A Note on "Privacy-Preserving and Secure Cloud Computing: A Case of Large-Scale Nonlinear Programming"

Zhengjun Cao, Lihua Liu

Abstract. We show that the outsourcing algorithm for the case of linear constraints [IEEE Trans. Cloud Comput., 2023, 11(1), 484-498] cannot keep output privacy, due to the simple translation transformation. We also suggest a remedy method by adopting a hybrid transformation which combines the usual translation transformation and resizing transformation so as to protect the output privacy.

Keywords: Nonlinear programming, linear constraints, output privacy, translation transformation, resizing transformation

1 Introduction

The secure outsourcing of large-scale nonlinear programming problem has many applications. Recently, Du et al. [\[1\]](#page-4-0) have presented two outsourcing algorithms for the case of linear constraints and the case of nonlinear constraints. In the considered scenario, there are two entities, the user $\mathcal U$ and the server $\mathcal S$. To keep the input and output privacies, the user needs to encrypt his input data by using some encryption techniques. After receiving the returned solution by the server, the user retrieves the true solution by the corresponding decryption. Though the algorithms are interesting, we find the outsourcing algorithm for the case of linear constraints cannot protect the output privacy, due to the simple translation transformation. We will suggest a method to fix this flaw.

2 Review of the two algorithms

The Algorithm I is designed for the case of linear constraints. The original problem is

P1 : Minimize $f(x)$ subject to $\mathbf{A}\mathbf{x} = \mathbf{b}, \ \ \mathbf{x} \geq 0$

where $f(x)$ is the nonlinear objective function, $A \in R^{m \times n}$ and $b \in R^m$ are linear constraints, $\boldsymbol{x} \in R^{n \times 1}$ is an *n*-dimension variable vector $(x_1, x_2, \dots, x_n)^\top$.

Z. Cao, Department of Mathematics, Shanghai University, Shanghai, 200444, China.

L. Liu, Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.

Email: liulh@shmtu.edu.cn

In order to keep the input privacy and output privacy, the problem is converted into

P4: Minimize
$$
f(z)
$$

subject to $A'z = b'$, $z \ge r$

where $z = x + r$, $A' = LPQAR$, $b' = LPQb$, r is a random vector, P, Q are two random diagonal matrixes, and L, R are two random permutation matrixes (see Algorithm 1, Algorithm 2, page 488, $\text{Ref.}[\mathbf{1}]).$

The Algorithm II is designed for the case of nonlinear constraints. The original problem is

P2: Minimize
$$
f(\boldsymbol{x})
$$

\nsubject to $g_i(\boldsymbol{x}) = 0, i = 1, \dots, m$
\n $h_j(\boldsymbol{x}) \leq b_j, j = 1, \dots, l$
\n $a_k \leq x_k \leq u_k, k = 1, \dots, n$

where the coefficient matrix and vector of the equality constraints are denoted as $G \in \mathbb{R}^{m \times n}, b \in$ $R^{l\times 1}$, and the inequality constraints are denoted by $\mathbf{H} \in R^{l\times n}$.

The problem is converted into

P5: Minimize
$$
f(z)
$$

\nsubject to $\hat{g}_i(z) = 0, i = 1, \dots, m$
\n $\hat{h}_j(z) \leq \hat{b}_j, j = 1, \dots, l$
\n $\hat{a}_k \leq z_k \leq \hat{u}_k, k = 1, \dots, n$

where $z = x + r$, $\hat{a}_k = a_k + r_k$, $\hat{u}_k = u_k + r_k$, r_k is the kth element of r, the corresponding matrixes and vectors are

$$
\hat{G}=XPQGY, \ \hat{H}=XTSHY, \ \hat{b}=XPQb.
$$

We refer to $\S 3.2$ in Ref. [\[1\]](#page-4-0) for the notation descriptions.

3 Some typos

As we see, the new problem P4 is specified with the equality constraints

$$
A'z = LPQAR(x+r) = LPQARx + LPQARr \neq LPQb
$$

So, the new vector b' must be specified as

$$
b^\prime = LPQARx + LPQARr
$$

Likewise, the new problem P5 is wrongly specified. In fact,

$$
\hat{G}z = XPQGY(x+r) = XPQGYx + XPQGYr = XPQGYr \neq 0
$$

Besides,

$$
\hat{H}\bm{z}=\bm{X}\bm{T}\bm{S}\bm{H}\bm{Y}(\bm{x}+\bm{r})=\bm{X}\bm{T}\bm{S}\bm{H}\bm{Y}\bm{x}+\bm{X}\bm{T}\bm{S}\bm{H}\bm{Y}\bm{r}\nleq \bm{X}\bm{P}\bm{Qb}
$$

These notations should be restated.

4 The loss of output privacy in Algorithm I

The outsourcing process of Algorithm I can be depicted as follows.

Notice that the original target vector x is converted into

$$
z = x + r \tag{1}
$$

where r is a random vector to mask x . The encryption involves only the simple translation transformation. In the later outsourcing process, the user needs to transfer the data

{ $f(z)$, **A'**, **b'**, **r**}, not { $f(z)$, **A'**, **b'**},

via an open channel.

Without the vector **r**, the server cannot recover the inequality constraints $z \ge r$, instead only the nonnegative constraints $z \geq 0$. But one cannot derive the solutions to $f(z)$, s.t., $A'z = b'$, $z \geq r$, from that of $f(z)$, s.t., $A'z = b', z \ge 0$. The original presentation has confused the inequality constraints $z \ge r$ with the nonnegative constraints $z \ge 0$. It neglected the necessity to transfer the vector **r** to the server.

The server returns the solution z^* to the user via the open channel. Clearly, the server who knows the vector r, can retrieve the target solution x^* by computing $x^* = z^* - r$. Besides, any adversary who has captured the vectors r, z^* via open channels can also retrieve the true solution x^* . Therefore, the Algorithm I cannot keep the output privacy, not as claimed. Du et al. have neglected the fact that the masking vector r must be sent to the server.

To fix the flaw, one needs to use a hybrid transformation which combines the usual translation transformation and resizing transformation. For example, the target vector can be converted into

$$
z = \lambda x + r \tag{2}
$$

where λ is a random positive number, and r is a random vector. In this case, only the user who knows the random number λ can retrieve the final solution by computing

$$
x^* = (z^* - r)/\lambda \tag{3}
$$

By the way, in the Algorithm II, the masking vector \boldsymbol{r} is not exposed due to that

$$
\hat{a}_k \le z_k \le \hat{u}_k, k = 1, \cdots, n,
$$

$$
\hat{a}_k = a_k + r_k, \ \hat{u}_k = u_k + r_k
$$

One cannot retrieve the masking vector r from the outsourced data $\{(\hat{a}_k, \hat{u}_k)\}_{k=1,\cdots,n}$.

5 Further discussions

 \diamondsuit Feasible region similarity. To keep the similarity between the feasible region of new outsourced problem and the original, one needs to use the general translation transformation and resizing transformation. If the target vector x is converted into

$$
z = Dx + r \tag{2'}
$$

where \bm{D} is a random nonsingular positive diagonal matrix, and \bm{r} is a random vector, the feasible region of the outsourced problem could be incompatible with the original. In this case, the recovered solution

$$
x^* = D^{-1}(z^* - r) \tag{3'}
$$

makes no sense.

 \diamondsuit Representations for nonlinear constraints. The Algorithm II is designed for the case of nonlinear constraints

$$
g_i(\mathbf{x}) = 0, i = 1, \cdots, m, h_j(\mathbf{x}) \le b_j, j = 1, \cdots, l.
$$

In general, the nonlinear constraints cannot be represented as

$$
\boldsymbol{Gx=0},\;\boldsymbol{Hx\le b}
$$

where $\mathbf{G} \in R^{m \times n}, \mathbf{b} \in R^{l \times 1}$, and $\mathbf{H} \in R^{l \times n}$. Naturally, the above representation is only suitable for linear constraints, not nonlinear constraints. These nonlinear constraints include x_j^2 or $x_ix_j (i \neq j)$ terms at least [\[2\]](#page-4-1). Du et al. have confused the representations for linear constraints and that for nonlinear constraints. Eventually, the Algorithm II is just a generalized version of Algorithm I, which is not suitable for the case of nonlinear constraints.

6 Conclusion

We show that the Du et al.'s outsourcing algorithms are flawed due to the simple translation transformation, and clarify that the algorithm for the case of nonlinear constraints is unsuitable. We also suggest a method to fix one algorithm. The findings in this note could be helpful for the future works on this topic.

References

- [1] W. Du, A. Li, Q. Li, P. Zhou: Privacy-Preserving and Secure Cloud Computing: A Case of Large-Scale Nonlinear Programming. IEEE Trans. Cloud Comput., 2023, 11(1), 484-498.
- [2] F. Hillier and G. Lieberman: Introduction to Operations Research, 11th Edition, McGraw Hill, 2021.