The 33rd Annual Conference of the Japanese Society for Artificial Intelligence, 2019

三層ニューラルネットワークにおけるRing-LWEベース準同型暗号を用いた効率的なプライバシー保護推論処理

Efficient Privacy-Preserving Prediction for Three-Layer Feedforward Neural Networks Using Ring-LWE-based Homomorphic Encryption

手塚 雄大 *1 (Takehiro Tezuka)　王 立華 *1,*2 (Lihua Wang)　林 卓也 *2 (Takuya Hayashi)　Kim Sangwook*1 (Sangwook Kim)　為井 智也 *1 (Tomoya Tamei)

大森 敏明 *1 (Toshiaki Omori)　小澤 誠一 *1 (Seiichi Ozawa)

*1神戸大学 Kobe University　*2国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

Concerns about privacy of data prevent from making good use of a huge amount of data. Data analysis while preserving privacy is a very important task. In this research, we propose a Privacy-Preserving Machine Learning that can efficiently compute inner product in a three-layered neural network using Ring-LWE-based Homomorphic Encryption. We propose a two-party model consisting of client and server: the former encrypts input data and receives a classification result from a server and the latter performs predicting process over the encrypted data using a trained classification model. This enables that the client acquires the inference result without revealing the privacy of their data and the server protects their model from exposing it. The proposed method costs 10.549 [ms] per one class for prediction process and performed keeping its accuracy close to the case of sigmoid and ReLU.

1. はじめに

近年，データの利活用が活発化される中で，複数の組織が持つ膨大なデータを統合し，利活用することで，新たなビジネスの創出や様々な社会問題の解決につなげることが期待されている．しかし，プライバシー保護やデータの機密性の確保が大きな壁となり，複数組織間でのデータ共有が問題解決につながっている事例は多くない．これに対して，データを秘匿化したまま解析するプライバシー保護データマイニングの技術が注目されている．また，データ分析には多様な知見やリソースが必要であり，分析モデルの公開は知的財産価値の喪失に繋がる．

そのような状況を踏まえて，Dowlin ら [Dowlin 16] は，学習済みの五層の畳み込みニューラルネットワークを暗号データに適用するモデルを構築した．Juvekar ら [Juvekar 18] は，暗号ライブラリ GAZELLE を作成し，garbled circuits を利用した四層ニューラルネットワークの予測モデルを構築した．

本研究では， Ring-LWE ベース準同型暗号を用いたプライバシー保護可能な三層ニューラルネットワーク (Privacy Preserving Three-Layer Feedforward Neural Networks : PP-TLFNNs) における効率的な推論処理を提案する．本稿では，入力層，中間層，出力層をそれぞれ一層ずつのニューラルネットワークを三層ニューラルネットワークと呼ぶことにする．提案手法では，学習済みモデルをもつサーバとサーバの持つモデルを用いて推論を行いたいクライアントの二者を考える．クライアントはデータを Ring-LWE ベースの準同型暗号により暗号化してサーバに暗号文を渡す．サーバは受け取った暗号データに対して学習済みの分類モデルを用いて推論処理を実行した後，推論結果が含まれる暗号文をクライアントに渡す．クライアントは受け取った暗号文を復号した値から対象データの推論結果を得る．ニューラルネットワークにおける活性化関数にはよく ReLU 関数や sigmoid 関数などが用いられるが，これらは有限次元の多項式で表すことはできない．したがって，提案手法では二次の多項式を用いて，中間層における非線形演算を乗法と加法の組み合わせのみで実現し，乗法性と加法性を備える準同型暗号での計算を可能とする．本研究では，データの Packing 方法の工夫により PP-TLFNNs の効率的な推論処理が可能となる．

本稿では，2 節で使用する準同型暗号について，3 節で準同型暗号を用いた三層ニューラルネットワークの効率的な順方向計算について述べる．4 節では推論に要する実時間性と分類精度の妥当性について評価し，5 節でまとめを述べる．

連絡先: 小澤 誠一，神戸大学数理･データサイエンスセンター，〒 657-8501 神戸市灘区六甲台町 1-1，TEL: 078-803-6466，E-MAIL: ozawasei@kobe-u.ac.jp

2. 準同型暗号

本研究では，準同型暗号として，Lauter ら [Lauter 11] により提案された Ring-LWE ベースの公開鍵準同型暗号方式を用いる．この方式を LNV-PHE（Public key Homomorphic Encryption）方式と呼ぶ. この方式は，加法準同型性と乗法準同型性を持つため，準同型内積演算ができる．

2.1 表記法

n を 2 のべき乗，$\mathcal{R} = \mathbb{Z}[x]/(x^n + 1)$ とする．Ring-LWE ベース暗号の平文空間を $\mathcal{R}_p = \mathcal{R}/p\mathcal{R} = \mathbb{Z}_p[x]/(x^n + 1)$，暗号文空間を $\mathcal{R}_q = \mathcal{R}/q\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$ とする．

整数 y と自然数 q に対して，$y - zq \in [-q/2, q/2)$ をみたす整数 z がただ一つに定まる．このとき，$[y]_q := y - zq$ とする．

同様に，多項式 $u = \sum_{i=0}^{n-1} u_i x^i \in \mathcal{R}$ に対して，$[u]_q := \sum_{i=0}^{n-1} [u_i]_q x^i$ とする．また，$u^{(t)}$ を以下のように定義する．

$$u^{(t)} := -\sum_{i=0}^{n-1} u_i x^{n-i} = u_0 - u_1 x^{n-1} - \cdots - u_{n-1} x.$$

ここで，[Wang 17b] より，任意の二つの多項式 $u, v \in \mathcal{R}$ に対して，次式が成り立つ．

$$(uv)^{(t)} = u^{(t)} v^{(t)}.$$

また，多項式 u の係数ベクトルを $\overline{u} := (u_0, ..., u_{n-1})$ で表す．

次元が等しいベクトル $\overline{u}$ と $\overline{v}=(v_0,...,v_{n-1})$ に対して，その内積を $\langle\overline{u},\overline{v}\rangle=\sum_{i=0}^{n-1}u_iv_i$ で定義する．

任意の有界な集合 $\mathcal{A}$ に対し，一様サンプリングを記号 $a\xleftarrow{\$}\mathcal{A}$ で表す．また，$f\xleftarrow{g}\mathcal{R}_{(0,s^2)}$ によって，各係数を独立に分散 s^2 の離散ガウス分布からサンプリングした多項式 $f\in\mathcal{R}$ を表す．

2.2 LNV-PHE 方式を用いた準同型内積演算

本稿では，公開鍵を pk，秘密鍵を sk とし，$c=(c_1,c_2),c'=(d_1,d_2)\in\mathcal{R}_q^2$ をそれぞれ平文 $m,m'\in\mathcal{R}_p$ の暗号文とする．

平文 m 及び暗号文 c に対する暗号化と復号化をそれぞれ $\mathsf{Enc}(pk,m)$，$\mathsf{Dec}(sk,c)$ とし，それらを以下のように定義する．

$$\mathsf{Enc}(pk,m)=(e_1a+pe_2,e_1P+pe_3+m)\in\mathcal{R}_q,$$
$$\mathsf{Dec}(sk,c)=[c_1S+c_2]_q \mod p\in\mathcal{R}_p.$$

ここで，$pk=(P,a),sk=S$．ただし，$r,S\xleftarrow{g}\mathcal{R}_{(0,s^2)}$, $a\xleftarrow{\$}\mathcal{R}_q$，$P=pr-aS\in\mathcal{R}_q$ であり，$e_1,e_2,e_3\xleftarrow{g}\mathcal{R}_{(0,s^2)}$ である．

上記の LNV-PHE 方式における加法 $(c_1+d_1,c_2+d_2)=\mathsf{Enc}(pk,m+m')$ と乗法 $(c_1m',c_2m')=\mathsf{Enc}(pk,mm')$ 準同型演算ができる．また，[Wang 17a] より以下の計算によって内積準同型演算を実現できる．内積準同型演算 $\mathsf{InnerP}(c,c')$ 及びその復号 $\mathsf{DecIP}(sk,ip)$ は下記の通りである．

$$ip_1=c_1^{(t)}d_1\in\mathcal{R}_q,$$
$$ip_2=c_1d_2^{(t)}+c_2^{(t)}d_1\in\mathcal{R}_q,$$
$$ip_3=(c_2^{(t)}d_2\in\mathcal{R}_q) \mod x\in\mathbb{Z}_q$$

とし，

$$\mathsf{InnerP}(c,c'):=(ip_1,ip_2,ip_3)=ip\in\mathcal{R}_q\times\mathcal{R}_q\times\mathbb{Z}_q.$$
$$\mathsf{DecIP}(sk,ip):=[(ip_1S^*+ip_2S) \mod x+ip_3]_q \mod p\in\mathbb{Z}_p.$$

ただし，$S^*=SS^{(t)}$ である．

3. 三層ニューラルネットワークにおける効率的なプライバシー保護推論処理 (PP-TLFNNs)

3.1 TLFNNs の順方向計算

入力次元を N, 中間層のノード数を L, クラス数を C とし，一層目の結合荷重を $W^{(1)}=\left(w_{ij}^{(1)}\right)_{N\times L}$，活性化関数を $g(x)=\alpha x^2+\beta x+\gamma$，二層目の結合荷重を $W^{(2)}=\left(w_{jk}^{(2)}\right)_{L\times C}$ とすると，TLFNNs の順方向計算による入力ベクトル $U=(u_1,...,u_N)$ に対する出力 $Z=(z_1,\ldots,z_C)$ は次式で表せる．

$$Z = g(U\cdot W^{(1)})\cdot W^{(2)}$$

したがって，各クラス $k=1,\ldots,C$ の出力値 z_k は活性化関数の各係数 α,β,γ について次のように整理できる．

$$\begin{aligned}z_k&=\sum_{j=1}^{L}g\left(\sum_{i=1}^{N}u_iw_{ij}^{(1)}\right)w_{jk}^{(2)}\\&=\alpha\sum_{j=1}^{L}(\sum_{i=1}^{N}u_iw_{ij}^{(1)})^2w_{jk}^{(2)}+\beta\sum_{j=1}^{L}(\sum_{i=1}^{N}u_iw_{ij}^{(1)}w_{jk}^{(2)})\\&\quad+\gamma\sum_{j=1}^{L}w_{jk}^{(2)}\\&:=z_k^{\alpha}+z_k^{\beta}+z_k^{\gamma},\end{aligned}$$

$j=1,...,L$ に対し，

$$A_j:=\sum_{i=1}^{N}u_iw_{ij}^{(1)}=\langle U,W_j^{(1)}\rangle$$
$$B_j^{[k]}:=\sum_{i=1}^{N}u_iw_{ij}^{(1)}w_{jk}^{(2)}=\langle U,W_j^{(1)}w_{jk}^{(2)}\rangle$$

とし，

$$A:=(A_1,...,A_j,...,A_L),\quad B^{[k]}:=(B_1^{[k]},...,B_j^{[k]},...,B_L^{[k]})$$

とすると，z_k^{α}, z_k^{β},z_k^{γ} はそれぞれ次のように書き直せる．

$$\begin{aligned}z_k^{\alpha}&:=\alpha\sum_{j=1}^{L}(\sum_{i=1}^{N}u_iw_{ij}^{(1)})^2w_{jk}^{(2)}\\&=\alpha\sum_{j=1}^{L}(\sum_{i=1}^{N}u_iw_{ij}^{(1)})(\sum_{i=1}^{N}u_iw_{ij}^{(1)}w_{jk}^{(2)})\\&=\alpha\sum_{j=1}^{L}A_jB_j^{[k]}=\alpha\langle A,B^{[k]}\rangle,\\z_k^{\beta}&:=\beta\sum_{j=1}^{L}(\sum_{i=1}^{N}u_iw_{ij}^{(1)}w_{jk}^{(2)})\\&=\beta\sum_{j=1}^{L}B_j^{[k]}=\beta\langle\mathbf{1},B^{[k]}\rangle,\\z_k^{\gamma}&:=\gamma\sum_{j=1}^{L}w_{jk}^{(2)}.\end{aligned}$$

3.2 Packing 方法

ベクトル $V=(v_1,...,v_N)$ に対して，Packing を下記のように定義する．

$$\mathsf{Poly}_1(V) := \sum_{i=1}^{N}v_ix^{i-1} \tag{1}$$

$$\mathsf{Poly}_2(V) := \sum_{i=1}^{N}v_ix^{(i-1)N} \tag{2}$$

式 (1), (2) を用いると，ベクトル $U=(u_1,...,u_N),W_j^{(1)}=\left(w_{1j}^{(1)},\ldots,w_{Nj}^{(1)}\right)$ 及び $W_j^{(2)}=\left(w_{2j}^{(2)},\ldots,w_{Lj}^{(2)}\right)$ に対して

$$\begin{aligned}V_{A_j}(x)&:=\mathsf{Poly}_1(U)(\mathsf{Poly}_1(W_j^{(1)}))^{(t)}\\&=A_j+\sum_{j=1}^{\lfloor n/N\rfloor}(0\cdot x^{jN})+[\text{other terms}],\\V_{B_j^{[k]}}(x)&:=\mathsf{Poly}_2(U)(\mathsf{Poly}_2(W_j^{(1)}w_{jk}^{(2)}))^{(t)}\\&=B_j^{[k]}+\sum_{j=0}^{\lfloor n/N\rfloor}\sum_{k=1}^{N-1}(0\cdot x^{k+jN})+[\text{other terms}]\end{aligned}$$

となり，$V_{A_j}(x),V_{B_j^{[k]}}(x)$ それぞれの定数項に $A_j,B_j^{[k]}$ が現れる．また，$V_{A_j}(x)$ と $V_{B_j^{[k]}}(x)$ の係数ベクトル $\overline{V_{A_j}(x)}$ と $\overline{V_{B_j^{[k]}}(x)}$ の内積は以下のようになる．

$$\langle\overline{V_{A_{[j]}}(x)},\overline{V_{B_{[j]}^{[k]}}(x)}\rangle=A_jB_j^{[k]}. \tag{3}$$

3.3 暗号文を用いた TLFNNs の順方向計算

暗号文 $\mathsf{Enc}(\mathsf{Poly}_1(U)) = (c_1, c_2), \mathsf{Enc}(\mathsf{Poly}_2(U)) = (d_1, d_2)$ に対して，下記の準同型計算を行うと，$V_{A_j}(x)$ と $V_{B_j^{[k]}}(x)$ の暗号文を求めることができる．

$$\begin{aligned}(\widehat{c_{1,[j]}}, \widehat{c_{2,[j]}}) &:= \left(c_1(\mathsf{Poly}_1(W_j^{(1)}))^{(t)}, c_2(\mathsf{Poly}_1(W_j^{(1)}))^{(t)}\right)\\ &= \mathsf{Enc}(\mathsf{Poly}_1(U)(\mathsf{Poly}_1(W_j^{(1)}))^{(t)})\\ &= \mathsf{Enc}(V_{A_j}(x)),\\ (\widehat{d_{1,[j]}^{[k]}}, \widehat{d_{2,[j]}^{[k]}}) &:= \left(d_1(\mathsf{Poly}_2(W_j^{(1)}))^{(t)} w_{jk}^{(2)}, d_2(\mathsf{Poly}_2(W_j^{(1)}))^{(t)} w_{jk}^{(2)}\right)\\ &= \mathsf{Enc}(\mathsf{Poly}_2(U)(\mathsf{Poly}_2(W_j^{(1)} w_{jk}^{(2)}))^{(t)})\\ &= \mathsf{Enc}(V_{B_j^{[k]}}(x)).\end{aligned}$$

したがって，式 (3) 及び [Wang 17a] より $A_j B_j^{[k]}$ は $(\widehat{c_{1,[j]}}, \widehat{c_{2,[j]}}), (\widehat{d_{1,[j]}^{[k]}}, \widehat{d_{2,[j]}^{[k]}})$ を用いて内積準同型演算で計算でき，また，加法準同型性より $z_k^{\alpha} = \alpha\langle A, B^{[k]}\rangle = \alpha\sum_{j=1}^{L} A_j B_j^{[k]}$ に対応する暗号文は下記のようにして計算できる．

$$\begin{aligned}ip_{\alpha}^{[k]} &= \alpha \sum_{j=1}^{L} \mathsf{InnerP}((\widehat{c_{1,[j]}}, \widehat{c_{2,[j]}}), (\widehat{d_{1,[j]}^{[k]}}, \widehat{d_{2,[j]}^{[k]}}))\\ &:= (ip_{\alpha,1}^{[k]}, ip_{\alpha,2}^{[k]}, ip_{\alpha,3}^{[k]}).\end{aligned}$$

ただし，

$$\begin{aligned}ip_{\alpha,1}^{[k]} &= \alpha \sum_{j=1}^{L} \widehat{c_{1,[j]}}^{(t)} \widehat{d_{1,[j]}^{[k]}} \in \mathcal{R}_q,\\ ip_{\alpha,2}^{[k]} &= \alpha \sum_{j=1}^{L} \left(\widehat{c_{2,[j]}}^{(t)} \widehat{d_{1,[j]}^{[k]}} + \widehat{c_{1,[j]}} \widehat{d_{2,[j]}^{[k]}}^{(t)}\right) \in \mathcal{R}_q,\\ ip_{\alpha,3}^{[k]} &= (\alpha \sum_{j=1}^{L} \widehat{c_{2,[j]}}^{(t)} \widehat{d_{2,[j]}^{[k]}} \bmod x) \in \mathbb{Z}_q.\end{aligned}$$

一方，$B_j^{[k]} = \langle (1, 0, ..., 0), \overline{V_{B_{[j]}^{[k]}}(x)}\rangle$ であるため，$z_k^{\beta} = \beta\sum_{j=1}^{L} B_j^{[k]}$ の暗号文は下記で計算できる．

$$ip_{\beta}^{[k]} = (0, ip_{\beta,2}^{[k]}, ip_{\beta,3}^{[k]})$$

ただし，

$$\begin{aligned}ip_{\beta,2}^{[k]} &= \beta \sum_{j=1}^{L} \widehat{d_{1,[j]}^{[k]}} \in \mathcal{R}_q,\\ ip_{\beta,3}^{[k]} &= (\beta \sum_{j=1}^{L} \widehat{d_{2,[j]}^{[k]}} \bmod x) \in \mathbb{Z}_q.\end{aligned}$$

また，

$$ip_{\gamma}^{[k]} = (0, 0, z_{\gamma}^{[k]}).$$

したがって，$z_k = z_k^{\alpha} + z_k^{\beta} + z_k^{\gamma}$ の結果を含む暗号文は

$$ip^{[k]} = ip_{\alpha}^{[k]} + ip_{\beta}^{[k]} + ip_{\gamma}^{[k]} := (ip_1^{[k]}, ip_2^{[k]}, ip_3^{[k]}).$$

により求められる．ただし，

$$\begin{aligned}ip_1^{[k]} &= ip_{\alpha,1}^{[k]} \in \mathcal{R}_q,\\ ip_2^{[k]} &= ip_{\alpha,2}^{[k]} + ip_{\beta,2}^{[k]} \in \mathcal{R}_q,\\ ip_3^{[k]} &= ip_{\alpha,3}^{[k]} + ip_{\beta,3}^{[k]} + z_k^{\gamma} \in \mathbb{Z}_q.\end{aligned}$$

3.4 スキーム

本節では，プライバシー保護可能な推論処理のスキームを 5 つの Step に分けて説明する．ただし，$\mathbb{Z}[x]/(x^n + 1)$ の次数 n は，入力ベクトルの次元 N に対して $n \geq N^2$ とする．

Step-0 サーバは $k = 1, ..., C$ に対して，事前に

$$\begin{aligned}\widetilde{\mathsf{Poly}_{\alpha}^{[k]}} &= \alpha \sum_{j=1}^{L} \mathsf{Poly}_1(W_j^{(1)}) \mathsf{Poly}_2(W_j^{(1)})^{(t)} w_{jk}^{(2)},\\ \widetilde{\mathsf{Poly}_{\beta}^{[k]}} &= \beta \sum_{j=1}^{L} \mathsf{Poly}_2(W_j^{(1)})^{(t)} w_{jk}^{(2)},\end{aligned}$$

及び $z_k^{\gamma} = \gamma\sum_{j=1}^{L} w_{jk}^{(2)}$ を計算しておく．

Step-1 クライアントは自分のデータ U を方式 (1), (2) を用いてエンコードし，下記のように暗号化してからサーバへ送る．

$$\begin{aligned}\mathsf{Enc}(pk, \mathsf{Poly}_1(U)) &= (c_1, c_2),\\ \mathsf{Enc}(pk, \mathsf{Poly}_2(U)) &= (d_1, d_2).\end{aligned}$$

Step-2 サーバは (c_1, c_2) と (d_1, d_2) を受け取ったら，下記の準同型計算を行い，

$$\begin{aligned}ip_1^{[k]} &= c_1^{(t)} d_1 \widetilde{\mathsf{Poly}_{\alpha}^{[k]}} \in \mathcal{R}_q,\\ ip_2^{[k]} &= d_1 \left(c_2^{(t)} \widetilde{\mathsf{Poly}_{\alpha}^{[k]}} + \widetilde{\mathsf{Poly}_{\beta}^{[k]}}\right) + c_1 d_2^{(t)} \widetilde{\mathsf{Poly}_{\alpha}^{[k]}}^{(t)} \in \mathcal{R}_q,\\ ip_3^{[k]} &= (d_2 \left(c_2^{(t)} \widetilde{\mathsf{Poly}_{\alpha}^{[k]}} + \widetilde{\mathsf{Poly}_{\beta}^{[k]}}\right) + z_k^{\gamma} \bmod x) \in \mathbb{Z}_q.\end{aligned}$$

結果 $ip^{[k]} := (ip_1^{[k]}, ip_2^{[k]}, ip_3^{[k]}) \in \mathcal{R}_q \times \mathcal{R}_q \times \mathbb{Z}_q, k = 1, 2, ..., C$ をクライアントに渡す．

Step-3 クライアントはサーバから受け取った結果を復号する．

$$\mathsf{DecIP}(sk, ip^{[k]}) = z_k \quad (k = 1, ..., C).$$

Step-4 クライアントは $\{z_k\}$ の最大値

$$z_{k^*} = \max_{k \in \{1,...,C\}} \{z_k\}$$

を求め，データ U をクラス k^* に分類する．

4. 実験

4.1 速度評価

3.4 節における各 Step の処理時間のベンチマークを測定した結果を表 1 に示す．計測は Core i7-7700K(4.20 GHz) のシングルスレッドで行った．実装には次のパラメータを用いた．

$$\begin{aligned}p &= 32749 \times 32719 \times 32717 \times 32713\\ q &= 2^{96} - 2^{32} + 1\\ n &= 4096, \quad s = 8.0\end{aligned}$$

平文は $p_i \in \{32749, 32719, 32717, 32713\}$ それぞれについて暗号化，計算を行い，復号時に中国剰余定理で p に持ち上げることで高速化を行った．また，実数値は 2^{16} を掛けて床関数により整数化を行った．

表 1: 各 Step の処理時間 (C : クラス数)

処理	時間 [ms]
事前計算 (Step-0)*1	$2747.336 \times C$
暗号化 (Step-1)	8.561
PP-TLFNNs の順方向計算 (Step-2)	$10.549 \times C$
復号 (Step-3)	$0.332 \times C$

表 2: 使用するデータセット

	データ数	特徴量数	クラス数
Satellite	6435	36	6
Australian	690	14	2
German	1000	20	2

Step-0 の事前計算は，モデルを製作した時点でサーバがあらかじめ計算しておく処理であり，クライアントとサーバ間での処理時間に直接的に影響を及ぼさないため，処理速度の実用性の評価はその他の結果から行うこととする．暗号化ではクラス数に依存せず， PP-TLFNNs の順方向計算および復号にかかる時間はクラス数に依存する．Satellite データセットであれば $C = 6$ であるため，順方向計算に 63.294 [ms]，復号に 1.992[ms] で処理できる．これらの結果から，処理速度は十分実用的であると言える．

4.2 精度評価

分類精度の評価には，UCI Machine Learning Repository [Dua 17] にて公開されている 3 つのデータセット Satellite : Statlog (Landsat Satellite) Data Set，Australian : Statlog (Australian Credit Approval) Data Set，German : Statlog (German Credit Data) Data Set を使用した．それぞれのデータセットに関する情報を表 2 に示す．また，これらのデータセットを使用するにあたって，前処理として各データそれぞれで平均が 0, 分散が 1 となるように正規化を行った．中間層の活性化関数には ReLU 関数を二次の多項式により近似したものを用いた．ここで，ReLU 関数の近似は学習過程で中間層に入力された最大値と最小値を含む $[-30, 30]$ の範囲で最小二乗法により行った．

モデルの学習では確率的勾配降下法により学習を行った．そして，求めた結合荷重を提案手法の推論処理で使用した．

本稿の実験では 5 分割の交差検定を行い，分類精度を評価した．中間層の活性化関数に Sigmoid 関数，ReLU 関数を用いた場合と二次関数を用いた PP-TLFNNs の分類精度を表 3 に示す．

表 3 の結果から，PP-TLFNNs は Sigmoid 関数や ReLU 関数を用いた TLFNNs に対して，近い精度で推論処理を行えたことがわかる．

5. まとめ

近年，データのプライバシーに対する懸念が，データの利活用の活発化への大きな障壁となっていた．それにより，複数組織が膨大なデータを所有していても，それらをより効果的に利用することが困難な問題があった．そのような状況に対して，データのプライバシーを保護した状態で解析を行える技術が求められている．そこで，本研究ではデータを暗号化した状態で推論処理を行えるモデルを構築した．

*1 実装では漸近的に高速なアルゴリズムを使用していないため，高速化の余地は残っている．

表 3: 分類精度の比較．PP-TLFNNs は暗号文実装のモデル，TLFNNs は平文実装のモデルを指す．

中間層における活性化関数	PP-TLFNNs	TLFNNs	
	二次関数	Sigmoid 関数	ReLU 関数
Satellite	0.871 ± 0.016	0.899 ± 0.027	0.900 ± 0.023
Australian	0.857 ± 0.041	0.875 ± 0.028	0.875 ± 0.039
German	0.741 ± 0.020	0.774 ± 0.026	0.778 ± 0.036

本稿では，準同型暗号を用いた三層ニューラルネットワークにおいて，Packing 方法の工夫により効率的な推論処理を提案した．速度評価では，それぞれの処理を実用的な時間で実現することを示した．また，精度評価では二次関数を用いたことによる精度の低下は見られたが，依然として高い精度で分類できることを示した．これにより，複数組織がデータの情報を漏らすことなく，それぞれのデータを解析することが可能となり，さらなるデータ利活用の促進が期待できる．

今後は活性化関数の近似手法の改良や暗号方式の工夫によるネットワーク構造の拡張等による分類精度の向上，さらには実データへの適用を目指したい．

謝辞

本研究の成果は JST CREST 研究領域「イノベーション創発に資する人工知能基盤技術の創出と統合化」研究課題「複数組織データ利活用を促進するプライバシー保護データマイニング」JST CREST JPMJCR168A，JSPS 科研費 JP15K00028 の助成を受けて得られたものです．

参考文献

[Dowlin 16] Dowlin, N., Gilad-Bachrach, R., Laine, K., Lauter, K., Naehrig, M. and Wernsing, J.: Cryptonets: Applying neural networks to encrypted data with high throughput and accuracyrq, *ICML 2016*, pp. 201-210 (2016)

[Juvekar 18] Juvekar, C., Vaikuntanathan, V. and Chandrakasan, A.: GAZELLE: A low latency framework for secure neural network inference, *Usenix Security 2018,* pp. 1651–1669 (2018).

[Lauter 11] Naehrig, M., Lauter, K. and Vaikuntanathan, V.: Can homomorphic encryption be practical?, *CCSW'11*, pp. 113–124 (2011).

[Wang 17a] Wang, L., Hayashi, T., Aono, Y. and Phong., L. T.: A generic yet efficient method for secure inner product., *NSS 2017, LNCS 10394*, pp. 217–232 (2017).

[Wang 17b] Wang, L., Aono, Y. and Phong, L. T.: A new secure matrix multiplication from Ring-LWE., *CANS 2017, LNCS 11261*, pp. 93–111 (2017).

[Dua 17] Dua, D. and Taniskidou, E.K.: UCI Machine Learning Repository, `http://archive.ics.uci.edu/ml`, (2017)