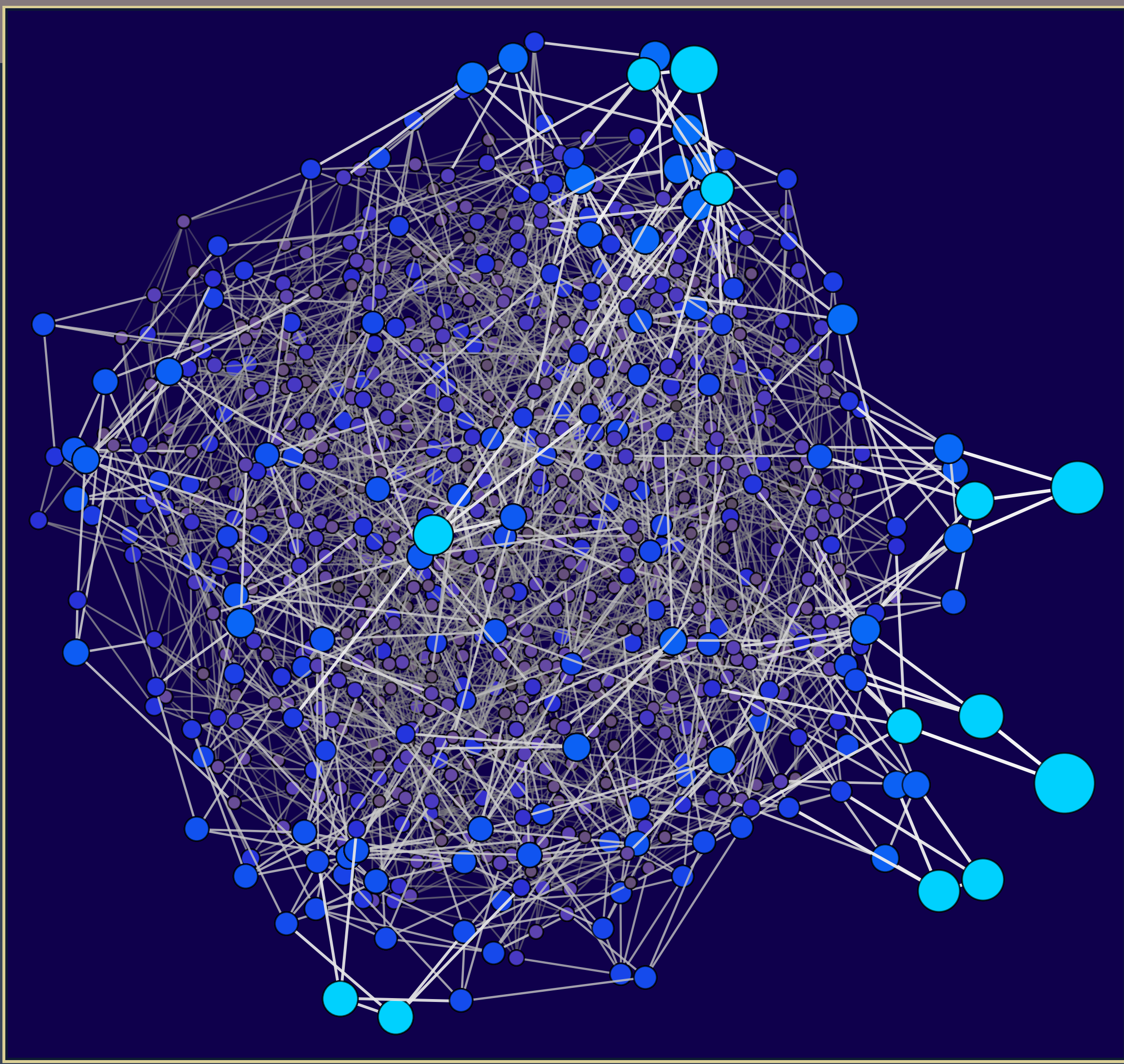
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Simultaneous diagonalization of incomplete matrices and applications

Jean-Sébastien Coron, Luca Notarnicola, and Gabor Wiese



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.127

Simultaneous diagonalization of incomplete matrices and applications

Jean-Sébastien Coron, Luca Notarnicola, and Gabor Wiese

We consider the problem of recovering the entries of diagonal matrices $\{U_a\}_a$ for $a = 1, \ldots, t$ from multiple "incomplete" samples $\{W_a\}_a$ of the form $W_a = PU_aQ$, where P and Q are unknown matrices of low rank. We devise practical algorithms for this problem depending on the ranks of P and Q. This problem finds its motivation in cryptanalysis: we show how to significantly improve previous algorithms for solving the approximate common divisor problem and breaking CLT13 cryptographic multilinear maps.

1. Introduction

1A. ***Problem statement.*** This work considers the following computational problem from linear algebra.

Definition 1.1 (Problems $\mathbb{A}$, $\mathbb{B}$, $\mathbb{C}$, $\mathbb{D}$). Let $n \geq 2$, $t \geq 2$ and $2 \leq p, q \leq n$ be integers. Let $\{U_a : 1 \leq a \leq t\}$ be diagonal matrices in $\mathbb{Q}^{n\times n}$. Let $\{W_a : 1 \leq a \leq t\}$ be matrices in $\mathbb{Q}^{p\times q}$ and $W_0 \in \mathbb{Q}^{p\times q}$ such that W_0 has full rank and there exist matrices $P \in \mathbb{Q}^{p\times n}$ of full rank p and $Q \in \mathbb{Q}^{n\times q}$ of full rank q, such that $W_0 = P \cdot Q$ and $W_a = P \cdot U_a \cdot Q$ for $1 \leq a \leq t$. We distinguish the following cases:

$$(\mathbb{A})\quad p = n \text{ and } q = n, \qquad (\mathbb{B})\quad p = n \text{ and } q < n,$$
$$(\mathbb{C})\quad p < n \text{ and } q = n, \qquad (\mathbb{D})\quad p < n \text{ and } q = p.$$

In each of the four cases, the problem is stated as follows:

(1) Given the matrices $\{W_a : 0 \leq a \leq t\}$, compute $\{(u_{1,i}, \ldots, u_{t,i}) : 1 \leq i \leq n\}$, where for $1 \leq a \leq t$, $u_{a,1}, \ldots, u_{a,n} \in \mathbb{Q}$ are the diagonal entries of matrices $\{U_a : 1 \leq a \leq t\}$ as above.

(2) Determine whether the solution is unique.

Problem $\mathbb{A}$ is straightforward for any $t \geq 1$ by simultaneous diagonalization of $W_0^{-1}W_a = Q^{-1}U_aQ$ for every a. Problems $\mathbb{B}$ and $\mathbb{C}$ are equivalent in view of their symmetry in p and q, and any algorithm for one solves the other upon transposing. Therefore, we shall devise algorithms for $\mathbb{C}$ and $\mathbb{D}$ only. We

MSC2010: 15A06, 94A60.
Keywords: simultaneous diagonalization, cryptanalysis, linear algebra, multilinear maps in cryptography, approximate common divisor problem.

refer to the matrices $\{W_a\}_a$ as "incomplete", as the low rank matrices P and/or Q "steal" information. Of interest is the case when p is much smaller than n. We remark that Problem $\mathbb{A}$ is an underlying problem in previous works [CP19; CHL$^+$15] in cryptanalysis.

1B. *Our contributions.* Mainly, we provide efficient algorithms for Problems $\mathbb{C}$ and $\mathbb{D}$ of Definition 1.1, and show how to minimize the parameters p and t with respect to n. We further propose two concrete applications of our algorithms in cryptography. We believe that our algorithms are of independent interest and hope that more applications are to be found.

Algorithms for Problems $\mathbb{C}$ *and* $\mathbb{D}$. Our approach to Problem $\mathbb{C}$ is to use the invertibility of Q and write $W_a = PU_aQ = PQQ^{-1}U_aQ = W_0Z_a$ with $Z_a = Q^{-1}U_aQ$, for every $1 \le a \le t$. As W_0 is not invertible, we cannot recover Z_a directly. However we interpret this as a system of linear equations to solve for $\{Z_a\}_a$. This system is, in general, underdetermined and does not yield the matrices $\{Z_a\}_a$ uniquely. However, exploiting the special feature that $\{Z_a\}_a$ commute among each other leads to additional linear equations. This enables us to recover $\{Z_a\}_a$ uniquely, and simultaneous diagonalization eventually yields the diagonal entries of $\{U_a\}_a$. We determine exact bounds on the parameters to ensure that we have at least as many linear equations as variables; we obtain that p and t can be set as $\mathcal{O}(\sqrt{n})$. Our algorithm is heuristic only, but performs well in practice.

We reduce Problem $\mathbb{D}$ to Problem $\mathbb{C}$ by "augmenting" Q with extra columns so that it becomes invertible. In this case, we show that p can be close to $2n/3$. We refer to Sections 3 and 4 for a complete description of our algorithms and provide the results of practical experiments in Section 6.

Improved algorithm for an approximate common divisor problem. Approximate common divisor problems have gained a lot of interest and different variants have been investigated. In [CH13], Cohn and Heninger study generalizations of the approximate common divisor problem via lattices. A simple version including only a single prime number is studied in [GGM16]. A lattice cryptanalysis of the single-prime version is described in [vDGHV10]. In this work we consider the multi-prime version (CRT-ACD Problem) from [CP19], which is a factorization problem with constraints based on Chinese remaindering.

We improve the two-step algorithm by [CP19]. Namely, we remark that [CP19] relies on solving a certain instance of Problem $\mathbb{A}$. By solving an appropriate instance of Problem $\mathbb{C}$ instead, we obtain a quadratic improvement in the number of input samples. Namely, letting n be the number of secret primes in the public modulus M, we can factor M given only $\mathcal{O}(\sqrt{n})$ input samples, whereas [CP19] uses $\mathcal{O}(n)$. We therefore achieve complete factorization of the public modulus while limiting the input size drastically.

Improved cryptanalysis of CLT13 multilinear maps. In 2013, [GGH13] described the first construction of cryptographic multilinear maps, and since then, many important applications in cryptography have been found. A similar construction over the integers was described in [CLT13] and a third construction based on the LWE Problem was proposed [GGH15]. In the recent years, many attacks against these constructions appeared. The most devastating is the so-called "zeroizing attack", exploiting the availability of low-level encodings of zero. The algorithm [CHL+15] recovers all secret parameters of [CLT13] in the multiparty Diffie–Hellman key exchange. Similar attacks have been described against GGH13 and GGH15; see [HJ16; CLLT16].

Our third contribution is therefore to improve the cryptanalysis of Cheon et al. [CHL+15] against CLT13 when fewer encodings are public. Namely, [CHL+15] relies on solving some instance of Problem $\mathbb{A}$. By solving instances of Problems $\mathbb{C}$ or $\mathbb{D}$ instead, we can lower the number of public encodings required for the cryptanalysis. Specifically, for a composite modulus x_0 of n primes, we obtain improved algorithms using only $\mathcal{O}(\sqrt{n})$ encodings of zero (compared to n in [CHL+15]), or in total $4n/3$ encodings (compared to $2n+2$ in [CHL+15]). We confirm our results with practical experiments in Section 6.

2. Notations and preliminary remarks

2A. *Notation.* For $n \in \mathbb{Z}_{\geq 1}$, let $[n]$ be the set $\{1, \ldots, n\}$. For a set R and $r, s \in \mathbb{Z}_{\geq 1}$, we let $R^{r\times s}$ be the set of $r \times s$ matrices with entries in R. For $A \in R^{r\times s}$ and $B \in R^{r\times s'}$, $[A|B] \in R^{r\times(s+s')}$ is the matrix obtained by concatenating the columns of A and B. We let 1_n be the identity matrix in dimension $n \in \mathbb{Z}_{\geq 1}$. For a set $\mathcal{S}$, its cardinality is denoted by $\#\mathcal{S}$.

2B. *Remarks about Definition 1.1.* (i) Let $\{W_a\}_a$ be as in Definition 1.1, $\pi \in \mathfrak{S}_n$ be a permutation with associated matrix $A_\pi \in \{0, 1\}^{n\times n}$ and D be any invertible diagonal $n \times n$ matrix. Then $P' = PDA_\pi$ and $Q' = A_\pi^{-1} D^{-1} Q$ satisfy $W_0 = P'Q'$ and $W_a = P'U'_a Q'$ for all $a \in [t]$, where $U'_a = A_\pi^{-1} U_a A_\pi$ is obtained from U_a by permuting its diagonal entries via π. Thus, P', $\{U'_a\}_a$ and Q' satisfy the same problem. For this reason, we only ask to recover the set $\{(u_{1,i}, \ldots, u_{t,i}) : 1 \leq i \leq n\}$ in Definition 1.1.

(ii) If $t = 1$ in Problem $\mathbb{C}$, then the problem is not solvable because its solution is not unique. Namely, we write $W_1 = W_0 Z_1$, where $Z_1 = Q^{-1} U_1 Q$ is diagonalizable with eigenvalues the diagonal entries of U_1. But also, for every $v \in \ker(W_0)$ one has $W_1 = W_0(Z_1 + vw_1^T)$ for some $w_1 \in \mathbb{Q}^n$. Now, Z_1 and $Z_1 + vw_1^T$ likely have different eigenvalues which means that the solution is not unique.

(iii) There are cases when the problem is clearly not solvable for $p < n$. For example, if $P = [1_p|0_{p\times(n-p)}]$ then for all a the matrix PU_a only involves the first p diagonal entries of U_a and the information on the remaining $n - p$ is lost. These cases will not occur for "generic" or "random" instances of the problem.

(iv) If a matrix $W_0 = PQ$ is not available as input (we call it a "special input" here), then one can recover ratios of diagonal entries of the matrices $\{U_a\}_a$, if $t \geq 3$. Namely, defining $P' = PU_1$ and assuming that U_1 is invertible, one obtains $W'_0 := P'Q = W_1$ and for $2 \leq a \leq t$, $W'_a := P'(U_a U_1^{-1})Q = W_a$. Running the algorithm on input $\{W'_a : 0 \leq a \leq t-1\}$ reveals the tuples of diagonal entries of the matrices $U_a U_1^{-1}$ for $1 \leq a \leq t-1$. We will use this approach in Section 5B3 to improve the (CLT13) multilinear map cryptanalysis.

(v) For simplicity, we have stated Definition 1.1 over $\mathbb{Q}$. More generally, we can consider matrices over a field $\mathbb{K}$ with exact linear algebra (e.g., solving linear systems, diagonalizing matrices, etc.). Our algorithms apply to that case.

3. An algorithm for Problem $\mathbb{C}$

We describe an algorithm to solve Problem $\mathbb{C}$ of Definition 1.1.

3A. ***Description.*** Consider integers $n, t \geq 2$ and $2 \leq p < n$ and an instance of Problem $\mathbb{C}$. We remark that it is enough to solve the following problem.

Definition 3.1 (Problem $\mathbb{C}'$). Let integers $n, t \geq 2$ and $2 \leq p < n$. Given

- a matrix $V \in \mathbb{Q}^{p\times n}$ of rank p and a basis matrix $E \in \mathbb{Q}^{n\times(n-p)}$ of $\ker(V)$,
- a set of matrices $\{Y_a : a \in [t]\} \subseteq \mathbb{Q}^{n\times n}$,

compute matrices $\{X_a : a \in [t]\} \subseteq \mathbb{Q}^{(n-p)\times n}$, such that the matrices $Y_a + EX_a$ for $a \in [t]$ commute with each other.

Proposition 3.2. *Let $\{W_a : 0 \leq a \leq t\}$ as in Problem $\mathbb{C}$. Let $E \in \mathbb{Q}^{n\times(n-p)}$ be a basis matrix of the kernel of W_0. Let W_0^+ be a right-inverse*[1] *of W_0. Define $V = W_0$ and $Y_a = W_0^+ W_a$ for $a \in [t]$. Assume that Problem $\mathbb{C}'$ is uniquely solvable for the input matrices V, E and $\{Y_a : a \in [t]\}$.*

Then Problem $\mathbb{C}$ is uniquely solvable for the input matrices $\{W_a : 0 \leq a \leq t\}$. Moreover, the matrix Q in the assumption of Problem $\mathbb{C}$ is unique up to multiplication by a permutation matrix and an invertible diagonal matrix if at least one of the matrices $\{U_a\}_a$ has pairwise distinct diagonal entries.

Proof. Write $W_0 = PQ$ and $W_a = PU_aQ$ as in Problem $\mathbb{C}$. For all $a \in [t]$, we will write $W_a = (PQ)(Q^{-1}U_aQ) = W_0Z_a$, where $Z_a := Q^{-1}U_aQ$. The matrices $\{Z_a : a \in [t]\}$ commute and are simultaneously diagonalizable. For every $a \in [t]$, Z_a can be written as $Z_a = Y_a + EX_a$ for some $X_a \in \mathbb{Q}^{(n-p)\times n}$ since $W_0Y_a = W_a$. Since the matrices $\{Z_a\}_a$ commute, V, E and $\{Y_a\}_a$ define a valid input for Problem $\mathbb{C}'$. By assumption, we can compute the matrices $\{X_a\}_a$ by solving Problem $\mathbb{C}'$ and these are unique. From the knowledge of $\{X_a\}_a$, we compute $Z_a = Y_a + EX_a$ for $a \in [t]$. Then these matrices are also unique. Thus the set of tuples of eigenvalues

$$\{(u_{1,i}, \ldots, u_{t,i}) : 1 \leq i \leq n\}$$

is unique and can be computed by simultaneous diagonalization.

For the last part of the statement, assume that we have matrices P', Q', diagonal matrices $\{U'_a\}_a$, which are necessarily of the form $U'_a = A^{-1}U_aA$ for a permutation matrix A, such that $W_0 = P'Q'$ and $W'_a = P'U'_aQ'$ for every a. By uniqueness of the matrices $\{Z_a\}_a$, we have

$$Z_a = Q^{-1}U_aQ = Q'^{-1}U'_aQ' = Q'^{-1}A^{-1}U_aAQ', \quad a \in [t]$$

or, equivalently $U_a(QQ'^{-1}A^{-1}) = (QQ'^{-1}A^{-1})U_a$ for $a \in [t]$. Thus, $D := QQ'^{-1}A^{-1}$ commutes with the matrices $\{U_a\}_a$ and so is diagonal itself, as one of $\{U_a\}_a$ has pairwise distinct entries. This gives $Q = DAQ'$ and proves the statement. $\square$

[1] If W_0 (of full rank p) is defined over the complex numbers, one can take $W_0^+ = W_0^*(W_0W_0^*)^{-1}$ where W_0^* is the conjugate transpose of W_0, and $W_0^* = W_0^T$ over the real numbers.

3A1. *Solving problem $\mathbb{C}'$.* We consider matrices $V, E, \{Y_a\}_a$ as in Problem $\mathbb{C}'$. We want to compute matrices $\{X_a\}_a$ such that the matrices $Z_a = Y_a + EX_a$ commute for all $a \in [t]$, that is, the Jacobi bracket $[Z_a, Z_b] = Z_aZ_b - Z_bZ_a$ is the zero matrix for all $a < b$. Using $Z_a = Y_a + EX_a$, this is equivalent to

$$0 = Y_aY_b - Y_bY_a + E \cdot S_{ab} + Y_aEX_b - Y_bEX_a, \tag{3-1}$$

where $S_{ab} := X_aY_b + X_aEX_b - X_bY_a - X_bEX_a$. Left multiplication by V and $VE = 0$ implies

$$VY_aY_b - VY_bY_a + VY_aEX_b - VY_bEX_a = 0,$$

which is equivalent to

$$\Delta_{ab} = VY_bEX_a - VY_aEX_b, \quad 1 \le a < b \le t, \tag{3-2}$$

where $\Delta_{ab} := VY_aY_b - VY_bY_a$ is completely explicit in terms of the input matrices. Equation (3-2) describes a system of linear equations over $\mathbb{Q}$ in the variables given by the entries of X_a and X_b. Since Δ_{ab} has size $p \times n$, this gives a system of np linear equations in the $2(n-p)n$ variables given by the entries of X_a and X_b. Writing (3-2) for every $(a, b) \in [t]^2$ with $a < b$ we obtain a system of $t(t-1)/2np$ linear equations and $t(n-p)n$ variables given by the entries of the matrices $\{X_a : a \in [t]\}$.

From this and Proposition 3.2, we deduce the following result.

Proposition 3.3. *A unique solution to Problem $\mathbb{C}$ is implied by the existence of a unique solution to the explicit system of linear equations given in* (3-2), *which is a system of $\frac{1}{2}t(t-1)np$ linear equations in $t(n-p)n$ variables. There are at least as many equations as variables as soon as*

$$\frac{p}{n} \ge \frac{2}{t+1}. \tag{3-3}$$

Since there is no obvious linear dependence in the equations of the system, we heuristically expect, in the generic case, to find a unique solution $\{X_a : a \in [t]\}$ under (3-3). This solves Problem $\mathbb{C}'$, and therefore Problem $\mathbb{C}$.

3B. ***Algorithm.*** We refer to this algorithm as Algorithm $\mathcal{A}_{\mathbb{C}}$ in the sequel.

Input: A valid input for Problem $\mathbb{C}$.

Output: “Success” or “Fail”. In case of “Success”, also output a solution. “Success” means uniqueness of the solution; “Fail” means that no solution was found.

1. Compute a basis matrix E of $\ker(W_0)$.
2. Define $W_0^+ = W_0^T(W_0W_0^T)^{-1}$ and for $(a, b) \in [t]^2$ with $a < b$, compute the matrices $\Delta_{ab} = W_aW_0^+W_b - W_bW_0^+W_a$.
3. Solve the system of linear equations described in (3-2).
   3.1. If the solution is not unique, output “Fail” and break.
   3.2. Otherwise, denote by $\{X_a : a \in [t]\}$ the unique solution.
4. Perform simultaneous diagonalization of $Z_a = W_0^+W_a + EX_a$ for $a \in [t]$.
5. Output “Success” with the tuples of eigenvalues of the matrices $\{Z_a\}_a$.

3C. ***Optimization of the parameters.*** We find minimal possible (with respect to n) values for t and p. In our applications in Section 5 we are led to minimize $p+t$ as a function of n. Following Proposition 3.3, we set $F_n(t) = p_n(t) + t = \frac{2n}{t+1} + t$ with $t \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}_{\geq 2}$. It is easy to see that F_n has a minimum at $t_0 = \sqrt{2n} - 1$ which gives $p = p_n(t_0) = \sqrt{2n}$. This shows that minimal values for p and t are $\mathcal{O}(\sqrt{n})$. This is confirmed practically in Section 6.

4. An algorithm for problem $\mathbb{D}$

We now present an algorithm to solve Problem $\mathbb{D}$ of Definition 1.1.

4A. ***Description.*** Consider integers $n, t \geq 2$ and $2 \leq p < n$ and an instance of Problem $\mathbb{D}$. The main idea of our algorithm is a reduction to Problem $\mathbb{C}$ which can be solved using Algorithm $\mathcal{A}_{\mathbb{C}}$. More precisely, we exhibit matrices (that are augmentations of $\{W_a\}_a$) $W'_0 = PQ'$ and $W'_a = PU_aQ'$ for $a \in [t]$, for the same diagonal matrices $\{U_a\}_a$ and for some $n \times n$ invertible matrix Q'.

4A1. *Reducing problem $\mathbb{D}$ to problem $\mathbb{C}$.* For $1 \leq a, b \leq t$, we define the matrices

$$\Delta_{ab} = W_a W_0^{-1} W_b - W_b W_0^{-1} W_a. \tag{4-1}$$

Note that $\Delta_{ab} = -\Delta_{ba}$. We have the following lemma.

Lemma 4.1. *Let $W_0 = PQ$ and $W_a = PU_aQ$ for $a \in [t]$ as in Problem $\mathbb{D}$. Let $B = QW_0^{-1}P - 1_n \in \mathbb{Q}^{n\times n}$ and let r denote its rank. Then*:

(i) $r = n - p$.

(ii) *There exist matrices $V_a \in \mathbb{Q}^{p\times r}$ and $G_a \in \mathbb{Q}^{r\times p}$ for $a \in [t]$ such that for all $1 \leq a < b \leq t$, one has $\Delta_{ab} = V_aG_b - V_bG_a$.*

Proof. (i) Let $C = QW_0^{-1}P$. Then $CQ = Q$ and the column-image of Q is contained in the eigenspace, say $\mathcal{E}$, of C for eigenvalue 1. So, $\mathcal{E}$ has dimension at least p. However, the rank of C is bounded above by the rank of Q, i.e., by p. Finally, $\mathcal{E}$ has dimension exactly p and the rank r of $B = C - 1_n$ equals $n - p$.

(ii) For every $1 \leq a, b \leq t$, we can write

$$\Delta_{ab} = PU_a(QW_0^{-1}P - 1_n)U_bQ - PU_b(QW_0^{-1}P - 1_n)U_aQ = PU_aBU_bQ - PU_bBU_aQ \tag{4-2}$$

since U_a and U_b commute. Since B has rank r, there exist matrices $B_1 \in \mathbb{Q}^{n\times r}$, $B_2 \in \mathbb{Q}^{r\times n}$ with $B = B_1B_2$. Setting $V_a = PU_aB_1$ and $G_a = B_2U_aQ$ gives the claim. □

The following properties of the matrix B defined in Lemma 4.1 are useful.

Lemma 4.2. *Let $W_0 = PQ$ and $W_a = PU_aQ$ for $a \in [t]$ as in Problem $\mathbb{D}$. Let $B \in \mathbb{Q}^{n\times n}$ be the matrix of Lemma 4.1 with respect to P and Q and let $r = n - p$. Let $B_1 \in \mathbb{Q}^{n\times r}$ and $B_2 \in \mathbb{Q}^{r\times n}$ be such that $B = B_1B_2$. Then*:

(i) $PB_1 = 0_{p\times r}$.

(ii) *The matrix $Q' := [Q|B_1]$ is an $n \times n$ invertible matrix.*

Proof. (i) The matrix B_2 defines a surjection $B_2 : \mathbb{Q}^n \to \mathbb{Q}^r$. Thus for every $x \in \mathbb{Q}^r$, we write $x = B_2 y$ for some $y \in \mathbb{Q}^n$ and obtain $PB_1 x = PB_1(B_2 y) = (PB)y = 0$.

(ii) Since $r = n - p$, Q' has size $n \times n$. To show its invertibility, we show that $\mathrm{im}(Q) \cap \mathrm{im}(B_1) = \{0\}$. Since B_2 is surjective, the images of B_1 and $B_1 B_2 = B$ coincide. Let $Qx = By \in \mathrm{im}(Q) \cap \mathrm{im}(B_1)$, with $x \in \mathbb{Q}^p$ and $y \in \mathbb{Q}^n$. This gives $Qx = (QW_0^{-1}P - 1_n)y = QW_0^{-1}Py - y$. Thus $y = QW_0^{-1}Py - Qx = Qz$ with $z = W_0^{-1}Py - x$. Therefore, $Qx = By = B(Qz) = 0$ because $BQ = 0$. □

We now show that finding matrices $\{V_a\}_a$ such that there exist $\{G_a\}_a$ satisfying $\Delta_{ab} = V_a G_b - V_b G_a$ for every a, b is sufficient to solve Problem $\mathbb{D}$. We view these matrices as being complementary to $\{W_a\}_a$ because they define themselves an instance of Problem $\mathbb{D}$ with the same solution as $\{W_a\}_a$ (see the proof of Lemma 4.1). This allows us to increase the rank of Q. We thus now formulate Problem $\mathbb{D}'$.

Definition 4.3 (Problem $\mathbb{D}'$). Let $n, t \geq 2$ and $2 \leq p < n$ be integers. For every $1 \leq a, b \leq t$, let $\Delta_{ab} \in \mathbb{Q}^{p \times p}$ be such that $\Delta_{ab} = V_a G_b - V_b G_a$ for $V_a \in \mathbb{Q}^{p \times (n-p)}$ of rank $n - p$ and $G_a \in \mathbb{Q}^{(n-p) \times p}$. The problem is as follows: Given the matrices Δ_{ab} for all $1 \leq a, b \leq t$, compute such matrices V_a for $a \in [t]$.

The following proposition links Problem $\mathbb{D}$ and Problem $\mathbb{C}$.

Proposition 4.4. *Let $W_0 = PQ$ and $W_a = PU_a Q$ for $a \in [t]$ be as in Problem $\mathbb{D}$. For $1 \leq a, b \leq t$, let Δ_{ab} be the matrices defined in* (4-1). *Moreover, assume that*:

(i) *Problem $\mathbb{D}'$ is uniquely solvable for the input matrices $\{\Delta_{ab} : 1 \leq a < b \leq t\}$ and denote the unique solution by $\{V_a : a \in [t]\}$.*

(ii) *Problem $\mathbb{C}$ is uniquely solvable for the input matrices $W_0' = [W_0 | 0_{p \times (n-p)}] \in \mathbb{Q}^{p \times n}$ and $W_a' = [W_a | V_a] \in \mathbb{Q}^{p \times n}$ for $a \in [t]$.*

Then Problem $\mathbb{D}$ is uniquely solvable on input $\{W_a : 0 \leq a \leq t\}$ and the unique solution is given by the unique solution to Problem $\mathbb{C}$ on input $\{W_a' : 0 \leq a \leq t\}$.

Proof. By Lemma 4.1 there exist $V_a \in \mathbb{Q}^{p \times r}$ and $G_a \in \mathbb{Q}^{r \times p}$ for $a \in [t]$ such that $\Delta_{ab} = V_a G_b - V_b G_a$ for all $1 \leq a < b \leq t$. Therefore the matrices $\{\Delta_{ab}\}_{a,b}$ define an instance of Problem $\mathbb{D}'$. By Proposition 4.4(i), we compute the unique solution $\{V_a\}_a$ for this problem.

Now, let $W_0' = [W_0 | 0_{p \times (n-p)}] \in \mathbb{Q}^{p \times n}$ and $W_a' = [W_a | V_a] \in \mathbb{Q}^{p \times n}$ for $a \in [t]$. Let $B = QW_0^{-1}P - 1_n$ as in Lemma 4.1 of rank $r = n - p$. Let $B_1 \in \mathbb{Q}^{n \times r}$ and $B_2 \in \mathbb{Q}^{r \times n}$ be a rank factorization of B; i.e., $B = B_1 B_2$. Letting $Q' := [Q | B_1] \in \mathbb{Q}^{n \times n}$, we have $PQ' = P[Q | B_1] = [W_0 | 0_{p \times r}] = W_0'$ and, by uniqueness of $\{V_a\}_a$ (see proof of Lemma 4.1),

$$PU_a Q' = PU_a [Q | B_1] = [W_a | V_a] = W_a'$$

for $a \in [t]$, as $PB_1 = 0_{n \times r}$ by Lemma 4.2(i). The matrix Q' is invertible by Lemma 4.2(ii). Therefore, W_0' and $\{W_a'\}_a$ define a valid input for Problem $\mathbb{C}$. By Proposition 4.4(ii), this problem is uniquely solvable and the solution must be the tuples of diagonal entries of the matrices $\{U_a\}_a$. This is also a solution to Problem $\mathbb{D}$ since the matrices $\{U_a\}_a$ are the same for the input matrices $\{W_a\}_a$ for Problem $\mathbb{D}$ and $\{W_a'\}_a$ for Problem $\mathbb{C}$. □

4A2. *Solving problem* $\mathbb{D}'$. In view of Proposition 4.4, it remains to compute matrices $\{V_a\}_a$ from $\{\Delta_{ab}\}_{a,b}$. We achieve this by standard linear algebra, and combining with Algorithm $\mathcal{A}_{\mathbb{C}}$ describes a full algorithm for Problem $\mathbb{D}$.

From now on we assume $t \geq 3$. Let $\Delta_{ab} = V_a G_b - V_b G_a$ for $1 \leq a, b \leq t$ as in Problem $\mathbb{D}'$. Let $r = n - p$ and r_{ab} be the rank of Δ_{ab}; clearly, $r_{ab} \leq \min(2r, p)$. We further assume $p > 2n/3$ (equivalently, $2r < p$), which is a necessary condition as otherwise the matrices Δ_{ab} likely have full rank and thus cannot reveal any information. We define $\mathcal{K}_{ab} := \operatorname{im}(\Delta_{ab}) = \mathcal{K}_{ba} \subseteq \mathbb{Q}^p$ and

$$\mathcal{K}_a = \bigcap_{b\in[t],b\neq a} \mathcal{K}_{ab},\ a \in [t].$$

Let $\mathcal{V}_a$ be the image of the matrix V_a for $a \in [t]$. We first argue that, heuristically, $\mathcal{V}_a \subseteq \mathcal{K}_{ab}$ for every $b \neq a$. Let $v \in \mathcal{V}_a$. If there exists $x \in \mathbb{Q}^p$ such that $v = V_a G_b x$ and $V_b G_a x = 0$ then $v = \Delta_{ab} x$, i.e., $v \in \mathcal{K}_{ab}$. Such an element x must therefore lie in $(x_0 + \ker(V_a G_b)) \cap \ker(V_b G_a)$, where $x_0 \in \mathbb{Q}^p$ is any vector such that $v = V_a G_b x_0$. It is easy to see that this intersection is nonempty if $\ker(V_a G_b) + \ker(V_b G_a) = \mathbb{Q}^p$. Heuristically, as $\{V_a\}_a$ have rank r, $\ker(V_a G_b) + \ker(V_b G_a)$ has dimension at least $2(p-r)$; accordingly we can heuristically expect that $\ker(V_a G_b) + \ker(V_b G_a) = \mathbb{Q}^p$ as soon as $2(p-r) > p$, i.e., $p > 2n/3$.

We now justify that, heuristically under a suitable parameter selection, $\mathcal{K}_a = \mathcal{V}_a$ for every $a \in [t]$. For fixed $a \in [t]$, we compute $\mathcal{K}_a$ modulo $\mathcal{V}_a$ and consider $\overline{\mathcal{K}_{ab}} := \mathcal{K}_{ab}/\mathcal{V}_a \subseteq \mathbb{Q}^{p-r}$ for $b \neq a$. Then $\mathcal{K}_a = \mathcal{V}_a$ if and only if $\overline{\mathcal{K}_a} := \bigcap_{b\neq a} \overline{\mathcal{K}_{ab}} = \{0\}$. Since $\mathcal{V}_a$ has dimension r, $\overline{\mathcal{K}_{ab}}$ has dimension $r_{ab} - r$. For every $b \neq a$, we view $\overline{\mathcal{K}_{ab}}$ as the kernel of $\mathbb{Q}^{p-r} \to \mathbb{Q}^{p-r}/\overline{\mathcal{K}_{ab}}$, represented by a matrix $A_{ab} \in \mathbb{Q}^{(p-r_{ab})\times(p-r)}$. Therefore $\overline{\mathcal{K}_a}$ is represented by an augmented matrix $A_a = [A_{a1}|\cdots|A_{a,a-1}|A_{a,a+1}|\cdots|A_{at}]$ describing the kernel of $\mathbb{Q}^{p-r} \to \bigoplus_{b\neq a} \mathbb{Q}^{p-r}/\overline{\mathcal{K}_{ab}}$. The matrix A_a has $\sum_{b\in[t],b\neq a}(p - r_{ab})$ rows and $p - r$ columns. Now, $\mathcal{K}_a = \mathcal{V}_a$ if and only if A_a has full rank; and heuristically, we expect this to be the case as soon as $\sum_{b\in[t],b\neq a}(p - r_{ab}) \geq p - r$.

Remark 4.5. (i) In fact, we expect that $r_{ab} = 2r$ for every a, b. Then, from what precedes, we expect, heuristically that $\mathcal{K}_a = \mathcal{V}_a$ for every a, if $(t-1)(p-2r) \geq p - r$, i.e.,

$$\frac{p}{n} \geq \frac{2t-3}{3t-5} \quad \text{or, equivalently,} \quad t \geq \frac{2p-n}{3p-2n} + 1. \tag{4-3}$$

(ii) We assumed $t \geq 3$ so that the intersections $\{\mathcal{K}_a\}_a$ are well-defined. If $t = 2$, $\mathcal{K}_1$ coincides with the image of Δ_{12}, which will not reveal V_1 and V_2.

We compute bases of $\{\mathcal{K}_a\}_a$ by standard linear algebra. For the rest of this section, assume $\mathcal{K}_a = \mathcal{V}_a$ for every a, and let C_a be a basis matrix for $\mathcal{K}_a$. Thus, there exists $M_a \in \mathrm{GL}_r(\mathbb{Q})$ such that $V_a = C_a M_a$. This gives for $a < b$:

$$\Delta_{ab} = V_a G_b - V_b G_a = C_a(M_a G_b) - C_b(M_b G_a) = C_a N_{ab} - C_b N_{ba} \tag{4-4}$$

with $N_{ab} = M_a G_b$. In (4-4), Δ_{ab} and C_a, C_b are known, which allows us to compute $N^{(ab)} = [N_{ab}|N_{ba}]^T$ as a solution to $\Delta_{ab} = [C_a| - C_b] \cdot N^{(ab)}$. Once the $\{N_{ab}\}_{a,b}$ are computed, we obtain a system of linear equations over $\mathbb{Q}$, given by

$$M_a^{-1} \cdot N_{ab} = G_b, \quad 1 \leq a < b \leq t. \tag{4-5}$$

It has $\frac{1}{2}t(t-1)rp$ equations (there are $\frac{1}{2}t(t-1)$ choices for pairs (a, b) and for each pair the matrix equality gives rp equations) and $tr^2 + trp = trn$ variables, given by the tr^2 entries of the matrices $\{M_a^{-1} : a \in [t]\}$ and the trp entries of the matrices $\{G_b : b \in [t]\}$. Heuristically, if $trn \leq \frac{1}{2}t(t-1)rp$, i.e., $2n \leq (t-1)p$, the system is expected to have a unique solution. This bound is automatically satisfied if (4-3) holds. This reveals $\{M_a : a \in [t]\}$ and thus $\{V_a : a \in [t]\}$ by computing $V_a = C_a M_a$.

Proposition 4.6. *Assume that $\mathcal{K}_a = \mathcal{V}_a$ for every $a \in [t]$ (see Remark 4.5(i)). Then, a unique solution to Problem $\mathbb{D}'$ is implied by the existence of a unique solution to the explicit system of linear equations given in (4-5), which is a system of $\frac{1}{2}t(t-1)(n-p)p$ linear equations in $t(n-p)n$ variables. There are at least as many equations as variables as soon as $p(t-1) \geq 2n$.*

4B. ***Algorithm.*** We refer to this algorithm as Algorithm $\mathcal{A}_{\mathbb{D}}$ in the sequel.

Input: A valid input for Problem $\mathbb{D}$.

Output: "Success" or "Fail", and in case of "Success", additionally output a solution. "Success" means that the computed solution is unique; "Fail" means that a solution was not found.

1. Compute $\Delta_{ab} = W_a W_0^{-1} W_b - W_b W_0^{-1} W_a$ for $1 \leq a \neq b \leq t$.
2. For $a \in [t]$, compute a basis matrix C_a of $\mathcal{K}_a := \bigcap_{b \in [t], b \neq a} \operatorname{im}(\Delta_{ab})$.
3. Check whether $\dim(\mathcal{K}_a) \neq n - p$ for all $a \in [t]$.
   - 3.1 If true, output "Fail" and break.
   - 3.2 Otherwise, for every $a < b$ compute N_{ab} as solutions to $\Delta_{ab} = [C_a | -C_b] \cdot [N_{ab} | N_{ba}]^T$.
4. Solve for $\{M_a\}_a$ the system of linear equations $M_a^{-1} N_{ab} = G_b$ for $(a, b) \in [t]^2, a < b$.
   - 4.1. If a unique solution is not found, output "Fail" and break.
5. Compute the matrices $\{V_a : a \in [t]\}$ as $V_a = C_a \cdot M_a$.
6. Run Algorithm $\mathcal{A}_{\mathbb{C}}$ on the matrices $W_0' = [W_0 | 0]$ and $W_a' = [W_a | V_a]$ for $a \in [t]$ and return its output.

Remark 4.7. Problem $\mathbb{D}$ of Definition 1.1 is symmetric in the sense that P and Q have the same rank. An asymmetric variant consists in having P and Q of ranks $p \neq q$. Our algorithm adapts to that case: if $p < q$, then "cutting" the last $q - p$ columns of $\{W_a\}_a$ means "cutting" the last $q - p$ columns of Q, which reduces to the symmetric case. This approach is however not very genuine, as it "cuts" information instead of possibly exploiting it. We leave it open to find a better algorithm.

4C. ***Optimization of the parameters.*** We find minimal possible values for t and p with respect to a given n. In Section 5B1 we will see that it is of interest to minimize $2p + t$ in order to minimize the number of public encodings in [CLT13]. According to (4-3), the main (heuristic) condition to be ensured is $p \geq \frac{2t-3}{3t-5}n$. We set $F_n(t) = 2p_n(t) + t = \frac{2t-3}{3t-5}n + t$ for $t \in \mathbb{R}_{>0} \backslash \left\{\frac{5}{3}\right\}$ and $n \geq 2$. Then F_n has a minimum at $t_0 = \frac{1}{3}(\sqrt{2n}+5)$, with $p_n(t_0) = \frac{2}{3}n + \frac{1}{3\sqrt{2}}\sqrt{n}$ and $F_n(t_0) = \frac{4}{3}n + \frac{2}{3}\sqrt{2n} + \frac{5}{3}$. In conclusion, we expect Algorithm $\mathcal{A}_{\mathbb{D}}$ to succeed for $p = \lceil p_n(t_0)\rceil$ and $t = \lceil t_0 \rceil$.

5. Applications

We describe two applications for our algorithms and obtain significant improvements on previous works.

5A. ***Improved algorithm for the CRT-ACD Problem.*** We consider the following "multi-prime" version of the approximate common divisor problem [CP19] based on Chinese remaindering:

Definition 5.1 (CRT-ACD problem). Let $n, \eta, \rho \in \mathbb{Z}_{\geq 1}$. Let $p_1, \dots, p_n$ be distinct η-bit prime numbers and $M = \prod_{i=1}^n p_i$. Consider a nonempty finite set $\mathcal{S}$ of integers in $\mathbb{Z} \cap [0, M)$ such that for every $x \in \mathcal{S}$,

$$x \equiv x_i \pmod{p_i}, \quad 1 \leq i \leq n,$$

for uniformly distributed integers $x_i \in \mathbb{Z}$ satisfying $|x_i| \leq 2^\rho$.

The CRT-ACD problem is stated as follows: given the set $\mathcal{S}$, the integers η, ρ and M factor M completely (i.e., find the prime numbers $p_1, \dots, p_n$).

Clearly, the larger the set $\mathcal{S}$, the more information one can exploit to factor M. Our interest is therefore to minimize the cardinality of the set $\mathcal{S}$ with respect to n.

5A1. *The algorithm of* [CP19]. Coron and Pereira propose an algorithm for the case $\#\mathcal{S} = n+1$. They proceed in two steps called the "orthogonal lattice attack" following [NS99] and the "algebraic attack" following [CHL+15]. We briefly review their algorithm; for a complete description we refer to [CP19, Section 4.3].

Let $\mathcal{S} = \{x_1, \dots, x_n, y\}$ and $x = (x_1, \dots, x_n) \in \mathcal{S}^n$. Then, the vector $b = (x, y \cdot x) \in \mathbb{Z}^{2n}$ is public, and by the Chinese remainder theorem, letting $x \equiv x^{(i)} \pmod{p_i}$ and $y \equiv y^{(i)} \pmod{p_i}$ for all $i \in [n]$, one has $b \equiv \sum_{i=1}^n c_i(x^{(i)}, y^{(i)}x^{(i)}) =: \sum_{i=1}^n c_i b^{(i)} \pmod{M}$, for some integers $c_1, \dots, c_n$. If the vectors $\{x^{(i)}\}_i$ are $\mathbb{R}$-linearly independent, then so are $\{b^{(i)}\}_i$ and they generate a $2n$-dimensional lattice $\mathcal{L}$ of rank n. Importantly, by Definition 5.1, the vectors $\{b^{(i)}\}_i$ are reasonably short vectors (of ℓ_2-norm approximately $2^{2\rho}$; and ρ is considered much smaller than η).

The "orthogonal lattice attack" is an algorithm, which on input b, outputs a basis of the completion $\overline{\mathcal{L}} = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Q}$ of $\mathcal{L}$, performing lattice reduction on the lattice $\langle b \rangle^{\perp_M}$ of vectors $v \in \mathbb{Z}^m$ such that $\langle v, b\rangle \equiv 0 \pmod{M}$. The parameters are chosen accordingly, and one essentially requires $2\rho < \eta$.

Upon finding a basis $\{b'^{(i)}\}_i$ of $\overline{\mathcal{L}}$, Coron and Pereira proceed with the "algebraic attack". The bases $\{b'^{(i)}\}_i$ of $\overline{\mathcal{L}}$ and $\{b^{(i)}\}_i$ of $\mathcal{L}$ are related via an unknown invertible base change matrix $Q \in \mathbb{Q}^{n\times n}$. Letting $P = [x^{(1)}|\cdots|x^{(n)}] \in \mathbb{Z}^{n\times n}$ with columns $\{x^{(i)}\}_i$, one obtains matrix relations

$$W_0 = P \cdot Q, \; W_1 = P \cdot U_1 \cdot Q, \tag{5-1}$$

where U_1 is $n \times n$ diagonal with entries $\{y^{(i)}\}_i$. The matrix W_0 is invertible (over $\mathbb{Q}$) and one computes the eigenvalues $\{y^{(i)}\}_i$ of $W_1 W_0^{-1} = PU_1P^{-1}$. Using $y \equiv y^{(i)} \pmod{p_i}$, one factors M by computing greatest common divisors.

5A2. *A naive improvement.* There is a naive generalization of [CP19] using only $\mathcal{O}(\sqrt{n})$ public instances in $\mathcal{S}$. However, we argue that this approach gives a worse range of parameters when combined with [CP19].

For integers $p \geq 2$ and $t \geq 1$ of size $\mathcal{O}(\sqrt{n})$, let $x = (y_1 \cdot z, \ldots, y_t \cdot z) \in \mathbb{Z}^{tp}$ of dimension $\mathcal{O}(n)$ for $y_1, \ldots, y_t \in \mathcal{S}$ and $z \in \mathcal{S}^p$. This variant reduces $\#\mathcal{S}$ considerably, as $\#\mathcal{S} = p + t = \mathcal{O}(\sqrt{n})$. However, [CP19] requires one to construct the vector $b = (x, y \cdot x)$ for $y \in \mathcal{S}$. This gives rise to residue vectors $\{b^{(i)}\}_i$ of approximate ℓ_2-norm $2^{3\rho}$ instead of $2^{2\rho}$ as in [CP19]. Therefore the stronger condition $3\rho < \eta$ will be required for the orthogonal lattice attack to succeed. In our improvement, we would like to lower $\#\mathcal{S}$ while continuing to use $2\rho < \eta$, as in [CP19].

5A3. *Our improved algorithm.* We recognize that (5-1) defines an instance of Problem $\mathbb{A}$ of Definition 1.1 with $t = 1$ because P and Q have rank n. Our improvement lies in generalizing the vector b to obtain an instance of Problem $\mathbb{C}$.

We consider $\#\mathcal{S} < n+1$ and write for convenience $\mathcal{S} = \{x_1, \ldots, x_p, y_1, \ldots, y_t\}$ with integers $2 \leq p < n$ and $2 \leq t < n$ satisfying $2n \leq (t+1)p$. We let $x = (x_1, \ldots, x_p) \in \mathcal{S}^p$ and $b = (x, y_1 \cdot x, \ldots, y_t \cdot x) \in \mathbb{Z}^{(t+1)p}$. As before, let $\{b^{(i)}\}_i$ denote the short residue vectors modulo the primes $\{p_i\}_i$ and $x \equiv x^{(i)} \pmod{p_i}$, $y_a \equiv y_a^{(i)} \pmod{p_i}$ for $a \in [t]$ and $i \in [n]$. By the Chinese remainder theorem, we observe that b lies in the lattice $\mathcal{L} = \bigoplus_{i=1}^n \mathbb{Z}b^{(i)}$ modulo M. Namely, there are integers $c_1, \ldots, c_n$ such that

$$b \equiv \sum_{i=1}^{n} c_i \begin{bmatrix} x^{(i)} \\ y_1^{(i)} \cdot x^{(i)} \\ \vdots \\ y_t^{(i)} \cdot x^{(i)} \end{bmatrix} =: \sum_{i=1}^{n} c_i b^{(i)} \pmod{M}.$$

As in [CP19], the orthogonal lattice algorithm reveals a basis $\{b'^{(i)}\}_i$ of $\overline{\mathcal{L}}$ and the ℓ_2-norm of $\{b^{(i)}\}_i$ is still approximately 2ρ.

Contrary to (5-1), we now derive matrix equations

$$W_0 = P \cdot Q,\ W_a = P \cdot U_a \cdot Q,\ a \in [t], \tag{5-2}$$

where $P \in \mathbb{Z}^{p \times n}$ has columns $\{x^{(i)}\}_i$ and $\{U_a\}_a$ are $n \times n$ diagonal with entries $\{y_a^{(i)}\}_{a,i}$. The matrix Q is a base change matrix from $\{b'^{(i)}\}_i$ to $\{b^{(i)}\}_i$. If W_0 has rank p, (5-2) now defines a valid input for Problem $\mathbb{C}$ of Definition 1.1 and Algorithm $\mathcal{A}_{\mathbb{C}}$ from Section 3 reveals the diagonal entries $\{y_a^{(i)}\}_{a,i}$ of the matrices $\{U_a\}_a$. One can then factor M by computing $\gcd(y_a - y_a^{(i)}, M)$.

From Section 3C we see that $\#\mathcal{S} = p + t$ is minimized for $p = \lceil\sqrt{2n}\rceil$ and $t + 1 = \lceil\sqrt{2n}\rceil$. Thus, $\#\mathcal{S} = 2\lceil\sqrt{2n}\rceil = \mathcal{O}(\sqrt{n})$. In summary, letting n be the number of secret primes in the public modulus M, we can factor M given only $\mathcal{O}(\sqrt{n})$ input samples, whereas [CP19] uses $\mathcal{O}(n)$.

Remark 5.2. We remark that we do not impact the security of the key-exchange from [CP19], as it uses certain encodings of matrices. However, the product of matrices does not commute, so our techniques do not apply to that case.

5B. ***Improved cryptanalysis of CLT13 multilinear maps.*** We consider now the CLT13 multilinear map scheme by Coron et al., [CLT13]. Cheon et al. [CHL$^+$15] described a polynomial-time attack against the Diffie–Hellman key exchange based on CLT13 when enough encodings of zero are public. Such encodings are for instance public in the rerandomization procedure. It is of interest to investigate this cryptanalysis when only a limited number of such encodings is available. Namely, not every CLT13-based construction necessarily reveals enough such encodings and the attack of Cheon et al. is prevented.

5B1. *CLT13 multilinear maps.* The CLT13 multilinear map is a construction over the integers based on the notion of graded encoding scheme [GGH13]. Its hardness relies on Chinese remainder representations and factorization. We fix an integer $n \geq 2$, thought of as a dimension for CLT13. The message space is $\bigoplus_{i=1}^{n} \mathbb{Z}/g_i\mathbb{Z}$ for some small secret primes $\{g_i\}_i$. The encoding space has a graded structure and supports homomorphic addition and multiplication. It is defined over $\bigoplus_{i=1}^{n} \mathbb{Z}/p_i\mathbb{Z}$ for large secret primes $\{p_i\}_i$ with public product $x_0 = \prod_i p_i$. More precisely, an encoding of a message $m = (m_i)_i \in \bigoplus_{i=1}^{n} \mathbb{Z}/g_i\mathbb{Z}$ at level $k \in [\kappa]$ (where κ denotes the multilinearity degree) is an integer c such that

$$c \equiv (r_i g_i + m_i) \cdot z^{-k} \pmod{p_i}$$

for all $i \in [n]$ where $z \in (\mathbb{Z}/x_0\mathbb{Z})^\times$ and r_i is a random "small" noise. By the Chinese remainder theorem, c is computed modulo x_0. For encodings c at the last level κ, a public zero-testing procedure allows one to test if c encodes zero. This procedure works by computing $\omega(c) := p_{zt} \cdot c$ for a public parameter $p_{zt} \in \mathbb{Z}/x_0\mathbb{Z}$. Then c encodes the zero message if ω is "small" compared to x_0. In [CLT13], one actually defines a vector of n zero-test parameters $\{p_{zt,i} : i \in [n]\}$ to define a proper zero-testing. For the precise parameter setting, we refer to [CLT13, Section 3.1].

5B2. *Cryptanalysis.* The algorithm from [CHL$^+$15] reveals all secret parameters given sufficiently many encodings of zero. We briefly recall the attack here, and for simplicity of exposition, assume $\kappa = 3$. Consider sets $\mathcal{A} = \{\alpha_j : j \in [n]\}$, $\mathcal{B} = \{\beta_1, \beta_2\}$ and $\mathcal{C} = \{\gamma_k : k \in [n]\}$ of encodings at level 1 and where all encodings in $\mathcal{A}$ encode zero. Therefore, there are $\#\mathcal{A} = n$ public encodings of zero and $\#(\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}) = 2n + 2$ encodings in total. In the previous notation, we write $\alpha_j \equiv \alpha_{ji}/z \pmod{p_i}$, $\beta_a \equiv \beta_{ai}/z \pmod{p_i}$ and $\gamma_k \equiv \gamma_{ki}/z \pmod{p_i}$ for all $i, j, k \in [n]$ and $a \in [2]$. Because the products $\alpha_j \beta_a \gamma_k$ encode zero at level 3, correct zero-testing ensures that the zero-test equations $\omega_{jk}^{(a)} = p_{zt}(\alpha_j \beta_a \gamma_k)$, given by

$$\omega_{jk}^{(a)} = \sum_{i=1}^{n} p_{zt,i} \alpha_{ji} \beta_{ai} \gamma_{ki} = \begin{bmatrix} \alpha_{j1} \cdots \alpha_{jn} \end{bmatrix} \begin{bmatrix} \beta_{a1} p_{zt,1} & & \\ & \ddots & \\ & & \beta_{an} p_{zt,n} \end{bmatrix} \begin{bmatrix} \gamma_{k1} \\ \vdots \\ \gamma_{kn} \end{bmatrix}$$

for certain explicit integers $p_{zt,i}$ for $i \in [n]$ defining the zero-test parameter, hold over $\mathbb{Z}$ instead of $\mathbb{Z}/x_0\mathbb{Z}$. Writing these relations out for all indices $(j, k) \in [n]^2$, the $n \times n$ matrices $W_a := (\omega_{jk}^{(a)})_{j,k \in [n]}$ for $a = 1, 2$ satisfy

$$W_a = P \cdot U_a \cdot Q \tag{5-3}$$

for secret matrices P, Q of full rank n (corresponding to encodings of $\mathcal{A}$ and $\mathcal{C}$, respectively) and diagonal matrices $\{U_a\}_a$ containing the elements $\{\beta_{ai} : i \in [n]\}$. If at least one of W_1, W_2 is invertible over $\mathbb{Q}$ (say, W_2), the attacker computes the eigenvalues $\{\beta_{1i}/\beta_{2i} : i \in [n]\}$ of $W_1 W_2^{-1}$. These ratios are enough to factor x_0. Indeed, letting $\beta_{1i}/\beta_{2i} = x_i/y_i$ for coprime integers x_i, y_i and using $\beta_a \equiv \beta_{ai}/z \pmod{p_i}$, we deduce $x_i\beta_2 - y_i\beta_1 \equiv (x_i\beta_{2i} - y_i\beta_{1i})/z \equiv 0 \pmod{p_i}$ for $i \in [n]$ and therefore $\gcd(x_i\beta_2 - y_i\beta_1, x_0) = p_i$ with high probability.

In summary, the Cheon et al. attack recovers all secret primes $\{p_i\}_i$ in polynomial time given the set $\mathcal{A}$ of level-one encodings of zero and the sets $\mathcal{B}$ and $\mathcal{C}$.

5B3. *Attacking CLT13 with fewer encodings.* We consider the following CLT13-based problem.

Definition 5.3 (CLT13 problem). Let $n \geq 2$ be the dimension of CLT13 and $x_0 = \prod_{i=1}^n p_i$. Let $\mathcal{E}$ be a finite nonempty set of encodings at level 1 and $\mathcal{E}_0 \subseteq \mathcal{E}$ a nonempty subset such that every element of $\mathcal{E}_0$ is an encoding of zero. The CLT13 problem is as follows: Given the sets $\mathcal{E}$ and $\mathcal{E}_0$, factor x_0.

We refer to $\mathcal{E}$ and $\mathcal{E}_0$ as the sets of "available encodings" and "available encodings of zero", respectively. It is not a loss of generality to consider level-one encodings. As in [CHL+15], we write $\mathcal{E} = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ with $\mathcal{A} \subseteq \mathcal{E}_0$. As recalled above, [CHL+15] requires $\#\mathcal{E}_0 \geq n$ to factor x_0, and a total number of public encodings $\#\mathcal{E} = 2n + 2$.

We aim at reducing the number of encodings needed for the factorization of x_0 and treat the following questions independently:

(i) Factor x_0 with fewer available encodings of zero, i.e., $\#\mathcal{E}_0 < n$.

(ii) Factor x_0 with fewer available encodings, i.e., $\#\mathcal{E} < 2n + 2$.

A naive improvement. As for the CRT-ACD problem, there is a naive improvement using fewer encodings, but assuming $\kappa = 4$. One can form product encodings $\alpha_j\beta_a\gamma_k\delta_\ell$ at level 4, where every encoding is at level 1. These can be partitioned into sets $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ such that $\mathcal{A}$ corresponds to encodings of zero with $\#\mathcal{A} = \mathcal{O}(\sqrt{n})$. However, this approach has the inconvenience of using $\kappa = 4$ and our improved attack aims at lowering the number of public encodings while $\kappa = 3$.

Minimizing the number of encodings of zero. We explain how to use Algorithm $\mathcal{A}_{\mathbb{C}}$ to factor x_0 using only $\#\mathcal{E}_0 = \mathcal{O}(\sqrt{n})$ level-one encodings of zero.

We fix integers $2 \leq p < n$ and $3 \leq t < n$ and assume again $\kappa = 3$. As in [CHL+15], we write $\mathcal{E} = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ with $\mathcal{A} \subseteq \mathcal{E}_0$. We let $\#\mathcal{A} = p$, $\#\mathcal{B} = t$ and $\#\mathcal{C} = n$; and claim $p = \mathcal{O}(\sqrt{n})$.

Every product encoding $c = \alpha_j\beta_a\gamma_k$ with $(\alpha_j, \beta_a, \gamma_k) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$ is an encoding of zero and by correct zero-testing we obtain integer matrix relations

$$W_a = P \cdot U_a \cdot Q, \quad a \in [t], \tag{5-4}$$

for $P \in \mathbb{Z}^{p\times n}$, $Q \in \mathbb{Z}^{n\times n}$ corresponding to encodings in $\mathcal{A}$ and $\mathcal{C}$, respectively, and diagonal matrices $\{U_a\}_a$ corresponding to $\mathcal{B}$. Exactly as in [CHL+15], the matrices $\{U_a\}_a$ contain integers β_{ai} such that $\beta_a \equiv \beta_{ai} \pmod{p_i}$ for $i \in [n]$. With high probability the ranks of P and Q are p and n, respectively. Defining $W'_0 = W_1$ and $W'_a = W_{a-1}$ for $2 \leq a \leq t$ we obtain an instance similar to Problem $\mathbb{C}$ of

Definition 1.1, but without a "special input matrix" PQ (see Section 2B). Using Algorithm $\mathcal{A}_{\mathbb{C}}$, we reveal eigenvalues (the diagonal entries) of the matrices $\{U_a U_1^{-1}\}_a$ as it is likely that U_1 will be invertible. We finally deduce the prime factorization of x_0 by taking greatest common divisors, as in [CHL+15].

By the optimization in Section 3C, we choose $t = \lceil \sqrt{2n} \rceil$ and $\#\mathcal{A} = p = \lceil \sqrt{2n} \rceil$.

Minimizing the total number of encodings. We now explain how to use Algorithm $\mathcal{A}_{\mathbb{D}}$ to factor x_0 using $\#\mathcal{E} = \frac{4}{3}n + \mathcal{O}(\sqrt{n})$ instead of $\#\mathcal{E} = 2n + 2$ as in [CHL+15].

Contrary to the previous case, we now use a set $\mathcal{C}$ with $\#\mathcal{C} = p$; so $\#\mathcal{E} = 2p + t$. It is now straightforward to see that upon correct zero-testing we derive equations as in (5-4) but with $Q \in \mathbb{Z}^{n \times p}$ instead. Thus, if both P and Q have rank p, we obtain Problem $\mathbb{D}$ of Definition 1.1 without "special input matrix" W_0. Then Algorithm $\mathcal{A}_{\mathbb{D}}$ reveals ratios of diagonal entries of $\{U_a U_1^{-1}\}$ and we consequently factor x_0.

Following Section 4C, we are led to minimize $\#\mathcal{E}(n) = 2p + t$ as a function of n. We can let $p = \left\lceil \frac{2}{3}n + \frac{1}{3\sqrt{2}}\sqrt{n} \right\rceil$ and $t = \left\lceil \frac{1}{3}\sqrt{2n} + \frac{5}{3} \right\rceil$ and obtain

$$\#\mathcal{E}(n) = 2\left\lceil \frac{2}{3}n + \frac{1}{3\sqrt{2}}\sqrt{n} \right\rceil + \left\lceil \frac{1}{3}\sqrt{2n} + \frac{5}{3} \right\rceil = \frac{4}{3}n + \mathcal{O}(\sqrt{n}).$$

Cryptanalysis with independent slots. In [CN19], Coron and Notarnicola cryptanalyze CLT13 when no encodings of zero are available beforehand, but instead only "partial-zero" encodings. Messages are nonzero modulo a product of several primes $g_1 \cdots g_\theta$ for some integer $\theta \in [n]$. We can improve this cryptanalysis following the same techniques as above. Let ℓ the number of partial-zero encodings. Since [CN19] is based on the algorithm of Cheon et al. to factor x_0, we can now replace it by Algorithm $\mathcal{A}_{\mathbb{C}}$ once ℓ encodings of zero are created. This means that we can set $\ell = \mathcal{O}(\sqrt{n})$, which brings a twofold improvement: first, lattice reduction (in the orthogonal lattice attack [CN19, Section 4]) is only run on a lattice of dimension $\mathcal{O}(\sqrt{n})$; and second, the number of partial-zero encodings is reduced to $\mathcal{O}(\sqrt{n})$.

6. Computational aspects and practical results

We describe practical parameters for algorithms $\mathcal{A}_{\mathbb{C}}$ and $\mathcal{A}_{\mathbb{D}}$. We have implemented our algorithms in SageMath: our source code is provided in https://pastebin.com/Yg6QgZTh. Our experiments are done on a standard Intel Core i7 3.3 GHz processor.

6A. ***Instance generation of problems*** $\mathbb{C}$ ***and*** $\mathbb{D}$**.** As for applications in cryptanalysis, we consider matrices with integer entries. To generate instances of Problems $\mathbb{C}$ and $\mathbb{D}$, given fixed integers n, t, p, we uniformly at random generate matrices P, Q and $\{U_a\}_a$ with entries in $[-k, k] \cap \mathbb{Z}$ for some $k \in \mathbb{Z}_{\geq 1}$ as in Definition 1.1. Setting $W_0 = PQ$ and $W_a = PU_aQ$ for $a \in [t]$ gives instances of Problems $\mathbb{C}$ or $\mathbb{D}$.

We perform the linear algebra over $\mathbb{Z}/\ell\mathbb{Z}$ for a large prime ℓ, instead of over $\mathbb{Q}$. It suffices to choose ℓ slightly larger than the diagonal entries of $\{U_a\}_a$ (e.g., $\ell = \mathcal{O}(\max_{a,i} |u_{ai}|)$, where u_{ai} for $i \in [n]$ denote the diagonal entries of U_a). The running time depends on the entry size of the generated matrices. The overall computational cost of our algorithms $\mathcal{A}_{\mathbb{C}}$ and $\mathcal{A}_{\mathbb{D}}$ is dominated by the cost of solving systems of linear equations and performing simultaneous diagonalization, which can be done by standard algorithms for nonsparse linear algebra.

		Algorithm $\mathcal{A}_{\mathbb{C}}$					Algorithm $\mathcal{A}_{\mathbb{D}}$				
n	entry size	practice p	practice t	theory $p_0(n)$	theory $t_0(n)$	running time	practice p	practice t	theory $p_0(n)$	theory $t_0(n)$	running time
15	1000	6	4	6	5	4 min 4 s	11	4	11	4	4 min 2 s
25	750	8	7	8	7	3 min 45 s	18	4	18	5	1 min 54 s
50	600	10	9	10	9	4 min 34 s	35	5	35	5	1 min 39 s
100	200	15	14	15	14	1 h 17 min	70	7	70	7	5 min 14 s
150	100	18	16	18	17	6 h 29 min	103	8	103	8	23 min 14 s
500	20	32	31	32	31	29 min 3 s	339	13	339	13	6 min 57 s

Table 1. Experimental data for Algorithms $\mathcal{A}_{\mathbb{C}}$ and $\mathcal{A}_{\mathbb{D}}$.

6B. ***Practical experiments.*** We gather in Table 1 practical parameters for problems $\mathbb{C}$ and $\mathbb{D}$, and our applications of Section 5. We compare p, t with the theoretical values $p_0(n), t_0(n)$ obtained in the two algorithms. For Section 3, $p_0(n) = \lceil\sqrt{2n}\rceil$ and $t_0(n) = \lceil\sqrt{2n}-1\rceil$. For Section 4, $p_0(n) = \left\lceil \frac{2}{3}n + \frac{\sqrt{n}}{3\sqrt{2}} \right\rceil$ and $t_0(n) = \left\lceil \frac{1}{3}(\sqrt{2n}+5) \right\rceil$. Here "entry size" is an approximation of the bit-size of the max-norm of each input matrix.

Our work is compared with [CP19] for the CRT-ACD problem in Table 2 and with [CHL$^+$15] for the cryptanalysis of CLT13 in Table 3. We give parameters for obtaining a complete factorization of M (in CRT-ACD) and x_0 (in CLT13) of approximate bit-size $n\eta$. For CRT-ACD, the column "this work" equals $\#\mathcal{S} = p+t$ (Series 1). For CLT13, "this work" shows $\#\mathcal{E} = 2p+t$ (Series 2) and $\#\mathcal{E}_0 = p$ (Series 3). Thus, for $n = 50$, our algorithm factors M (in CRT-ACD) using only 19 public samples, whereas [CP19] requires 51 samples; and similarly breaks CLT13 with only 10 public encodings of zero, while [CHL$^+$15] uses 50.

In conclusion, these practical experiments overall confirm our theory, as well as the quadratic improvement over [CP19] and [CHL$^+$15].

Series 1					num. of samples	
n	η	ρ	p	t	this work	[CP19]
20	1000	200	7	6	13	21
30	1000	100	8	7	15	31
50	800	100	10	9	19	51

Table 2. Experimental data for the CRT-ACD problem.

			Series 2		num. of encodings		Series 3		num. of encodings of zero	
n	η	ρ	p	t	this work	[CHL$^+$15]	p	t	this work	[CHL$^+$15]
20	1000	200	15	4	34	42	7	6	7	20
30	1000	100	22	5	49	62	8	7	8	30
50	800	100	35	5	75	102	10	9	10	50

Table 3. Experimental data for the CLT13 Problem.

Acknowledgments

We thank the anonymous reviewers of ANTS-XIV for their helpful comments. Notarnicola acknowledges support by the Luxembourg National Research Fund through grant PRIDE15/10621687/-SPsquared.

References

[CH13] Henry Cohn and Nadia Heninger, *Approximate common divisors via lattices*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium (Berkeley, CA) (Everett W. Howe and Kiran S. Kedlaya., eds.), Open Book Ser., no. 1, Math. Sci. Publ., 2013, pp. 271–293. MR 3207418

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé, *Cryptanalysis of the multilinear map over the integers*, Advances in cryptology—EUROCRYPT 2015, I, Lecture Notes in Comput. Sci., no. 9056, Springer, 2015, pp. 3–12. MR 3344918

[CLLT16] Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi, *Cryptanalysis of GGH15 multilinear maps*, Advances in cryptology—CRYPTO 2016, II, Lecture Notes in Comput. Sci., no. 9815, Springer, 2016, pp. 607–628. MR 3565321

[CLT13] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi, *Practical multilinear maps over the integers*, Advances in cryptology—CRYPTO 2013, I (Ran Canetti and Juan A. Garay, eds.), Lecture Notes in Comput. Sci., no. 8042, Springer, 2013, pp. 476–493. MR 3126439

[CN19] Jean-Sébastien Coron and Luca Notarnicola, *Cryptanalysis of CLT13 multilinear maps with independent slots*, Advances in Cryptology—ASIACRYPT 2019, II, no. 11922, Springer, 2019, pp. 356–385.

[CP19] Jean-Sébastien Coron and Hilder V. L. Pereira, *On Kilian's randomization of multilinear map encodings*, Advances in Cryptology—ASIACRYPT 2019, II, vol. 11922, Springer, 2019, pp. 325–355.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi, *Candidate multilinear maps from ideal lattices*, Advances in cryptology—EUROCRYPT, 2013 (Thomas Johansson and Phong Q. Nguyen, eds.), Lecture Notes in Comput. Sci., no. 7881, Springer, 2013, pp. 1–17. MR 3095515

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi, *Graph-induced multilinear maps from lattices*, Theory of cryptography, II (Yevgeniy Dodis and Jesper Buus Nielsen, eds.), Lecture Notes in Comput. Sci., no. 9015, Springer, 2015, pp. 498–527. MR 3354209

[GGM16] Steven D. Galbraith, Shishay W. Gebregiyorgis, and Sean Murphy, *Algorithms for the approximate common divisor problem*, LMS J. Comput. Math. **19** (2016), 58–72, suppl. A. MR 3540946

[HJ16] Yupu Hu and Huiwen Jia, *Cryptanalysis of GGH map*, Advances in cryptology—EUROCRYPT 2016, I, Lecture Notes in Comput. Sci., no. 9665, Springer, 2016, pp. 537–565. MR 3516383

[NS99] Phong Nguyen and Jacques Stern, *The hardness of the hidden subset sum problem and its cryptographic implications*, Advances in cryptology—CRYPTO 1999, Lecture Notes in Comput. Sci., no. 1666, Springer, 1999, pp. 31–46. MR 1729292

[vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan, *Fully homomorphic encryption over the integers*, Advances in cryptology—EUROCRYPT 2010, Lecture Notes in Comput. Sci., no. 6110, Springer, 2010, pp. 24–43. MR 2660481

Received 27 Feb 2020.

JEAN-SÉBASTIEN CORON: jean-sebastien.coron@uni.lu
Faculté des Sciences, de la Technologie et de la Communication, University of Luxembourg, Esch-sur-Alzette, Luxembourg

LUCA NOTARNICOLA: luca.notarnicola@uni.lu
Faculté des Sciences, de la Technologie et de la Communication, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

GABOR WIESE: gabor.wiese@uni.lu
Faculté des Sciences, de la Technologie et de la Communication, University of Luxembourg, Esch-sur-Alzette, Luxembourg

msp

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand

https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

---

msp

MATHEMATICAL SCIENCES PUBLISHERS

798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840

contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS