Supplementary Materials - *DynaMO*: Protecting Mobile DL Models through Coupling Obfuscated DL Operators

1 PROOF

Lemma 1.1. ***(Coupled Weight Transformation on Linear Model)***: *A sub-network f consists of multiple linear layers $\{L_1, L_2, \cdots, L_n\}$ and the i-th layer is $L_i : X_i = W_{i-1}^\top X_{i-1} + b_{i-1}$ where $i \in [1, n]$. The output of the sub-network f w.r.t. to the input X_0 would be $f(X_0)$. If W_1 is transformed to aW_1, W_n is transformed to $\frac{1}{a}W_n$, and b_i is transformed to ab_i for $i \in [1, n-1]$, then the transformed network f^s w.r.t. to the input X_0 would be $f^s(X_0)$ and we have $f^s(X_0) = f(X_0)$.*

Proof. Let us denote the scaled layer as L^s. For L^s_k where $k \in [1, n-1]$, we have

$$
\begin{aligned}
&X_1^s = aW_1^\top X_0 + ab_0 = aX_1 \\
&X_2^s = W_2^\top X_1^s + ab_1 = aW_2^\top X_1 + ab_1 = aX_2 \\
&\cdots \\
&X_{n-1}^s = W_{n-1}^\top X_{n-2}^s + ab_{n-1} = aW_{n-1}^\top X_{n-2} + +ab_{n-1} = aX_{n-1}.
\end{aligned} \tag{1}
$$

Then for L^s_n, we have $X^s_n = \frac{1}{a}W_n^\top X^s_{n-1} + ab_n = \frac{1}{a}W_n^\top (aX_{n-1}) + b_n = X_n$. Therefore, this gives us $f^s(X_0) = f(X_0)$. □

Theorem 1.2. ***(Coupled Weights Obfuscation)***: *We consider a general non-linear layer $ReLU_\beta(\beta \geq 0)$,* i.e.,

$$
ReLU_\beta(x) = \begin{cases} \beta, & if \quad x \geq \beta; \\ x, & else\ if \quad 0 < x < \beta; \\ 0, & otherwise. \end{cases}
$$

If W_i and b_i in the sub-network f are scaled to aW_i and ab_i for $i \in [1, n]$ with $0 < a < 1$, respectively, then, $ReLU_\beta(\frac{1}{a}I_{n+1}^\top ReLU_\beta(f^s(X_0))) = I_{n+1}^\top ReLU_\beta(f(X_0))$.

Proof. From Equation (1), we can conclude that $f^s(X_0) = aX_n$. Then, for the original sub-network f we have

$$
\mathrm{ReLU}_\beta(f(x_0)) = \mathrm{ReLU}_\beta(x_n) = \begin{cases} \beta, & \text{if} \quad x_n \geq \beta; \\ x_n, & \text{else if} \quad 0 < x_n < \beta; \\ 0, & \text{otherwise,} \end{cases} \tag{2}
$$

where x_0 and x_n are elements in X_0 and X_n, respectively. Thus,

$$
\mathrm{ReLU}_\beta\big(f(x_0)\big) = \begin{cases} \beta, & \text{if} \quad x_n \geq \beta; \\ x_n, & \text{else if} \quad 0 < x_n < \beta; \\ 0, & \text{otherwise.} \end{cases} \tag{3}
$$

Author's Contact Information:

Then, for the scaled sub-network f^s we have

$$\mathrm{ReLU}_\beta(f^s(x_0)) = \mathrm{ReLU}_\beta(ax_n) = \begin{cases} \beta, & \text{if} \quad x_n \geq \frac{\beta}{a}; \\ ax_n, & \text{else if} \quad 0 < x_n < \frac{\beta}{a}; \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

$$\frac{1}{a}\mathrm{ReLU}_\beta(ax_n) = \begin{cases} \frac{\beta}{a}, & \text{if} \quad x_n \geq \frac{\beta}{a}; \\ x_n, & \text{else if} \quad 0 < x_n < \frac{\beta}{a}; \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Note that $\frac{\beta}{a} > \beta$, thus,

$$\mathrm{ReLU}_\beta(\frac{1}{a}\mathrm{ReLU}_\beta\big(f^s(x_0)\big)) = \begin{cases} \beta, & \text{if} \quad x_n \geq \beta; \\ x_n, & \text{if} \quad 0 < x_n < \beta; \\ 0, & \text{otherwise.} \end{cases} \tag{6}$$

Therefore, we can conclude that $\forall x_0 \sim X_0$, the following holds: $\mathrm{ReLU}_\beta(\frac{1}{a}\mathrm{ReLU}_\beta\big(f^s(x_0)\big)) = \mathrm{ReLU}_\beta\big(f(x_0)\big)$. Thus, it follows that: $\mathrm{ReLU}_\beta(\frac{1}{a}\mathrm{ReLU}_\beta\big(f^s(X_0)\big)) = \mathrm{ReLU}_\beta\big(f(X_0)\big)$. Note that since the weights I_{n+1} forms an Identity matrix, the equation $\mathrm{ReLU}_\beta(\frac{1}{a}I_{n+1}^\top\mathrm{ReLU}_\beta\big(f^s(X_0)\big)) = I_{n+1}^\top\mathrm{ReLU}_\beta\big(f(X_0)\big)$ still holds. □