} & \left[\underline{b}^1 \mid \dots \mid \underline{b}^n \right] \cdot Q \\ &= \left[\begin{array}{c|c|c} \underline{x}^1 & & \underline{x}^n \\ y_1^1 \underline{x}^1 & \dots & y_1^n \underline{x}^n \\ \vdots & & \vdots \\ y_t^1 \underline{x}^1 & & y_t^n \underline{x}^n \end{array} \right] \cdot Q \end{aligned}$$

for $Q \in GL_n(\mathbb{Q})$

• Step 2: Diagonalization

writing out components with

$$P := [\underline{x}^1 \mid \dots \mid \underline{x}^n] \in \mathbb{Z}^{p \times n}$$

$$U_i := \text{diag}(y_1^i, \dots, y_n^i) \in \mathbb{Z}^{n \times n}$$

this gives public matrices

$$W_0 := P \cdot Q$$

$$W_i := P U_i Q, \quad i \in \{1, \dots, t\}$$

our algorithm ^{*} reveals

diagonal entries of $\{U_i\}$

• Step 3: gcd computation

gcd computation reveals
prime factors $\{p_i\}$ of N

^{*} with $p, t = O(\sqrt{n})$

$$|S| = p + t$$

Cryptanalysis of CLT13-maps

Cryptanalysis of CLT13-maps

- CLT13: construction of approximate multilinear maps based on graded encoding schemes
- hardness: factorization and CRT-representations

Cryptanalysis of CLT13-maps

- CLT13: construction of approximate multilinear maps based on graded encoding schemes

hardness: factorization and CRT-representations

applications: multiparty DH-key exchange, program obfuscation, ...

Cryptanalysis of CLT13-maps

- CLT13: construction of approximate multilinear maps based on graded encoding schemes

hardness: factorization and CRT-representations

applications: multiparty DH-key exchange, program obfuscation, ...

- [CHL⁺15]: total break of the DH-key exchange on CLT13 with $O(n)$ encodings of zero

Cryptanalysis of CLT13-maps

- CLT13: construction of approximate multilinear maps based on graded encoding schemes

hardness: factorization and CRT-representations

applications: multiparty DH-key exchange, program obfuscation, ...

- [CHL⁺15]: total break of the DH-key exchange on CLT13 with $O(n)$ encodings of zero
↳ this work: $O(\sqrt{n})$

Cryptanalysis of CLT13-maps

- CLT13: construction of approximate multilinear maps based on graded encoding schemes
hardness: factorization and CRT-representations
applications: multiparty DH-key exchange, program obfuscation, ...
- [CHL⁺15]: total break of the DH-key exchange on CLT13 with $O(n)$ encodings of zero
↳ this work: $O(\sqrt{n})$
- impact: enough low-level encodings (of zero) are not always available to the attacker
→ cryptanalysis with limited number of encodings

Cryptanalysis of CLT13-maps

- CLT13: construction of approximate multilinear maps based on graded encoding schemes
hardness: factorization and CRT-representations
applications: multiparty DH-key exchange, program obfuscation, ...
- [CHL⁺15]: total break of the DH-key exchange on CLT13 with $O(n)$ encodings of zero
↳ this work: $O(\sqrt{n})$
- impact: enough low-level encodings (of zero) are not always available to the attacker
→ cryptanalysis with limited number of encodings
- idea: "variable" vs "fixed" number of encodings

Thank you for your
attention