A Practical Approach to the Secure Computation of the Moore–Penrose Pseudoinverse over the Rationals

Niek J. Bouman[*] Niels de Vreede[†]

Technische Universiteit Eindhoven
the Netherlands
{n.j.bouman,n.d.vreede}@tue.nl

May 8, 2019

Abstract

We devise an efficient and *data-oblivious* algorithm for solving a bounded integral linear system of arbitrary rank over the rational numbers via the Moore–Penrose pseudoinverse, using finite-field arithmetic. This particular problem setting stems from our goal to run the algorithm as a secure multiparty computation (MPC). Beyond MPC, our algorithm could be valuable in other scenarios, like secure enclaves in CPUs, where data-obliviousness is crucial for protecting secrets.

We compute the Moore–Penrose inverse over a finite field of sufficiently large order, so that we can recover the rational solution from the solution over the finite field.

Previous work by Cramer, Kiltz and Padró (*CRYPTO 2007*) proposes a constant-rounds protocol for computing the Moore–Penrose pseudoinverse over a finite field. The asymptotic complexity (counted as the number of secure multiplications) of their solution is $O(m^4 + n^2 m)$, where m and n, $m \leq n$, are the dimensions of the linear system.

To reduce the number of secure multiplications, we sacrifice the constant-rounds property and propose a protocol for computing the Moore–Penrose pseudoinverse over the rational numbers in a linear number of rounds, requiring only $O(m^2 n)$ secure multiplications.

To obtain the common denominator of the pseudoinverse, required for constructing an integer-representation of the pseudoinverse, we generalize a result by Ben-Israel for computing the squared volume of a matrix. Also, we show how to precondition a symmetric matrix to achieve generic rank profile while preserving symmetry and being able to remove the preconditioner after it has served its purpose. These results may be of independent interest.

[*] supported by H2020-EU SODA

[†] supported by H2020-EU PRIViLEDGE

1 Introduction

Motivated by the goal of performing elementary statistical tasks such as linear regression *securely*, we revisit the topic of secure linear algebra. In this paper, "securely" refers to *secure multiparty computation* (MPC) [CDN15], however, our results might be of use in other settings as well, for example, for mitigating certain side-channel attacks in trusted execution environments in CPUs.

Secure linear algebra goes back to the work of Cramer and Damgård [CD01], who proposed constant-rounds MPC protocols for various basic tasks in linear algebra. In that paper, as well as in later papers in the same line of work, like [NW06, KMWF07, CKP07, MW08], the focus is on linear algebra *over a finite field.*

Our goal is to obtain, in an "MPC-friendly" way, an (approximate) solution to a linear system *over the real numbers.* In this paper we choose to approximate real arithmetic by (exact) rational arithmetic, or, in fact, integer arithmetic, using appropriate scaling. Our main reason behind this choice is the close connection between the finite field $\mathbb{Z}/p\mathbb{Z}$ and integer arithmetic, since we target MPC schemes that offer finite-field arithmetic. Hence, the protocols that we propose in this paper will employ finite-field arithmetic *as a tool, rather than as a goal.* We note that there are various papers targeting the same problem that explore other choices, such as secure fixed-point arithmetic (see, e.g., [NWI$^+$13, GSB$^+$17]) or secure floating-point arithmetic (e.g., [BKLS18]).

In an earlier joint work with Blom and Schoenmakers [BBSdV19], we focused on the case of solving full-rank systems; in this paper we deal with the unknown-rank case. Also, we would like to obtain meaningful solutions in case the system is over- or underdetermined. The *Moore–Penrose pseudoinverse* gives natural solutions in both cases: in the overdetermined case, which is the relevant case for linear regression, it yields the least-squares solution; in the underdetermined case it gives the minimum-norm solution.

Concretely, given a matrix A with integral elements of arbitrary rank, we propose a protocol for computing the Moore–Penrose pseudoinverse over the rational numbers in a linear number of rounds. The computational complexity, counted as the number of secure multiplications, is $O(m^2n)$, where m and n, $m \leq n$, are the dimensions of the system. In multiplicative-linear-secret-sharing-based MPC schemes, such as Shamir's scheme, we may count a secure inner product as a single secure multiplication; in that case the complexity reduces to $O(mn)$.

It should be rather easy to implement our protocol in any finite-field-based arithmetic secret-sharing MPC framework; beyond elementary finite-field arithmetic our protocol merely requires secure subprotocols for sampling (public) random elements, performing a zero test on a secret-shared field element, computing the reciprocal of a secret-shared field element, and computing the determinant of an invertible secret-shared matrix.

$$\begin{tikzcd}
A \in \mathbb{Z}^{m\times n} \arrow[r, "\operatorname{mod} p"] \arrow[d, "\pi"] & \tilde{A} \in \mathbb{F}_p^{m\times n} \arrow[d, "\text{Pseudoinverse}"] \\
A^\dagger \in \mathbb{Q}^{n\times m} \arrow[d, "d"] & \tilde{A}^\dagger \in \mathbb{F}_p^{n\times m} \arrow[d, "d"] \\
dA^\dagger \in \mathbb{Z}^{n\times m} & d\tilde{A}^\dagger \in \mathbb{F}_p^{n\times m} \arrow[l, "\mathrm{id}"']
\end{tikzcd}$$

(a) Our approach. The map d represents scalar multiplication by $d = (\operatorname{vol} A)^2$ and id represents the identity map. The solutions $dA^\dagger$ and $d\tilde{A}^\dagger$ coincide, provided that p is chosen large enough, i.e., according to the theorem in Section 4.2.

$$\begin{tikzcd}
A \in \mathbb{Z}^{m\times n} \arrow[r, "\operatorname{mod} q"] \arrow[d, "\pi"] & \tilde{A} \in \mathbb{F}_q^{m\times n} \arrow[d, "\text{Pseudoinverse}"] \\
A^\dagger \in \mathbb{Q}^{n\times m} & \tilde{A}^\dagger \in \mathbb{F}_q^{n\times m} \arrow[l, "\nu"']
\end{tikzcd}$$

(b) Approach using rational reconstruction [Wan81]. The map ν represents the elementwise rational reconstruction procedure. All reconstructed fractions will be in lowest terms (numerator and denominator have no common nontrivial factors). There is, however, a price to be paid, in that $q \geq 2p^2$. Also, the map ν (the Euclidean algorithm) is not "MPC-friendly".

Figure 1: Comparison between our approach and the approach via rational reconstruction. In the diagrams, the map $\pi : \mathbb{Q}^{m\times n} \to \mathbb{Q}^{n\times m}, A \mapsto A^\dagger$ applies the Moore–Penrose inverse over the rationals.

Circumventing Rational Reconstruction. In [BBSdV19], a key trick for obtaining the inverse of an invertible integer matrix B over the rational numbers from the corresponding inverse over the finite field $\mathbb{Z}/p\mathbb{Z}$ *without requiring rational reconstruction* [Wan81], was to form the integer-valued *adjugate matrix* by multiplying B^{-1} by $\det B$. In a similar spirit, we compute the pseudoinverse $A^\dagger$ over the finite field $\mathbb{Z}/p\mathbb{Z}$ and identify the conditions under which it corresponds to the pseudoinverse over the rational numbers. Essentially, this comes down to choosing p sufficiently large; see Section 4.2. We can then obtain an integer representation of the pseudoinverse by forming the pair $(dA^\dagger, d)$, where $dA^\dagger$ is an integer matrix containing the numerators of the pseudoinverse and d is the common denominator of the pseudoinverse, which coincides with the squared *volume* of A [BI92], which we write as $(\operatorname{vol} A)^2$. Figure 1 illustrates our approach and compares it to the alternative route of rational reconstruction.

Although taking the square of the volume is rather excessive in certain cases (for example, the magnitude of the common denominator of B^{-1}, for any *invertible* matrix B, equals $|\det B| = \operatorname{vol} B$), it is essentially the price we have to pay for not knowing whether we are dealing with such a special case.

Computing the Pseudoinverse and Its Common Denominator. To compute the Moore–Penrose pseudoinverse of A obliviously, we first compute a *reflexive generalized inverse* of the symmetric product $AA^\mathsf{T}AA^\mathsf{T}$ by means of block-recursive elimination. We then compute the Moore–Penrose pseudoinverse from this generalized inverse.

Regarding the common denominator, Springer computes $(\operatorname{vol} A)^2$ via an integer-preserving rank decomposition [Spr83]. To circumvent the need for constructing such a rank decomposition, we seek a simpler alternative. Ben-Israel gives a method for computing $(\operatorname{vol} A)^2$ that requires an orthonormal basis for the left nullspace of A [BI92]. Although an *orthonormal* basis might not even exist over a finite field, we can easily construct a matrix K whose columns span the left nullspace of A. We generalize Ben-Israel's result so that we can compute $(\operatorname{vol} A)^2$ from A and K.

Preconditioning for Computing Pseudoinverses. As noted above, we will compute the Moore–Penrose inverse via a generalized inverse that is obtained using block-recursive elimination.

Deterministic elimination algorithms typically employ pivoting to avoid problems like division by zero. Pivoting involves searching for and applying suitable row and/or column swaps prior to each elimination step. In secure computation, however, we aim to avoid pivoting because searching for particular elements and applying data-dependent row and column swaps, *obliviously*, is expensive (in a computational- and round-complexity sense).

An MPC-friendly alternative is to transform the matrix to be eliminated into an equivalent matrix for which the elimination procedure will succeed *without any pivoting*; this approach is called *preconditioning*. In case of Gaussian elimination, for example, the condition of *generic rank profile*[1] guarantees that pivoting can be omitted. As we prove in this paper, generic rank profile is also a sufficient condition for correctness of the particular block-recursive elimination algorithm that we use.

When dealing with a square, full rank matrix B over a finite field $\mathbb{F}$ with large order, one way to achieve generic rank profile with high probability is by pre-multiplying B by a preconditioner matrix R that is chosen uniformly at random from the set of all invertible matrices having the same size as B. When computing the inverse of RB, we can apply the rule $(RB)^{-1} = B^{-1}R^{-1}$, which we will refer to as the *reverse order law* for matrix inversion, to show that the inverse of the preconditioner can easily be removed by post-multiplying by R. For a matrix A with arbitrary rank r, pre-multiplying by a randomly chosen invertible matrix R (of appropriate size) is not sufficient for achieving generic rank profile; we additionally need to mix A's columns by multiplying A by a preconditioner matrix from the right.

A major problem that arises when trying to remove a preconditioner when computing the pseudoinverse, is that the reverse order law for pseudoinverses does not hold in general [Gre66, Har86]. In particular, unfortunately, we have

[1] A matrix A of rank r has *generic rank profile* if and only if all upper-left square submatrices of A up to dimension $r \times r$ are invertible.

that $(LAR)^\dagger$ does not necessarily equal $R^\dagger A^\dagger L^\dagger$ for invertible preconditioner matrices L and R. Hence, we cannot simply extract $A^\dagger$ from $(LAR)^\dagger$ like we could do above for B^{-1}. We circumvent this problem by removing the preconditioner immediately after computing the reflexive generalized inverse, for which the reverse-order law does hold.

An additional constraint in our setting is that the preconditioner should preserve symmetry, since the symmetry property enables significant computational savings during elimination. A preconditioner for this particular scenario seems to be lacking in the literature. We resolve this by proving that the preconditioner $A \mapsto UAU^\intercal$ for a uniformly random matrix U fulfills all our constraints.

Interestingly, and unlike Gaussian elimination, when working over the real or complex numbers, the particular block-recursive algorithm that we use for computing the reflexive generalized inverse does not even require its input to have generic rank profile, hence no preconditioning is needed in this case. Nonetheless, in fields with positive characteristic, the condition emerges from the phenomenon of self-orthogonality.

1.1 Related Work

Cramer, Kiltz and Padró [CKP07] propose a constant-rounds protocol for securely computing the Moore–Penrose pseudoinverse over a finite field. Their approach is to first compute the characteristic polynomial of the Gram matrix $A^\intercal A$, from which they then compute the rank of A (via a technique by Mulmuley [Mul87]) as well as the pseudoinverse of A (via the Cayley–Hamilton theorem).

An important theme in [CKP07] is to ensure that A (and $A^\intercal$) are *suitable*, which guarantees, informally speaking, that certain subspaces that are orthogonal over a field with characteristic zero, remain orthogonal over fields with positive characteristic. In our work, where we focus on the setting where the modulus (hence the field's characteristic) is chosen sufficiently large, existence of the pseudoinverse is guaranteed by a result in [BRP90]. (We state this result in the next section.) Nonetheless, as described in the previous section, we do take special precautions, namely, applying preconditioning, to avoid problems related to working over a field with positive characteristic when computing a reflexive generalized inverse.

For an $m \times n$ matrix where $m \leq n$, the complexity (number of secure multiplications) of Cramer et al.'s solution is $O(m^4 + n^2 m)$. Our solution, albeit not constant-rounds, has complexity $O(m^2 n)$, and even $O(mn)$ when assuming availability of a "cheap inner product", where the hidden constants in the Big-Oh of our solution are single-digit integers. By "cheap inner product", we mean that an inner product between two vectors of the same but arbitrary length has the same communication and round complexity as a single secure multiplication. It is possible to perform multiplication of an $m \times \ell$ matrix by an $\ell \times n$ matrix using no more than mn "cheap inner products". Because the coefficients of the result matrix may all be mutually independent, it is reasonable to take the complexity of such a matrix product to be equal to mn.

We leave it to further research to compare the practical performance of our method to that of [CKP07] in various application scenarios (i.e., various matrix-dimension regimes, network latency, bounded computational resources and storage space, etc.).

Relation to the LEU Decomposition. An earlier work by the authors [BdV18] proposes to use Malaschonok's *LEU* decomposition [Mal10] for solving linear systems of arbitrary rank in the context of secure computation. (Note that [BdV18] does not deal with the problem of computing the Moore–Penrose pseudoinverse.) Our new protocol Pseudoinverse is superior to the *LEU*-decomposition-based protocol; in terms of round complexity, $O(m)$ versus $O(m^{1.59})$, as well as in terms of the asymptotic computational complexity, $O(m^2)$ versus $O(m^2 \log m)$ secure inner products for a square $m \times m$ matrix.

2 Preliminaries

Secret Sharing and Secure Computation. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We use $\mathbb{F}$ to denote an arbitrary field. We assume the use of an MPC protocol based on arithmetic secret-sharing over $\mathbb{F}_p$. Our protocols will inherit the security properties (passive vs. active) from the underlying MPC protocol and of the subprotocols invoked by our protocol. The notation $[\![x]\!]$ represents an element $x \in \mathbb{F}_p$ that is secret-shared among the parties in the MPC protocol. Notation for secure arithmetic then follows naturally, for example, $[\![c]\!] \leftarrow [\![a]\!] + [\![b]\!]$ describes the addition of a and b where the result is stored in a new secret-shared element c, and $[\![d]\!] \leftarrow [\![a]\!][\![b]\!]$ describes an invocation of the multiplication protocol to securely compute the product of a and b and store the result in d. For arbitrary integer matrices A and B, the notation $[\![A]\!]$ expresses that all elements of A are secret-shared over $\mathbb{F}_p$, and $[\![A]\!] + [\![B]\!]$ and $[\![A]\!][\![B]\!]$ represent secure matrix addition (which coincides with elementwise addition) and secure matrix multiplication, respectively. Our protocols assume the availability of subprotocols for securely inverting a field element (see [BIB89]), for securely sampling private as well as public random field elements (e.g., [CDI05]), denoted as $[\![a]\!] \overset{\$}{\leftarrow} \mathbb{F}_p$ and $a \overset{\$}{\leftarrow} \mathbb{F}_p$ respectively, and for performing a secure zero test [DFK$^+$06, NO07]. The latter is denoted as protocol IsZero, which returns $[\![1]\!]$ if its argument equals zero and returns $[\![0]\!]$ otherwise.

Generalized Inverses. A *generalized inverse* of a matrix A is a matrix X associated to A that exists for a class of matrices larger than the class of invertible matrices, shares some properties with the ordinary inverse, and reduces to the ordinary inverse when A is non-singular. In this paper, we classify generalized inverses using the following four properties, also known as the *Penrose equations*:

$$(1)\, AXA = A, \quad (2)\, XAX = X, \quad (3)\, (AX)^{\mathsf{T}} = AX, \quad (4)\, (XA)^{\mathsf{T}} = XA.$$

The matrix X that satisfies all four Penrose equations for a given matrix A is called the *Moore–Penrose pseudoinverse*, or simply *pseudoinverse* of A, which we denote as $A^{\dagger}$. The Moore–Penrose inverse of A over $\mathbb{F}$ exists if and only if $\operatorname{rank}(AA^{\mathsf{T}}) = \operatorname{rank}(A^{\mathsf{T}}A) = \operatorname{rank} A$ [Pea68, Thm 1], and if it exists it is unique. We will also focus on generalized inverses of A which only satisfy equations (1) and (2); such generalized inverses are called *reflexive generalized inverses* and we denote any reflexive generalized inverse of A by A^{-}. Note that reflexive generalized inverses are not necessarily unique. For an extensive treatment of generalized inverses, the reader is referred to [BIG03].

For a square matrix A partitioned as

$$A = \begin{pmatrix} E & F \\ G & H \end{pmatrix} \tag{5}$$

such that E is square, A/E denotes the *generalized Schur complement*

$$A/E = H - GE^{-}F.$$

Submatrices, Their Determinants and Rank Properties. For any $n \in \mathbb{N}$, we write $[n]$ for the set $\{1, \ldots, n\}$. For any $m \times n$ matrix A and index sets $\mathcal{I} \subset [m]$ and $\mathcal{J} \subset [n]$, $[A]_{\mathcal{I},\mathcal{J}}$ denotes the determinant of the submatrix of A obtained by selecting all rows in $\mathcal{I}$ and all columns in $\mathcal{J}$. Furthermore, $A_{[k]}$ denotes the leading principal submatrix of order k, and we use $[A]_k$ a shorthand for $[A]_{[k],[k]}$, i.e., the leading principal minor or order k. Thus, it holds that $\det A_{[k]} \;=\; [A]_k$.

Let A be a matrix of rank r. We say that a matrix A has *generic rank profile* [KL96] if for all $k \in [r]$, it holds that A's leading principal minor of order k is nonzero.

Let A be partitioned as in (5). If $\det E \neq 0$, then *Schur's determinant formula* asserts that

$$\det A = \det(E)\det(A/E) = \det(E)\det(H - GE^{-1}F).$$

A direct consequence of [MS74a, Thm 19] is that

$$\operatorname{rank} A \geq \operatorname{rank} E + \operatorname{rank}(A/E).$$

Hence, if A has generic rank profile and E has at least dimension $r \times r$ where $r = \operatorname{rank} A$, then A/E is the null matrix.

The Volume of a Matrix. For any matrix A with rank r and nonzero singular values $\sigma_1, \ldots, \sigma_r$, its *volume* is defined as $\operatorname{vol} A = \prod_{i=1}^{r} \sigma_i$. Note that this definition implies that we define the volume of the zero matrix to be one, which will be convenient for our purpose but deviates from Ben-Israel's definition of matrix volume for this special case [BI92]. A matrix over an integral domain has a pseudoinverse if and only if its squared volume is a unit (i.e., an invertible element) of the integral domain [BRP90]. The fact that, for any matrix $A \in \mathbb{R}^{m \times n}$, the singular values of AA^{T} are the squares of the singular values of A leads to the following equation:

$$\operatorname{vol}(AA^{\mathsf{T}}) = (\operatorname{vol} A)^2, \tag{6}$$

which holds over an arbitrary field. In case A is a square nonsingular matrix, i.e., $m = n$ and $\det A \neq 0$, its volume coincides with the absolute value of its determinant:

$$\operatorname{vol} A = |\det A|. \tag{7}$$

Combining the two preceding equations gives

$$(\operatorname{vol} A)^2 = \det(AA^{\mathsf{T}}), \tag{8}$$

in the case that $\operatorname{rank} A = m$.

3 Block-Recursive Elimination

In this section we present ObliviousRGInverse, our oblivious protocol for computing a reflexive generalized inverse of any symmetric matrix over $\mathbb{F}_p$ that has generic rank profile. First, we define the *extended reciprocal* of an element $c \in \mathbb{F}$ as zero if $c = 0$ and c^{-1}, i.e., the (ordinary) reciprocal, otherwise. Note that the reflexive generalized inverse of a 1×1 matrix is equal to the 1×1 matrix containing the extended reciprocal of its only coefficient. ScalarRGInverse is a secure protocol for computing the extended reciprocal.

Protocol 1 ScalarRGInverse($[\![a]\!]$)

```
$[\![z]\!] \leftarrow$ IsZero($[\![a]\!]$)
**return** $[\![a + z]\!]^{-1} - [\![z]\!]$
```

ObliviousRGInverse is given as Protocol 2. On line 4, the partitioning is done such that E and G are square and their dimensions differ by at most one. We remark that the side notes with label "symmetric" in ObliviousRGInverse indicate that the resulting matrix is symmetric, which is to be exploited in an implementation.

It is easy to see that protocol ObliviousRGInverse is oblivious: it only branches on the dimensions of the matrix, which are considered public, and otherwise only performs elementary arithmetic operations, and calls to secure subprotocols (including recursive calls to itself).

Protocol 2 $\mathsf{ObliviousRGInverse}(\llbracket A \rrbracket)$

```
if $n = 1$ then
    return $\mathsf{ScalarRGInverse}(\llbracket a_{1,1} \rrbracket)$
else
    $\begin{pmatrix} \llbracket E \rrbracket & \llbracket F \rrbracket \\ \llbracket F^\mathsf{T} \rrbracket & \llbracket G \rrbracket \end{pmatrix} \leftarrow \llbracket A \rrbracket$        ▷ split as evenly as possible
    $\llbracket X \rrbracket \leftarrow \mathsf{ObliviousRGInverse}(\llbracket E \rrbracket)$
    $\llbracket XF \rrbracket \leftarrow \llbracket X \rrbracket \llbracket F \rrbracket$
    $\llbracket G - F^\mathsf{T} XF \rrbracket \leftarrow \llbracket G \rrbracket - \llbracket F^\mathsf{T} \rrbracket \llbracket XF \rrbracket$        ▷ symmetric
    $\llbracket Y \rrbracket \leftarrow \mathsf{ObliviousRGInverse}(\llbracket G - F^\mathsf{T} XF \rrbracket)$
    $\llbracket XFY \rrbracket \leftarrow \llbracket XF \rrbracket \llbracket Y \rrbracket$
    $\llbracket X + XFYF^\mathsf{T} X \rrbracket \leftarrow \llbracket X \rrbracket + \llbracket XFY \rrbracket \llbracket XF \rrbracket^\mathsf{T}$        ▷ symmetric
    return $\begin{pmatrix} \llbracket X + XFYF^\mathsf{T} X \rrbracket & -\llbracket XFY \rrbracket \\ -\llbracket XFY \rrbracket^\mathsf{T} & \llbracket Y \rrbracket \end{pmatrix}$
```

3.1 Correctness Analysis

Rohde [Roh65] shows that a reflexive generalized inverse A^- of a symmetric, positive-semidefinite matrix *over the real numbers*[2]

$$A = \begin{pmatrix} E & F \\ F^\mathsf{T} & G \end{pmatrix} \tag{9}$$

can be expressed in Banachiewicz–Schur form as

$$A^- = \begin{pmatrix} E^- + E^- FS^- F^\mathsf{T} E^- & -E^- FS^- \\ -S^- F^\mathsf{T} E^- & S^- \end{pmatrix}, \tag{10}$$

where E^- is a reflexive generalized inverse of E and S^- is a reflexive generalized inverse of $S = G - F^\mathsf{T} E^- F$. This form allows for a block-recursive algorithm for computing the reflexive generalized inverse over the real numbers. As proved by Marsaglia and Styan, the correctness of Rohde's result *over an arbitrary field* depends on the following additional condition.

Lemma 1 ([MS74b], statement tailored to our needs)**.** *Over an arbitrary field, Equation* (10) *is a reflexive generalized inverse of A if and only if*

$$\operatorname{rank} A = \operatorname{rank} E + \operatorname{rank} S, \tag{11}$$

or, equivalently, the following three conditions are satisfied simultaneously

$$\begin{cases} (I - EE^-)F(I - S^- S) = 0 & (12) \\ (I - SS^-)F^\mathsf{T}(I - E^- E) = 0 & (13) \\ (I - EE^-)FS^- F^\mathsf{T}(I - E^- E) = 0, & (14) \end{cases}$$

[2] Rohde [Roh65] actually shows his result for complex matrices, but for our purposes it is more convenient to state his result for real matrices.

where E^- and S^- are reflexive generalized inverses of E and $S = A/E$ respectively.

Lemma 2. *Over an arbitrary field, a sufficient condition for Equation* (10) *to be a reflexive generalized inverse of a symmetric matrix A is that A has generic rank profile.*

Proof. We partition A as in Equation (9) arbitrarily but such that E is square. Now we can make a case distinction on E: (i) E is invertible. Then E^- coincides with the ordinary inverse and it immediately follows that $(I - EE^-) = (I - E^-E) = 0$, thus satisfying (12)–(14) from Lemma 1.

(ii) E is not invertible. Since A has generic rank profile, it then immediately follows that $\operatorname{rank} A = \operatorname{rank} E$ and furthermore that $\operatorname{rank} S = 0$, thus satisfying (11). □

Lemma 3. *For any $m \times n$ matrix A over an arbitrary field, any k such that $A_{[k]}$ is invertible, and any i such that $0 \leq i \leq k - \operatorname{rank} A$ it holds that*

$$A_{[k+i]}/A_{[k]} = (A/A_{[k]})_{[i]}.$$

Proof. Let

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix},$$

where $A_{11} = A_{[k]}$ is an invertible $k \times k$ matrix and A_{22} is an $i \times i$ matrix. Then

$$\begin{aligned} (A/A_{[k]})_{[i]} &= \left(\begin{pmatrix} A_{22} & A_{23} \\ A_{32} & A_{33} \end{pmatrix} - \begin{pmatrix} A_{21} \\ A_{31} \end{pmatrix} A_{11}^{-1} \begin{pmatrix} A_{12} & A_{13} \end{pmatrix} \right)_{[i]} \\ &= A_{22} - A_{21} A_{11}^{-1} A_{12} \\ &= A_{[k+i]}/A_{[k]}. \end{aligned}$$ □

Corollary 4. *Protocol* ObliviousRGInverse*, when run on a symmetric matrix A over $\mathbb{F}_p$ having generic rank profile, correctly computes a reflexive generalized inverse.*

Proof. For the base case, we have already argued correctness of the extended reciprocal near the beginning of Section 3. For the recursive step applied to A, note that for an arbitrary partitioning but such that E is a $k \times k$ matrix for some integer k, it is easy to see that E is symmetric and has generic rank profile. Correctness then follows from Lemma 2.

We prove that S is symmetric and has generic rank profile by distinguishing two cases. If E is not invertible, then $\operatorname{rank} A = \operatorname{rank} E$ and S is necessarily the (square) null matrix, which is symmetric and has generic rank profile. Otherwise, E is invertible and $S = A/E = G - F^T E^{-1} F$, which is clearly symmetric. For generic rank profile, we can apply Schur's determinant formula to the leading principal minors of A: for any i such that $0 \leq i \leq \operatorname{rank} A - k$ we have $0 \neq \det(A_{[k+i]}) = \det(E)\det(A_{[k+i]}/E)$. Then, applying Lemma 3 gives $\det(A_{[k+i]}/E) = \det((A/E)_{[i]}) \neq 0$, i.e., A/E has generic rank profile. In both cases, correctness now follows from Lemma 2. □

Remark. We have proved that generic rank profile is sufficient for correctness—we did not prove that this condition is necessary. This leaves open the possibility that a weaker condition on the input matrix (weaker than generic rank profile) would suffice for correctness of ObliviousRGInverse. In the next section we will compute $(AA^{\mathsf{T}}AA^{\mathsf{T}})^{-}$, from which we construct $A^{\dagger}$. To ensure the correctness of ObliviousRGInverse we will actually randomize its input, $AA^{\mathsf{T}}AA^{\mathsf{T}}$, so that it has generic rank profile with high probability and then undo the randomization on the result. One might raise the question whether choosing the modulus p large enough to guarantee the existence of $A^{\dagger}$, could immediately guarantee correctness of ObliviousRGInverse without requiring $AA^{\mathsf{T}}AA^{\mathsf{T}}$ to have generic rank profile. We do not address this question, as our randomization technique suffices and introduces only minimal overhead.

3.2 Complexity Analysis

We first state the complexity (number of secure operations) of protocol ObliviousRGInverse when run on a square matrix whose dimensions are a power of two.

Proposition 5. *Protocol* ObliviousRGInverse*, when run on an $m \times m$ matrix over $\mathbb{F}_p$, where $m = 2^k$ for integer k, requires than $\frac{3}{2}m(m-1) + \frac{1}{2}m\log_2 m$ secure inner products and exactly m invocations of* ScalarRGInverse*.*

Correctness of Proposition 5 is easily proved using induction on k.

If the dimensions of the matrix, m, are not a power of two, it is not always possible to divide the matrix evenly in step 4 of the protocol. In these cases the number of secure inner products required is slightly greater than the number stated in Proposition 5. For general dimensions, we prove the following proposition. We note that this bound is not tight.

Proposition 6. *Protocol* ObliviousRGInverse*, when run on an $m \times m$ matrix over $\mathbb{F}_p$, requires fewer than $\frac{3}{2}m(m-1) + m\log_2 m$ secure inner products and exactly m invocations of* ScalarRGInverse*.*

We also express the complexity of protocol ObliviousRGInverse in terms of elementary secure multiplications, for MPC schemes for which the "cheap inner product" is not available. Note that the bound given here is exact if we assume the naïve algorithm for matrix multiplication. A more advanced algorithm would result in sub-cubic, but still super-quadratic complexity.

Proposition 7. *Protocol* ObliviousRGInverse*, when run on an $m \times m$ matrix over $\mathbb{F}_p$, requires at most $\frac{1}{2}m^3 + \frac{1}{2}m^2 - m$ secure multiplications and exactly m invocations of* ScalarRGInverse*.*

The proofs of Proposition 6 and 7 can be found in the appendix.

4 Computing the Moore–Penrose Pseudoinverse

We will compute the Moore–Penrose pseudoinverse using a formula (see, e.g., [RM71, p. 207]) that computes $A^\dagger$ in terms of a reflexive generalized inverse:

$$A^\dagger = A^\mathsf{T}(AA^\mathsf{T}AA^\mathsf{T})^- AA^\mathsf{T}. \tag{15}$$

Before proposing our protocol Pseudoinverse, we deal with three remaining questions, namely how to compute the common denominator, how to choose an appropriate modulus, and how to reliably compute $(AA^\mathsf{T}AA^\mathsf{T})^-$, as $AA^\mathsf{T}AA^\mathsf{T}$ does not necessarily have generic rank profile, which is required by protocol ObliviousRGInverse for correctness.

4.1 Computing the Common Denominator

Over the rational numbers, a common denominator d such that $dA^\dagger$ is integer-valued if A is integer-valued is $d = (\operatorname{vol} A)^2$ [Spr83, Satz 10]. The squared volume is minimal in the sense that there exist matrices for which it is the smallest possible common denominator.

If we would have an *orthonormal* basis for the left or right nullspace of A, then we could use [BI92, Thm. (4.1)] to compute $(\operatorname{vol} A)^2$ directly. An orthonormal basis does not necessarily exist over an arbitrary field. Instead, we generalize [BI92, Thm. (4.1)] by relaxing the requirements on the nullspace basis.

Lemma 8. *Let $A \in \mathbb{F}^{m\times k}$ be a matrix of rank r. Let $B \in \mathbb{F}^{m\times \ell}$ be a matrix of rank $m - r$ such that its columns are orthogonal to the columns of A, i.e., $B^\mathsf{T}A = 0$. Then,*

$$\det(AA^\mathsf{T} + BB^\mathsf{T}) = (\operatorname{vol} A)^2(\operatorname{vol} B)^2.$$

Proof. Note that $AA^\mathsf{T} + BB^\mathsf{T} = \begin{pmatrix} A & B\end{pmatrix}\begin{pmatrix} A & B\end{pmatrix}^\mathsf{T}$. Because the columns of A are orthogonal to those of B, the matrix $\begin{pmatrix} A & B\end{pmatrix}$ has rank $r + (m - r) = m$ and hence

$$\det(\begin{pmatrix} A & B\end{pmatrix}\begin{pmatrix} A & B\end{pmatrix}^\mathsf{T}) = (\operatorname{vol}\begin{pmatrix} A & B\end{pmatrix})^2 = (\operatorname{vol} A)^2(\operatorname{vol} B)^2,$$

where the first equality holds by equation (8), and the second equality is [BI92, Example 5.1]. □

Theorem 9. *Let $A \in \mathbb{F}^{m\times n}$ be a matrix of rank r. Let $K = I - AA^\dagger \in \mathbb{F}^{m\times m}$. Then,*

$$(\operatorname{vol} A)^2 = \det(AA^\mathsf{T} + K).$$

Proof. By property (3) of the pseudoinverse, we have that $K = K^\mathsf{T}$. This fact, and property (1) of the pseudoinverse imply that $KK^\mathsf{T} = KK = K$ and $K^\mathsf{T}A = 0$, i.e., K is idempotent and its columns are orthogonal to the columns of A.

Combining equation (6) with the fact that K is idempotent and symmetric gives us that $\operatorname{vol} K = \operatorname{vol}(KK^\mathsf{T}) = (\operatorname{vol} K)^2$. Since the volume of a matrix is nonzero, we conclude that $\operatorname{vol} K = 1$.

Orthogonality of the columns of K and A implies that $\operatorname{rank} K \leq m - r$ and

$$\operatorname{rank} K = \operatorname{rank}(I - AA^\mathsf{T}) \geq \operatorname{rank} I - \operatorname{rank}(AA^\mathsf{T}) = m - r$$

follows from subadditivity of matrix rank. Applying Lemma 8 gives us

$$\det(AA^\mathsf{T} + K) = \det(AA^\mathsf{T} + KK^\mathsf{T}) = (\operatorname{vol} A)^2(\operatorname{vol} K)^2 = (\operatorname{vol} A)^2. \qquad \square$$

4.2 Bound on the Modulus

Springer [Spr83] has proved the following upper bound on the magnitudes of the numerators and the common denominator of the pseudoinverse. Choosing p larger than twice this bound will guarantee that: (i) $d = (\operatorname{vol} A)^2$ is an invertible element in $\mathbb{F}_p$, which is a necessary and sufficient condition for existence of $A^\dagger$ over $\mathbb{F}_p$ [BRP90] (see also Section 2), and (ii) that the pair $(dA^\dagger, d)$ over $\mathbb{F}_p$ coincides with $(dA^\dagger, d)$ over $\mathbb{Z}$, and (iii) that the product $AA^\mathsf{T}AA^\mathsf{T}$ occurring in Equation (15) has the same rank as A (which we will need in Theorem 14).

Lemma 10 ([Spr83, Satz 12])**.** *Let $N_0 = (\operatorname{vol} A)^2$ and $Z_0 = (z_{ij}) \in \mathbb{Z}^{m\times n}$ be an integer matrix of rank r such that $A^\dagger = \frac{1}{N_0}Z_0$. Let $\mu = \min(m, n)$. Then,*

$$\max(|N_0|, \max_{i,j} |z_{ij}|) \leq \max\left(\frac{\|A\|_F^{2r}}{r^r}, \frac{\|A\|_F^{2r-1}}{\sqrt{r^r(r-1)^{r-1}}}\right), \tag{16}$$

and

$$\max(|N_0|, \max_{i,j} |z_{ij}|) \leq \max\left(\frac{\|A\|_F^{2\mu}}{\mu^\mu}, \frac{\|A\|_F^{2\mu-1}}{\sqrt{\mu^\mu(\mu-1)^{\mu-1}}}\right), \tag{17}$$

where $\|A\|_F = \sqrt{\sum_{ij} |a_{ij}|^2}$ is the Frobenius norm of A.

Remark. In a setting in which the rank r is unknown, one would use (17).

For our construction, we further require that

$$\operatorname{rank}(AA^{\mathsf{T}}AA^{\mathsf{T}}) = \operatorname{rank} A. \tag{18}$$

This requirement holds unconditionally over fields of characteristic zero, but not necessarily over finite fields. Nonetheless, as we show below, it turns out that existence of the Moore–Penrose inverse already implies (18).

Proposition 11. *Let A be an arbitrary matrix over $\mathbb{F}$. The Moore–Penrose inverse of A exists if and only if*

$$\operatorname{rank}(AA^{\mathsf{T}}AA^{\mathsf{T}}) = \operatorname{rank} A.$$

Proof. Recall from Section 2 that the Moore–Penrose inverse exists over $\mathbb{F}$ if and only if $\operatorname{rank}(AA^{\mathsf{T}}) = \operatorname{rank}(A^{\mathsf{T}}A) = \operatorname{rank} A$. Let $A = VW$ be a rank decomposition of A, i.e., V and W have full column-rank and full row-rank, respectively. Over an arbitrary field, a rank decomposition exists but is not necessarily unique; see, e.g., [Rao73]. Then,

$$\operatorname{rank}(AA^{\mathsf{T}}) = \operatorname{rank}(VWW^{\mathsf{T}}V^{\mathsf{T}}) = \operatorname{rank} A \iff \operatorname{rank} WW^{\mathsf{T}} = \operatorname{rank} A,$$

and similarly,

$$\operatorname{rank}(A^{\mathsf{T}}A) = \operatorname{rank}(W^{\mathsf{T}}V^{\mathsf{T}}VW) = \operatorname{rank} A \iff \operatorname{rank} V^{\mathsf{T}}V = \operatorname{rank} A.$$

Also note that both WW^{T} and $V^{\mathsf{T}}V$ have dimension $r \times r$ with $r = \operatorname{rank} A$, i.e., they are invertible. We now write $AA^{\mathsf{T}}AA^{\mathsf{T}}$ in terms of V and W, and multiply by V^{T} from the left and by V from the right, by which we obtain :

$$V^{\mathsf{T}}AA^{\mathsf{T}}AA^{\mathsf{T}}V = (V^{\mathsf{T}}V)(WW^{\mathsf{T}})(V^{\mathsf{T}}V)(WW^{\mathsf{T}})(V^{\mathsf{T}}V).$$

Thus, $\operatorname{rank} V^{\mathsf{T}}AA^{\mathsf{T}}AA^{\mathsf{T}}V = \operatorname{rank} A$, if and only if $\operatorname{rank} AA^{\mathsf{T}}AA^{\mathsf{T}} = \operatorname{rank} A$. □

4.3 Symmetric Preconditioning

A *preconditioner* is a mapping $A \mapsto h(A)$ for matrices A from a given class, where the goal is to achieve a certain property, either with certainty or with high probability. This property is typically an input condition from some computational technique. For a more elaborate and formal introduction into preconditioning we refer to [CEK^{+}02]. Here, we restrict to preconditioners for achieving *generic rank profile* for symmetric matrices of the form $A = BB^{\mathsf{T}}$ over an arbitrary field of positive characteristic.

To ensure correctness of protocol ObliviousRGInverse, we need a preconditioner with the following three properties:

(i) achieves generic rank profile with high probability;

(ii) preserves symmetry, i.e., $h(A)$ is symmetric;

(iii) is *removable.* Informally speaking, this means that the preconditioner can be efficiently removed once “it has done its job”. Formally, a preconditioner is removable with respect to computing a reflexive generalized inverse if there exists an efficiently computable mapping g such that $g(h(A)^-) \in \mathcal{A}^-$, where $\mathcal{A}^-$ denotes the set of reflexive generalized inverses of A.

Although several preconditioners for achieving generic rank profile have been proposed in the literature, we are not aware of an existing result that covers all of the above properties simultaneously. For example, the Toeplitz preconditioner by Kaltofen and Saunders [KS91] fails to satisfy (ii), and the diagonal preconditioner proposed in [EK97] (combined with a suitable linear-independence preconditioner, see [CEK$^+$02]) fails to satisfy (iii).

In this section we will show that for a symmetric matrix A, the preconditioner $h(A) = UAU^\mathsf{T}$ with U a uniformly random (invertible) matrix is sufficient for satisfying (i)–(iii). It is easy to see that (ii) holds. We prove property (i) in Theorem 14 and (iii) in Lemma 15.

Lemma 12 (Schwartz–Zippel)**.** *Let $g \in \mathbb{F}[x_1, \dots, x_n]$ be a nonzero polynomial of total degree $d \geq 0$ over a field $\mathbb{F}$. Let $\mathcal{S} \subseteq \mathbb{F}$ and let $\alpha_1, \dots, \alpha_n$ be chosen independently and uniformly at random from $\mathcal{S}$. Then,*

$$\Pr[g(\alpha_1, \dots, \alpha_n) = 0] \leq \frac{d}{|\mathcal{S}|}.$$

Lemma 13 (See, e.g., [BvzGH82, Lem. 2-(iii)])**.** *The probability that a uniformly random matrix $U \in \mathbb{F}^{m \times m}$ is invertible equals*

$$\Pr(\det U \neq 0) = \prod_{k=1}^{m} \left(1 - |\mathbb{F}|^{-k}\right).$$

Theorem 14. *Let $A \in \mathbb{F}^{m \times n}$ be arbitrary, let r be the rank of A and let AA^T have the same rank as A. Let $U \in \mathbb{F}^{m \times m}$ be chosen uniformly at random. Then, the probability that U is invertible and $UAA^\mathsf{T}U^\mathsf{T}$ has generic rank profile is*

$$\Pr_U \left(\det U \neq 0 \wedge [UAA^\mathsf{T}U^\mathsf{T}]_k \neq 0 \quad \forall k \in [r]\right) > 1 - \frac{r(r+1)+2}{|\mathbb{F}|}.$$

Proof. We view $U = (u_{i,j})$ as a polynomial matrix with $u_{i,j}$ as indeterminates. For every $1 \leq k \leq r$, we apply the Cauchy–Binet formula to obtain an expression for the leading principal minor of order k of the matrix $UAA^\mathsf{T}U^\mathsf{T}$, which is a polynomial in the variables $u_{i,j}$, where we let $\mathcal{K} = [k]$,

$$\begin{aligned}
f_k(u_{1,1}, \dots, u_{i,j}, \dots, u_{m,m}) &= [UAA^\mathsf{T}U^\mathsf{T}]_{\mathcal{K},\mathcal{K}} \\
&= \sum_{\substack{\mathcal{I}\subset[m]\\|\mathcal{I}|=k}} [UA]_{\mathcal{K},\mathcal{I}}[A^\mathsf{T}U^\mathsf{T}]_{\mathcal{I},\mathcal{K}} = \sum_{\substack{\mathcal{I}\subset[m]\\|\mathcal{I}|=k}} \big([UA]_{\mathcal{K},\mathcal{I}}\big)^2 \\
&= \sum_{\substack{\mathcal{I}\subset[m]\\|\mathcal{I}|=k}} \Big(\sum_{\substack{\mathcal{J}\subset[m]\\|\mathcal{J}|=k}} [U]_{\mathcal{K},\mathcal{J}}[A]_{\mathcal{J},\mathcal{I}}\Big)^2.
\end{aligned}$$

It follows immediately from the structure of this formula that the total degree of f_k is $2k$.

Let us now prove that none of the polynomials f_k for all $1 \le k \le r$ is equal to the zero polynomial. Because AA^T is symmetric, there exists an invertible matrix $S = (s_{i,j})$ such that $SAA^\mathsf{T}S^\mathsf{T} = \Lambda$ where $\Lambda = \mathrm{diag}(\lambda_1, \dots, \lambda_r, 0, \dots, 0)$ with $\lambda_i \neq 0$ for all $1 \le i \le r$ [Alb38, Thm. 6]. Hence,

$$f_k(s_{1,1}, \dots, s_{i,j}, \dots, s_{m,m}) = \prod_{i=1}^{k} \lambda_i \neq 0 \qquad \forall k \in [r].$$

The Schwartz–Zippel lemma asserts that $\Pr[f_k(U_{1,1}, \dots, U_{m,m}) = 0] \le \frac{2k}{|\mathbb{F}|}$, where the $U_{i,j}$ represent the elements of U when viewed as (uniformly random and independent) random variables. Hence, by applying the union bound over k we obtain

$$\Pr[f_1(U) \neq 0 \wedge \cdots \wedge f_r(U) \neq 0] \ge 1 - \frac{\sum_{k=1}^r 2k}{|\mathbb{F}|} = 1 - \frac{r(r+1)}{|\mathbb{F}|}.$$

Combining this bound with that of Lemma 13 gives

$$\begin{aligned}
&\Pr_U\big(\det U \neq 0 \wedge [UAA^\mathsf{T}U^\mathsf{T}]_k \neq 0 \quad \forall k \in [r]\big) \\
&\quad\ge \prod_{k=1}^{m} \Big(1 - |\mathbb{F}|^{-k}\Big) - \frac{r(r+1)}{|\mathbb{F}|} > \frac{|\mathbb{F}|-2}{|\mathbb{F}|-1} - \frac{r(r+1)}{|\mathbb{F}|} > 1 - \frac{r(r+1)+2}{|\mathbb{F}|},
\end{aligned}$$

where we used that

$$\begin{aligned}
\prod_{k=1}^{m}(1-x_k) > \prod_{k=1}^{\infty}(1-x_k) &= 1 - x_1 - x_2(1-x_1) - x_3(1-x_1)(1-x_2) - \dots \\
&> 1 - \sum_{k=1}^{\infty} x_k.
\end{aligned}$$

With $x_k = |\mathbb{F}|^{-k}$, we get that $\prod_{k=1}^m \big(1 - |\mathbb{F}|^{-k}\big) > 1 - (|\mathbb{F}|-1)^{-1}$.

□

We now prove that the preconditioner $h(A) = UAU^{\mathsf{T}}$ with invertible U is removable.

Lemma 15. *Let A be a matrix over $\mathbb{F}$ and let $\mathcal{A}^{-}$ denote the set of reflexive generalized inverses of A. Let U be an invertible matrix over $\mathbb{F}$ and let $Y = (UAU^{\mathsf{T}})^{-}$ be a reflexive generalized inverse of UAU^{T}. Then, $U^{\mathsf{T}}YU \in \mathcal{A}^{-}$.*

Proof. Given the Penrose equations (1) and (2) for Y, we need to show that the Penrose equations (1) and (2) hold for A^{-}. Since U is invertible,

$$A(U^{\mathsf{T}}YU)A = U^{-1}(UAU^{\mathsf{T}})Y(UAU^{\mathsf{T}})(U^{\mathsf{T}})^{-1} = U^{-1}(UAU^{\mathsf{T}})(U^{\mathsf{T}})^{-1} = A.$$

Furthermore,

$$(U^{\mathsf{T}}YU)A(U^{\mathsf{T}}YU) = U^{\mathsf{T}}Y(UAU^{\mathsf{T}})YU = U^{\mathsf{T}}YU. \qquad \square$$

4.4 Construction

Our protocol Pseudoinverse, on input of a secret-shared matrix $\llbracket A \rrbracket \in \mathbb{F}_p^{m\times n}$, computes the pair $(\llbracket A^{\dagger} \rrbracket, \llbracket (\operatorname{vol} A)^2 \rrbracket)$ and is given as Protocol 3. Protocol Pseudoinverse makes use of a secure subprotocol Determinant for computing the determinant of an invertible matrix in $\mathbb{F}_p^{m\times m}$ in secret-shared form. A possible instantiation of Determinant can be found in [CD01], where it is called protocol Π_0. See also [BBSdV19], which slightly modifies this protocol to reduce its randomness complexity.

Protocol 3 Pseudoinverse($\llbracket A \rrbracket$)

```
if $m > n$ then
    return Pseudoinverse($\llbracket A \rrbracket^{\mathsf{T}}$)$^{\mathsf{T}}$
$\llbracket AA^{\mathsf{T}} \rrbracket \leftarrow \llbracket A \rrbracket \llbracket A \rrbracket^{\mathsf{T}}$                                ▷ symmetric
$\llbracket AA^{\mathsf{T}}AA^{\mathsf{T}} \rrbracket \leftarrow \llbracket AA^{\mathsf{T}} \rrbracket \llbracket AA^{\mathsf{T}} \rrbracket$                    ▷ symmetric
$U \xleftarrow{\$} \mathbb{F}_p^{m\times m}$
$\llbracket X \rrbracket \leftarrow U^{\mathsf{T}}$ObliviousRGInverse($U \llbracket AA^{\mathsf{T}}AA^{\mathsf{T}} \rrbracket U^{\mathsf{T}}$)$U$
$\llbracket XAA^{\mathsf{T}} \rrbracket \leftarrow \llbracket X \rrbracket \llbracket AA^{\mathsf{T}} \rrbracket$
$\llbracket A^{\dagger} \rrbracket \leftarrow \llbracket A^{\mathsf{T}} \rrbracket \llbracket XAA^{\mathsf{T}} \rrbracket$
$\llbracket K \rrbracket \leftarrow I - \llbracket AA^{\mathsf{T}} \rrbracket \llbracket XAA^{\mathsf{T}} \rrbracket$          ▷ symmetric; in parallel with $\llbracket A^{\dagger} \rrbracket$
$\llbracket d \rrbracket \leftarrow$ Determinant($\llbracket AA^{\mathsf{T}} \rrbracket + \llbracket K \rrbracket$)
return ($\llbracket A^{\dagger} \rrbracket, \llbracket d \rrbracket$)
```

We note that the rank of A is given by $\operatorname{Tr}(AA^{\dagger})$ [BO71]. It can be computed obliviously in Pseudoinverse as $\llbracket r \rrbracket = m - \operatorname{Tr}(\llbracket K \rrbracket)$.

Corollary 16. *Protocol* Pseudoinverse*, when run on an arbitrary $m \times n$ matrix over $\mathbb{F}_p$, correctly computes the Moore–Penrose pseudoinverse with probability at least*

$$\Pr(\mathit{success}) \geq \left[1 - \frac{m(m+1)+2}{|\mathbb{F}|}\right] \cdot P_{\mathsf{Determinant}},$$

where $P_{\mathsf{Determinant}}$ denotes the success probability of protocol Determinant*.*

4.5 Complexity Analysis

Proposition 17. *Protocol* Pseudoinverse*, when run on an arbitrary $m \times n$ matrix over $\mathbb{F}_p$, requires $mn + \frac{5}{2}m^2 + \frac{3}{2}m$ secure inner products (or: $m^2n + \frac{5}{2}m^3 + \frac{3}{2}m^2$ secure multiplications), one invocation of protocol* Determinant *on a symmetric $m \times m$ matrix and one invocation of* ObliviousRGInverse *on a symmetric $m \times m$ matrix.*

Protocol Determinant, instantiated as in [BBSdV19], when invoked on a $m \times m$ matrix, requires secure sampling of m^2 random elements, and performing $2m^2 + m - 1$ secure inner products (or: $\frac{4}{3}m^3 + \frac{2}{3}m - 1$ secure multiplications) and m^2 open operations.

The field inversion technique from Bar-Ilan–Beaver [BIB89] requires secure sampling of one random element and one multiply-and-open operation.

Corollary 18. *Protocol* Pseudoinverse*, when run on an arbitrary $m \times n$ matrix over $\mathbb{F}_p$, with protocol* Determinant *instantiated as in [BBSdV19], requires in total $nm + 6m^2 + o(m^2)$ secure inner products (or: $nm^2 + \frac{13}{3}m^3 + o(m^3)$ secure multiplications), m^2 public random elements, m^2 private random elements, m^2 openings, m secure zero tests and m secure field inversions.*

Remark. It is straightforward to adapt Protocol 3 such that it does not compute the pseudoinverse of a given matrix A, but instead directly solves the linear system $A\boldsymbol{x} = \boldsymbol{b}$ for the vector $\boldsymbol{x}$. By carefully arranging the order of evaluation of the matrix-vector products, one can avoid the matrix-matrix product that gives rise to the mn term. Then, the complexity (number of secure inner products) becomes $O(n + m^2)$ in case $m \leq n$, and $O(n^2)$ otherwise. Note, however, that this adaptation imposes an additional constraint on the size of the modulus; the field should now be large enough to uniquely represent the coefficients of the vector $A^\dagger \boldsymbol{b}$.

Bibliography

[Alb38] A.A. Albert. Symmetric and alternate matrices in an arbitrary field, I. *Transactions of the American Mathematical Society*, 43(3):386–436, 1938.

[BBSdV19] F. Blom, N.J. Bouman, L.A.M. Schoenmakers, and N. de Vreede. Efficient secure ridge regression from randomized Gaussian elimination, 2019. To appear.

[BdV18] N.J. Bouman and N. de Vreede. New protocols for secure linear algebra: Pivoting-free elimination and fast block-recursive matrix decomposition. Cryptology ePrint Archive, Report 2018/703, 2018. http://eprint.iacr.org/2018/703.

[BI92] A. Ben-Israel. A volume associated with $m \times n$ matrices. *Linear Algebra and its Applications*, 167:87–111, 1992.

[BIB89] J. Bar-Ilan and D. Beaver. Non-cryptographic fault-tolerant computing in constant number of rounds of interaction. In *Proc. 8th Symp. on Princip. of Distr. Comp.*, pages 201–209, NY, 1989. ACM.

[BIG03] A. Ben-Israel and T.N.E. Greville. *Generalized Inverses - Theory and Applications.* CMS Books in Mathematics. Springer, 2003.

[BKLS18] D. Bogdanov, L. Kamm, S. Laur, and V. Sokk. Rmind: A tool for cryptographically secure statistical analysis. *IEEE Trans. Dependable Sec. Comput.*, 15(3):481–495, 2018.

[BO71] T.L. Boullion and P.L. Odell. *Generalized Inverse Matrices.* Wiley, 1971.

[BRP90] R.B. Bapat, K.P.S. Bhaskara Rao, and K. Manjunatha Prasad. Generalized inverses over integral domains. *Linear Algebra and its Applications*, 140:181–196, 1990.

[BvzGH82] A. Borodin, J. von zur Gathen, and J. Hopcroft. Fast parallel matrix and GCD computations. *Information and Control*, 52(3):241–256, 1982.

[CD01] R.J.F. Cramer and I.B. Damgård. Secure distributed linear algebra in a constant number of rounds. In *Proc. CRYPTO 2001, Santa Barbara, USA*, pages 119–136. Springer, 2001.

[CDI05] R.J.F. Cramer, I.B. Damgård, and Y. Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In *Proc. TCC 2005*, volume 3378 of *LNCS*, pages 342–362. Springer, 2005.

[CDN15] R.J.F. Cramer, I.B. Damgård, and J.B. Nielsen. *Secure multiparty computation and secret sharing: An information theoretic approach.* Cambridge University Press, 2015.

[CEK$^+$02] L. Chen, W. Eberly, E. Kaltofen, B.D. Saunders, W.J. Turner, and G. Villard. Efficient matrix preconditioners for black box linear algebra. *Linear Algebra Its Appl.*, 343–344:119–146, 2002.

[CKP07] R.J.F. Cramer, E. Kiltz, and C. Padró. A note on secure computation of the Moore–Penrose pseudoinverse and its application to secure linear algebra. In *Proc. CRYPTO 2007*, volume 4622, pages 613–630. Springer, 2007.

[DFK$^+$06] I.B. Damgård, M. Fitzi, E. Kiltz, J.B. Nielsen, and T. Toft. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In *Proc. TCC 2006*, volume 3876 of *LNCS*, pages 285–304. Springer, 2006.

[EK97] W. Eberly and E. Kaltofen. On randomized Lanczos algorithms. In *Proc. ISSAC '97*, pages 176–183. ACM, 1997.

[Gre66] T. Greville. Note on the generalized inverse of a matrix product. *SIAM Review*, 8(4):518–521, 1966.

[GSB$^+$17] A. Gascón, P. Schoppmann, B. Balle, M. Raykova, J. Doerner, S. Zahur, and D. Evans. Privacy-preserving distributed linear regression on high-dimensional data. *PoPETs*, 2017(4):345–364, 2017.

[Har86] R.E. Hartwig. The reverse order law revisited. *Linear Algebra and its Applications*, 76:241–246, 1986.

[KL96] E. Kaltofen and A. Lobo. On rank properties of Toeplitz matrices over finite fields. In *Proc. ISSAC '96*, pages 241–249. ACM, 1996.

[KMWF07] E. Kiltz, P. Mohassel, E. Weinreb, and M. Franklin. Secure linear algebra using linearly recurrent sequences. In *Proc. TCC 2007*, volume 4392 of *LNCS*, pages 291–310. Springer, 2007.

[KS91] E. Kaltofen and B.D. Saunders. On Wiedemann's method of solving sparse linear systems. In *Proc. 9th Int. Symp. AAECC*, volume 539 of *LNCS*, pages 29–38. Springer, 1991.

[Mal10] G. Malaschonok. Fast generalized Bruhat decomposition. In *International Workshop on Computer Algebra in Scientific Computing*, pages 194–202. Springer, 2010.

[MS74a] G. Marsaglia and G.P.H. Styan. Equalities and inequalities for ranks of matrices. *Linear and Multilinear Algebra*, 2(3):269–292, 1974.

[MS74b] G. Marsaglia and G.P.H. Styan. Rank conditions for generalized inverses of partitioned matrices. *Sankhyā: The Indian Journal of Statistics, Series A*, pages 437–442, 1974.

[Mul87] K. Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Combinatorica*, 7(1):101–104, 1987.

[MW08] P. Mohassel and E. Weinreb. Efficient secure linear algebra in the presence of covert or computationally unbounded adversaries. In *Proc. CRYPTO 2008*, volume 5157 of *LNCS*, pages 481–496. Springer, 2008.

[NO07] T. Nishide and K. Ohta. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In *Proc. PKC 2007*, volume 4450 of *LNCS*, pages 343–360. Springer, 2007.

[NW06] K. Nissim and E. Weinreb. Communication efficient secure linear algebra. In *Proc. TCC 2006*, volume 3876 of *LNCS*, pages 522–541. Springer, 2006.

[NWI+13] V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft. Privacy-preserving ridge regression on hundreds of millions of records. In *Proc. 2013 IEEE Symp. on Security and Privacy*, pages 334–348. IEEE, 2013.

[Pea68] Martin H. Pearl. Generalized inverses of matrices with entries taken from an arbitrary field. *Linear Algebra and its Applications*, 1(4):571–587, 1968.

[Rao73] C.R. Rao. *Linear Statistical Inference and its Applications*. Wiley, 1973.

[RM71] C.R. Rao and S.K. Mitra. *Generalized inverse of matrices and its applications*. Wiley, 1971.

[Roh65] C.A. Rohde. Generalized inverses of partitioned matrices. *Journal of the Society for Industrial and Applied Mathematics*, 13(4):1033–1035, 1965.

[Spr83] J. Springer. Die exakte Berechnung der Moore–Penrose-Inversen einer Matrix durch Residuenarithmetik. *Zeitschrift für Angewandte Mathematik und Mechanik*, 63(3):203–210, 1983.

[Wan81] P. S. Wang. A *p*-adic algorithm for univariate partial fractions. In *Proc. SYMSAC '81*, pages 212–217. ACM, 1981.

Proofs of Proposition 6 and 7

The proof is by complete induction. It is clear that the number of invocations of ScalarRGInverse required when ObliviousRGInverse is run on an $m \times m$ matrix is equal to m. Let $D(m)$ denote the number of secure inner products required to run protocol ObliviousRGInverse on an $m \times m$ matrix. Similarly, let $M(m)$ be the number of secure multiplications required, in case a “cheap inner product” is not available. Then, we have to show that

$$D(m) < \frac{3}{2}m(m-1) + m\log_2 m; \qquad \text{and} \tag{19}$$

$$M(m) \leq \frac{1}{2}m^3 + \frac{1}{2}m^2 - m. \tag{20}$$

Inspection of the protocol shows that

$$D(1) = 0;$$

$$D(2k) = 2D(k) + 3k^2 + k; \text{ and} \tag{21}$$

$$D(2k+1) = D(k) + D(k+1) + 3k^2 + 4k + 1, \tag{22}$$

where we distinguish between even ($m = 2k$) and odd ($m = 2k+1$) dimensions. Similarly, for $M(m)$, we have

$$M(1) = 0;$$

$$M(2k) \leq 2M(k) + 3k^3 + k^2; \text{ and} \tag{23}$$

$$M(2k+1) \leq M(k) + M(k+1) + 3k^3 + \frac{11}{2}k^2 + \frac{5}{2}k. \tag{24}$$

The inequalities in (23) and (24) can be replaced with equalities in case the naïve algorithm for matrix multiplication is used.

In the base case $m = 1$, the propositions clearly hold. Assume the propositions hold for all $m' < m$. Then for odd $m = 2k+1$ substitution of (19) in (22) yields

$$\begin{aligned} D(2k+1) &< \frac{3}{2}m(m-1) + k + 1 + k\log_2 k + (k+1)\log_2(k+1) \\ &= \frac{3}{2}m(m-1) + \log_2\left(k^k(k+1)^{k+1}2^{k+1}\right) \\ &< \frac{3}{2}m(m-1) + (2k+1)\log_2(2k+1), \end{aligned}$$

where the last inequality follows from monotonicity of the logarithm and from the following inequality:

$$\begin{aligned} 2^{k+1}k^k(k+1)^{k+1} &= 2^{1-k}(2k+1-1)^k(2k+1+1)^k(k+1) \\ &= 2^{1-k}((2k+1)^2-1)^k(k+1) \\ &< 2^{1-k}(2k+1)^{2k}(k+1) \\ &< (2k+1)^{2k+1}. \end{aligned}$$

For the case of even m, Proposition 6 follows immediately by substituting equation (19) in (21). Similarly, Proposition 7 follows from the substitution of (20) in (23) and (24).