Further Optimization of Secure Logistic Regression Algorithm

Secure logistic regression algorithm in Textbox 2 reduces the ciphertext modulus to \( \log p \cdot \lfloor \log \deg (g) \rfloor + 3 \) + \( \lceil \log (n/\alpha) \rceil \) bits to update the encryption of \( \beta \) at each iteration. For the efficient implementation, we employ some techniques to reduce the number of consumed bits during the evaluation procedure. We express the evaluation circuit as follows:

\[
\beta \leftarrow \beta + (4\alpha n) \sum_{i=0}^{\lfloor \log (n/\alpha) \rfloor} (z_i/8) \cdot (2g(z_i^T \beta) - 1) \cdot (z_i/8). \tag{A-1}
\]

If the client generates encryptions of \( p \cdot (z_i/8) \) instead of \( p \cdot z_i \), the required bit length of ciphertext modulus per iteration can be reduced. On the other hand, the server uses a pre-computation step to reduce the complexity of the update equation: it performs AllSum procedure and applies the rescaling operation with the scale factor of \( \lfloor n/4\alpha \rfloor \) on \( ct.z_j \) for all \( j = 0, 1, \ldots, d \). As a result, we obtain a ciphertext \( ct.sum_j \) that encrypts an approximate value of \( (4\alpha p/2^n) \sum_{i=0}^{\lfloor \log (n/4\alpha) \rfloor} z_i^j \) in each plaintext slot. These ciphertexts will be stored during evaluation and used for updating the \( j \)-th component of weight vector \( \beta \). In particular, the ciphertexts \( ct.beta_0, \ldots, ct.beta_d \) corresponding to the entries of \( \beta \) become \( ct.sum_0, \ldots, ct.sum_d \) at the first iteration.

Figure S1 shows how to evaluate the arithmetic circuit \( (2g(z_i^T \beta) - 1) \cdot (z_i/8) \) when \( g(x) = g_3(x) \) or \( g(x) = g_7(x) \). We take encryptions of \( p \cdot \beta \) and \( p \cdot (z_i/8) \) as inputs of the algorithm to minimize the number of required multiplications and depth. Consequently, the proposed method reduces the ciphertext modulus by \( 3 \log p \cdot \lfloor \log (n/4\alpha) \rfloor \) bits or \( 4 \log p \cdot \lfloor \log (n/4\alpha) \rfloor \) bits when \( g(x) = g_3(x) \) or \( g(x) = g_7(x) \), respectively.

Figure S1. Evaluation procedure of least squares approximations \( (2g(z_i^T \beta) - 1) \cdot (z_i/8) \) when \( g(x)=g_3(x) \) (left) and \( g(x)=g_7(x) \) (right).