边缘协同的轻量级隐私保护分类框架

熊金波[1,2,3]，周永洁[1,4]，毕仁万[2]，万良[1]，田有亮[1,3,4]

（1. 贵州大学计算机科学与技术学院，贵州 贵阳 550025；2. 福建师范大学计算机与网络空间安全学院，福建 福州 350117；
3. 贵州省公共大数据重点实验室，贵州 贵阳 550025；4. 贵州大学密码学与数据安全研究所，贵州 贵阳 550025）

摘 要：针对边端计算环境下存在感知图像数据泄露与隐私保护分类框架计算低效的问题，提出一种边缘协同的轻量级隐私保护分类框架（PPCF），该框架支持加密特征提取和分类，在边缘节点协同分类过程中实现对数据传输和计算过程的隐私保护。首先，基于加性秘密共享技术设计一系列安全计算协议；在此基础上，两台非共谋的边缘服务器协同执行安全卷积、安全批量归一化、安全激活、安全池化等深度神经网络计算层以实现 PPCF。理论与安全性分析证明了 PPCF 的正确性和安全性，性能评估结果显示，PPCF 可达到与明文环境等同的分类精度；与同态加密和多轮迭代计算方案相比，PPCF 在计算开销和通信开销方面具有明显优势。

关键词：边缘协同；隐私保护目标分类；加性秘密共享；深度神经网络；安全计算协议
中图分类号：TN309
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022004

Towards edge-collaborative, lightweight and privacy-preserving classification framework

XIONG Jinbo[1,2,3], ZHOU Yongjie[1,4], BI Renwan[2], WAN Liang[1], TIAN Youliang[1,3,4]

1. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
2. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
3. State Key Laboratory of Public Big Date, Guiyang 550025, China
4. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China

Abstract: Aiming at the problems of data leakage of perceptual image and computational inefficiency of privacy-preserving classification framework in edge-side computing environment, a lightweight and privacy-preserving classification framework (PPCF) was proposed to supports encryption feature extraction and classification, and achieve the goal of data transmission and computing security under the collaborative classification process of edge nodes. Firstly, a series of secure computing protocols were designed based on additive secret sharing. Furthermore, two non-collusive edge servers were used to perform secure convolution, secure batch normalization, secure activation, secure pooling and other deep neural network computing layers to realize PPCF. Theoretical and security analysis indicate that PPCF has excellent accuracy and proved to be security. Actual performance evaluation show that PPCF can achieve the same classification accuracy as plaintext environment. At the same time, compared with homomorphic encryption and multi-round iterative calculation schemes, PPCF has obvious advantages in terms of computational cost and communication overhead.

Keywords: edge-collaborative, privacy-preserving object classification, additive secret sharing, deep neural network, secure computing protocol

收稿日期：2021−09−18；**修回日期**：2021−12−15

通信作者：万良，wangliangtr@163.com

基金项目：国家自然科学基金资助项目（No.61872090，No.61872088，No.U1836205，No.61772008）；贵州省科技重大专项计划基金资助项目（No.20183001）；福建省自然科学基金资助项目（No.2019J01276）；贵州省科技计划基金资助项目（黔科合基础[2019]1098）；贵州省高层次创新型人才基金资助项目（黔科合平台人才[2020]6008）；贵阳市科技计划基金资助项目（筑科合[2021]1-5）

Foundation Items: The National Natural Science Foundation of China (No.61872090，No.61872088，No.U1836205，No.61772008), Science and Technology Major Support Program of Guizhou Province (No.20183001), The Natural Science Foundation of Fujian Province (No.2019J01276), Key Program of The National Natural Science Union Foundation of China (No.U1836205), Science and Technology Program of Guizhou Province (No.[2019]1098), Project of High-level Innovative Talents of Guizhou Province (No. [2020]6008), Science and Technology Program of Guiyang Province (No.[2021]1-5)

0 引言

近年来，以卷积神经网络（CNN, convolutional neural network）为代表的深度计算模型备受关注，常用于图像处理和计算机视觉等任务[1]。在自动驾驶应用中，CNN 还可用于动态障碍物分类和检测，使自动驾驶车辆对周围环境做出正确反应[2-3]。随着 CNN 研究的深入，需要传输和处理的感知数据呈爆炸式增长[4]，目标分类和检测等复杂的计算任务需要巨大的计算资源来支撑，同时给复杂多变的网络环境带来了时延。因此，将资源密集型的计算任务卸载至边缘节点[5]，整个过程可使移动终端节省计算通信资源。但是，在边缘环境执行 CNN 训练和推理计算时，边缘节点是半可信的，当边缘通道存在恶意攻击者时，CNN 的计算过程和计算结果面临着泄露风险。因此，神经网络在边缘节点协同计算过程中的隐私安全问题尤为重要[4]，同时保证计算的正确性和效率也是本文的目标。

目前，已有学者把 CNN 模型应用在边缘计算中。Yang 等[6]提出基于边缘的 EdgeCNN 和 EdgeCNN-G 模型，两者可以在边缘设备上协同执行深度学习任务，而且后者可以支持群卷积计算。Wang 等[7]针对云边缘计算环境提出一种基于 CNN 的零件模型视觉分类系统，以高性能和低时延方式实现了高效率的零件分类。Wong 等[8]提出一种人机结合方法以实现新的深度神经网络 AttoNets，该网络支持边缘设备执行边缘深度学习，在大大降低计算开销和参数量情况下，具备较高的准确率。

就神经网络隐私计算目标而言，大多数学者采用同态加密构建密态神经网络模型。Hesamifard 等[9]使用同态加密训练神经网络模型，采用低次多项式逼近激活函数，但是该方案计算开销较大，时延较高。Gilad-Bachrach 等[10]提出基于全同态加密的隐私保护神经网络模型，采用平方函数近似替代激活函数，但是该模型仅能实现小型的 CNN 密态神经网络。Chou 等[11]提出一种更高效的密态网络，利用同态加密稀疏地表示网络参数。为了克服上述密态模型仅能支持 CPU 设置的局限性，Al-Badawi 等[12]提出了兼容 GPU 设置的同态加密神经网络模型，有效提高了模型的运算速度。Zhang 等[13]提出一种新颖的隐私保护深度网络模型，将昂贵的计算任务都卸载至云服务器，并支持密态网络训练。然而，同态加密需要消耗大量的加密开销，不适合实时性敏感的物联网应用。

此外，在神经网络隐私计算中，混淆电路、秘密共享、不经意传输等方案也受到研究学者的关注。Rouhani 等[14]提出第一个可证明安全的框架，并采用混淆电路对密态网络做预测，实现了较低的开销。Liu 等[15]基于不经意传输提出一种隐私保护分类模型，对密态网络的计算分为在线和离线阶段，并把基于加性秘密共享设计的乘法协议应用到神经网络。Riazi 等[16]提出混合安全多方计算框架，采用加性秘密共享技术计算线性层，混淆电路等协议计算非线性层，大大提升了计算效率，但同样存在较高的计算开销问题。由于计算密集型的加密算法会降低 CNN 模型的利用效率，Huang 等[17]提出一种基于边缘计算的轻量级特征提取框架，通过加性秘密共享设计一系列安全子协议并外包给两台边缘服务器和一个可信第三方协同执行隐私计算，实现了较高的计算效率，然而，运用符号进位加法计算的修正线性单元（ReLU, rectified linear unit）耗费大量的开销，不适于神经网络的深度计算任务。熊金波等[18]基于加性秘密共享技术提出针对边缘环境下的轻量级安全区域建议网络，与同态加密、多轮迭代逼近和符号进位加法等方法相比，该方法更高效。Wagh 等[19]提出安全三方计算网络 SecureNN，利用布尔计算非线性函数，带来了较低的通信开销，此外，该网络能支持恶意敌手。Wagh 等[20]进一步提升 SecureNN 的安全协议性能，并且设计了更多的非线性协议，但多轮迭代逼近方案耗费大量的计算开销。

针对于边缘环境下的感知图像数据泄露和当前隐私保护分类框架效率优化问题，本文考虑到网联自动驾驶应用场景，选择经典且较深的分类 CNN，即残差神经网络（ResNet, residual neural network）[21]执行训练推理，设计并实现一种边缘协同的轻量级隐私保护分类框架（PPCF, lightweight and privacy-preserving classification framework）。本文采用两台不共谋的边缘服务器使用一系列安全计算协议来协同支持加密特征的提取和分类任务，用户不需要始终在线与服务器协同计算参数以承担较多的通信开销压力，而且与以往均针对三方或多方的秘密共享方案相比，降低了通信和带宽资源。本文贡献如下。

1) 基于加性秘密共享技术设计通用的安全卷积（SConv, secure convolution）、安全批量归一化

（SBN, secure batch normalization）、安全激活（SRU6, secure ReLU6）、安全全局平均池化（SGAP, secure global average pooling）和安全全连接（SFC, secure fully connected），以上安全计算协议的计算复杂度与明文环境下的网络层函数同阶，而且通信复杂度控制在常数轮，与同态加密和多轮迭代方案相比，其在计算和通信开销方面具有明显优势。

2) 基于经典的 ResNet 设计并实现一种边缘协同的轻量级 PPCF，用户不需要与服务器在线协作，两台边缘服务器可以实现端对端的隐私保护目标分类任务，而且不需要中间过程解密或者恢复计算结果。此外，PPCF 可以同时保护模型参数、用户数据和推理结果。

3) 理论分析和性能评价结果表明，PPCF 能够实现目标分类的正确性和安全性，而且计算误差在 1×10^{-4} 内，可达到与明文环境同等的分类精度，能维持安全和效率之间的平衡。

1　预备知识

1.1　ResNet

ResNet[21]是深度残差学习网络，比普通 CNN 增加了残差块和批量归一化（BN, batch normalization）设计。残差块运用映射跨层连接的思想，使某一层的输出直接跨过几层作为某层的输入，解决网络变深带来的准确率下降问题。在图 1 中，x 表示输入，$H(x)=f_{(x)}+x$ 表示输出。当 $f_{(x)}=0$ 时，$H(x)=x$，该过程不会产生额外参数，也不会增加计算复杂度。同时，学习目标变成学习 $H(x)-x$ 的差值，使残差网络 $f_{(x)}$ 逼近于零，不再是学习一个完整的输出。

训练 CNN 比较困难，使它们在合理时间内收敛更难，BN 最重要的作用是加速深层网络的收敛和融合，其原理如图 2 所示，使训练数据集满足均值为 0、方差为 1 的分布规律，其中，n 表示深度，b 表示高度。在 ResNet 的训练阶段，网络不断地计算每一批训练数据的均值和方差，最终把计算得到的整个数据集均值和方差运用在推理阶段做预测。批量归一化操作为

$$\mathrm{BN}(x)=\gamma\frac{x-\hat{\mu}_B}{\hat{\sigma}_B}+\beta,\quad x\in B \tag{1}$$

$$\hat{\mu}_B=\frac{1}{|B|}\sum_{x\in B}x \tag{2}$$

$$\hat{\sigma}_B^2=\frac{1}{|B|}\sum_{x\in B}(x-\hat{\mu}_B)^2+\varepsilon \tag{3}$$

其中，$\hat{\mu}_B$ 是均值，$\hat{\sigma}_B$ 是标准差，γ 和 β 是学习到的参数。防止分母为 0，加上一个接近于 0 的正数 ε。

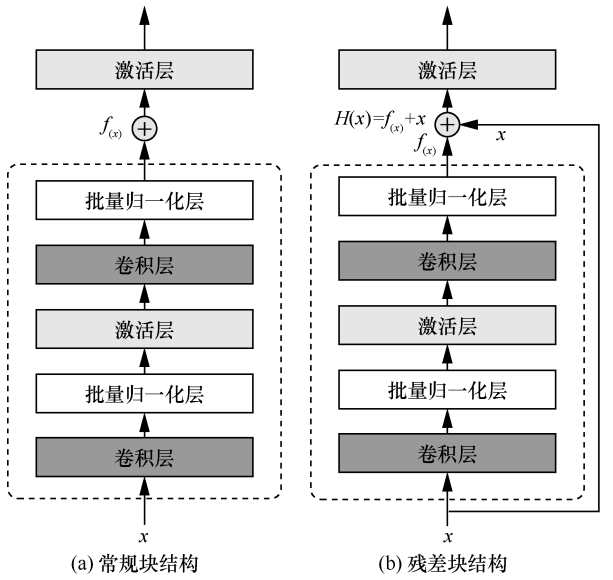


图 1　常规块和残差块结构

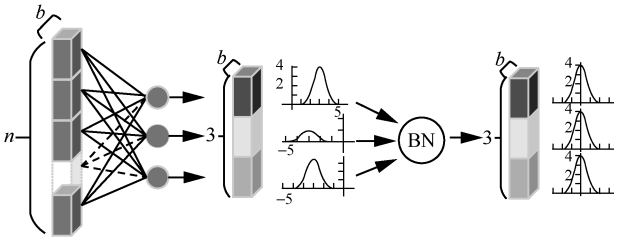


图 2　BN 原理

1.2　基本安全计算协议

相对于计算复杂的同态加密原语，加性秘密共享[22]不再局限于秘钥管理，能更好地保护秘密的完整性和安全性。一般地，受信任方将秘密拆分成 n 份子秘密，分别给 n 个参与者持有，并规定不少于 $k(k\leqslant n)$ 的参与者可以重构秘密，以及哪些参与者不能重构得到关于秘密的任何信息。其中，秘密分发者将秘密随机分发，秘密的保存者通过加法运算就能重构秘密。首先，用户把输入图像 x 像素级地随机拆分为 x_1 和 x_2，满足 $x=x_1+x_2$，分别发至两台边缘服务器 S_1 和 S_2，S_1 和 S_2 协同对 x_1 和 x_2 执行目标分类任务。在毕仁万等[23]的工作中，基于加性秘密共享技术提出了 7 种安全的子协议，以下协议采用固定点数计算，随机选择 $\kappa_1'\in\mathbb{Z}_n$，n 为素数，得到另一分量 $\kappa_2'=\kappa'-\kappa_1'$，描述如下。

安全乘法−加法转换（STMA, secure transforming multiply-add）协议[23]。S_1 拥有 $u_1 \in \mathbb{Z}_n$，S_2 拥有 $u_2 \in \mathbb{Z}_n$，S_1 和 S_2 协同执行 $f_1, f_2 \leftarrow \text{STMA}(u_1, u_2)$，满足 $f_1 + f_2 = u_1 u_2$。

安全加法−乘法转换（STAM, secure transforming add-multiply）协议[23]。S_1 拥有 $u_1' \in \mathbb{Z}_n$，S_2 拥有 $u_2' \in \mathbb{Z}_n$，S_1 和 S_2 协同执行 $f_1', f_2' \leftarrow \text{STAM}(u_1', u_2')$，满足 $f_1' f_2' = u_1' + u_2'$。

安全乘法（SMul, secure multiplication）协议[23]。S_1 拥有 $\overline{u}_1, v_1 \in \mathbb{Z}_n$，$S_2$ 拥有 $\overline{u}_2, v_2 \in \mathbb{Z}_n$，$S_1$ 和 S_2 协同执行 $f_1'', f_2'' \leftarrow \text{SMul}(\overline{u}_1, \overline{u}_2, v_1, v_2)$，满足 $f_1'' + f_2'' = (\overline{u}_1 + \overline{u}_2) \cdot (v_1 + v_2)$。

安全点乘（SecDotMul, secure dot multiplication）协议[24]。S_1 拥有 $\hat{u}_1, \hat{v}_1 \in \mathbb{Z}_n$，$S_2$ 拥有 $\hat{u}_2, \hat{v}_2 \in \mathbb{Z}_n$，$S_1$ 和 S_2 协同执行 $\hat{f}_1, \hat{f}_2 \leftarrow \text{SecDotMul}(\hat{u}_1, \hat{u}_2, \hat{v}_1, \hat{v}_2)$，满足 $\hat{f}_1 + \hat{f}_2 = (\hat{u}_1 + \hat{u}_2)(\hat{v}_1 + \hat{v}_2)$。

安全平方根（SSqr, secure square root）协议[23]。S_1 拥有 $v_1' \in \mathbb{Z}_n$，S_2 拥有 $v_2' \in \mathbb{Z}_n$，S_1 和 S_2 协同执行 $\overline{f}_1, \overline{f}_2 \leftarrow \text{SSqr}(v_1', v_2')$，满足 $\overline{f}_1 + \overline{f}_2 = (v_1' + v_2')^{0.5}$。

安全除法（SDiv, secure division calculation）协议[23]。S_1 拥有 $x_1', y_1' \in \mathbb{Z}_n$，$S_2$ 拥有 $x_2', y_2' \in \mathbb{Z}_n$，$S_1$ 和 S_2 协同执行 $Y_1, Y_2 \leftarrow \text{SDiv}(x_1', x_2', y_1', y_2')$，满足 $Y_1 + Y_2 = \dfrac{x_1' + x_2'}{y_1' + y_2'}$。

安全比较（SComp, secure comparison）协议[23]。S_1 拥有 $x_1'', y_1'' \in \mathbb{Z}_n$，$S_2$ 拥有 $x_2'', y_2'' \in \mathbb{Z}_n$，$S_1$ 和 S_2 协同执行 $\tilde{f} \leftarrow \text{SComp}(x_1'', x_2'', y_1'', y_2'')$，$\tilde{f}$ 表示符号位，若 $(x_1'' + x_2'') \geqslant (y_1'' + y_2'')$，$\tilde{f} = 0$；若 $(x_1'' + x_2'') < (y_1'' + y_2'')$，$\tilde{f} = 1$。

2 模型定义

2.1 系统模型

本文旨在解决感知图像数据在信道传输、边缘节点分类过程和分类后结果的隐私安全问题，并尽可能减少计算和通信开销。系统模型如图 3 所示，4 种不同类型的参与者组成 PPCF，即发送端 C、接收端 Q、两台边缘服务器 S_1 和 S_2 及可信第三方服务器 T。

1) C 通过移动传感器采集到海量的图像数据，将图像随机拆分为 2 个图像分量 I_1 和 I_2，该过程可视作图像加密，然后与模型明文训练下的 $\hat{w}_1, \hat{w}_2$ 和 $\hat{\mu}_1, \hat{\mu}_2$ 等网络参数一并提交给 S_1 和 S_2，满足 $I = I_1 + I_2$，$\hat{w} = \hat{w}_1 + \hat{w}_2$，$\hat{\mu} = \hat{\mu}_1 + \hat{\mu}_2$。

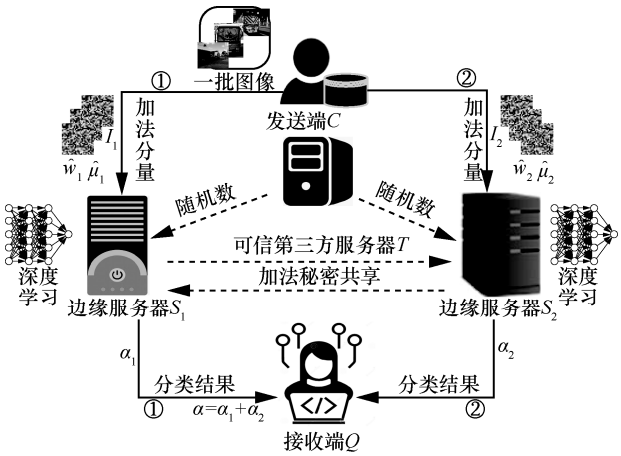


图 3 系统模型

2) T 负责离线生成随机数，并分配给 S_1 和 S_2。

3) S_1 和 S_2 接收到拆分的分量和随机数后，将 I_1, I_2、$\hat{w}_1, \hat{w}_2$ 和 $\hat{\mu}_1, \hat{\mu}_2$ 隐藏至随机数中进行交互。根据本文提出的安全计算协议顺序地执行安全计算层，并各自把分类结果 α_1 和 α_2 提交给 Q。

4) Q 执行简单加法恢复完整的图像分类结果，该过程视作分类结果解密，即 $\alpha = \alpha_1 + \alpha_2$。

2.2 安全模型

在 PPCF 计算中，两台边缘服务器是诚实且好奇的，它们遵循协议，但对对方数据感兴趣。T 总是诚实的，不会影响模型的安全性。此外，S_1 和 S_2 不能共谋或同时被破坏，因为明文数据可以通过简单相加恢复。参与方之间用安全通道传递信息，以防止隐私数据被泄露。

类似于安全模型[17-18,24-25]，敌手 $\mathcal{A}$ 最多可以攻击两台边缘服务器中的某一台（S_1 或 S_2）并获得相应的图像分量（I_1 或 I_2）。同样，敌手 $\mathcal{A}$ 最多能窃听某一条通信链路（① 或 ②），且不能干扰 S_1、S_2、T、Q 及 C 之间的通信。

3 PPCF 设计

3.1 PPCF 概述

PPCF 结构如图 4 所示，S_1 和 S_2 顺序地协同执行安全卷积层、安全批量归一化层、安全激活层、安全最大池化层[18]、安全全局平均池化和安全全连接层等深度神经网络安全层计算，分别输出分类的结果分量 α_1 和 α_2，满足 $\alpha = \alpha_1 + \alpha_2$。为实现加密特征的提取和分类，PPCF 把分量 I_1, I_2、$\hat{w}_1, \hat{w}_2$ 和 $\hat{\mu}_1, \hat{\mu}_2$ 等网络参数传到 S_1 和 S_2，S_1 和 S_2 利用大小为 7×7 的卷积核协同执行安全卷积计算。在每个卷积计算后执行安全

批量归一化计算，使特征分量满足正态分布。然后，安全激活层将分量的负特征值设置为 0。S_1 和 S_2 再利用大小为 3×3 及步距为 2 的卷积核分别对 2 个特征分量协同执行安全最大池化计算。接下来，S_1 和 S_2 分别在本地执行求和及除法操作，得到安全全局平均池化结果。最后，将 2 个池化后的结果分量分别提交至安全全连接层，得到最终的分类结果，此时把 2 个分量相加即能恢复明文环境下的分类结果。

3.2　安全卷积和安全批量归一化层

关于安全卷积计算，本文提出 SConv 协议，S_1 和 S_2 拥有输入和权重参数 t_1,t_2 和 w_1,w_2，且 $t=t_1+t_2$ 和 $w=w_1+w_2$，S_1 和 S_2 协同执行安全点乘协议 $y_1,y_2=\text{SecDotMul}(t_1,t_2,w_1,w_2)$，结果相加得 $y_1+y_2=wt$。然而，安全批量归一化层负责非线性计算

$$\text{BN}(x)=\gamma\frac{x-\dfrac{1}{|B|}\sum\limits_{x\in B}x}{\sqrt{\dfrac{1}{|B|}\sum\limits_{x\in B}(x-\hat{\mu}_B)^2+\varepsilon}}+\beta \tag{4}$$

特别地，针对 PPCF 的 BN 计算提出 SBN 协议，已知 S_1 和 S_2 分别拥有输入 n_1 和 n_2，权重 w_1' 和 w_2'，偏置 b_1' 和 b_2'，满足 $n=n_1+n_2$，$w=w_1'+w_2'$，$b=b_1'+b_2'$，获取训练阶段下的方差和均值参数 δ_1,δ_2 和 μ_1,μ_2，满足 $\delta=\delta_1+\delta_2$，$\mu=\mu_1+\mu_2$。首先，S_1 和 S_2 分别在本地计算方差与 ε 的相加值，ε 为两者共同拥有，令 $\varepsilon=1\times10^{-5}$。然后，$S_1$ 和 S_2 协同执行 SSqr 协议获得输出 out_1 和 out_2，满足 $\text{out}=\text{out}_1+\text{out}_2$。$S_1$ 和 S_2 协同执行 SDiv 协议获得输出 out_1' 和 out_2'，满足 $\text{out}'=\text{out}_1'+\text{out}_2'$，$S_1$ 和 S_2 继续协同执行 SMul 协议获得输出 out_1'' 和 out_2''，满足 $\text{out}''=\text{out}_1''+\text{out}_2''$。$S_1$ 和 S_2 分别在本地计算与偏置 b_1' 和 b_2' 的相加值，获得批量归一化结果 p_1' 和 p_2'，满足 $p=p_1'+p_2'$。此过程中，输入数据和隐私推理阶段的参数不会被泄露，特别地，明文训练下的网络参数 δ_1,δ_2 和 μ_1,μ_2 也能被保护。具体过程如协议 1 所示。

协议 1　SBN 协议

输入　S_1 拥有 $n_1,w_1',b_1',\delta_1,\mu_1,\varepsilon$，$S_2$ 拥有 $n_2,w_2',b_2',\delta_2,\mu_2,\varepsilon$

输出　S_1 输出 p_1'，S_2 输出 p_2'

1) S_1 计算 $q_1\leftarrow\delta_1+\varepsilon$，$S_2$ 计算 $q_2\leftarrow\delta_2+\varepsilon$
2) S_1 和 S_2 协同执行 $\text{out}_1,\text{out}_2\leftarrow\text{SSqr}(q_1,q_2)$，满足 $\text{out}\leftarrow\text{out}_1+\text{out}_2$
3) S_1 计算 $y_1''\leftarrow n_1-\mu_1$，$S_2$ 计算 $y_2''\leftarrow n_2-\mu_2$
4) S_1 和 S_2 协同执行 $\text{out}_1',\text{out}_2'\leftarrow\text{SDiv}(y_1'',y_2'',\text{out}_1,\text{out}_2)$，满足 $\text{out}'\leftarrow\text{out}_1'+\text{out}_2'$
5) S_1 和 S_2 协同执行 $\text{out}_1'',\text{out}_2''\leftarrow\text{SMul}(\text{out}_1',\text{out}_2',w_1',w_2')$，满足 $\text{out}''\leftarrow\text{out}_1''+\text{out}_2''$
6) S_1 计算并返回 $p_1'\leftarrow\text{out}_1''+b_1'$，$S_2$ 计算并返回 $p_2'\leftarrow\text{out}_2''+b_2'$，且 $p\leftarrow p_1'+p_2'$

3.3　安全激活层

ReLU 是激活层常用的激活函数之一，但该函数上限无穷大，产生很多不可用的神经元。因此本文采用 ReLU6 函数做激活隐私计算，它设置了上限，ReLU6 函数负责非线性计算，即

$$f_{(s)}=\min(\max(0,s),6),\ s\in[0,6] \tag{5}$$

显然，此函数不能拆分，因此本文提出 SRU6 协议。已知输入 s_1 和 s_2，满足 $s=s_1+s_2$，S_1 和 S_2 协同执行 SComp 协议获得 s_1,s_2 与 6 的比较结果，即 s 的

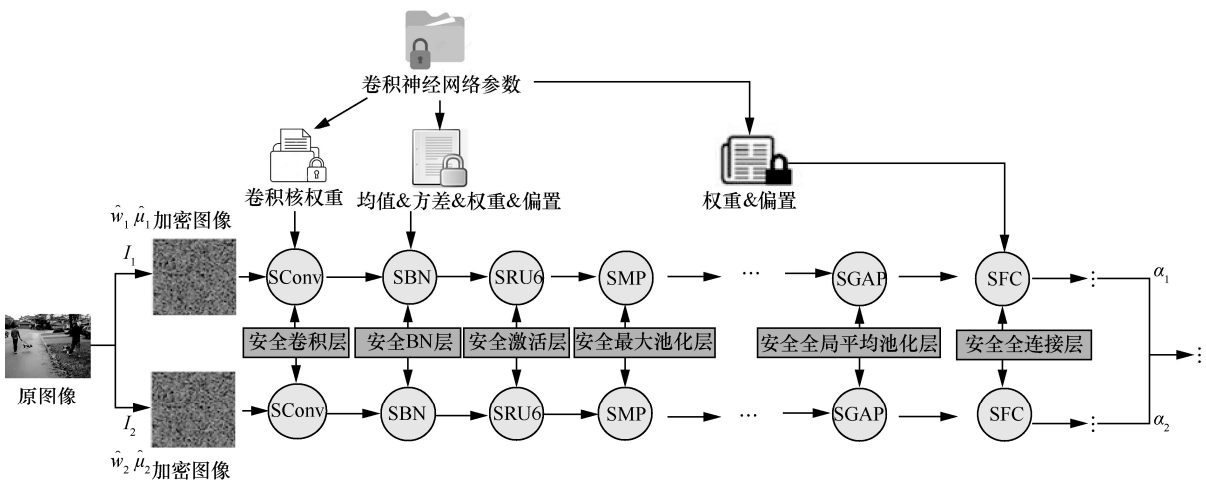


图 4　PPCF 结构

符号位 θ_1，若 $s \geqslant 6$，$\theta_1 = 0$；若 $s<6$，$\theta_1 = 1$。S_1 和 S_2 分别将输入 s_1 和 s_2 与 θ_1 相乘获得激活结果 P_1 和 P_2，满足 $P=P_1+P_2$。判断该激活结果值是否为 0，若 P_1 和 P_2 为 0，则把该值置为 6。然后，S_1 和 S_2 协同执行 SComp 协议获得 P_1, P_2 与 0 的比较结果 θ_2，θ_2 为 P 的符号位。若 $P \geqslant 0$，$\theta_2 = 0$，否则，$\theta_2 = 1$。最后，S_1 和 S_2 分别将 P_1 和 P_2 与 $1-\theta_2$ 相乘得到激活结果 P_1' 和 P_2'，满足 $P'=P_1'+P_2'$。具体过程如协议 2 所示。

协议 2 SRU6 协议

输入 S_1 拥有 s_1，S_2 拥有 s_2

输出 S_1 输出 P_1'，S_2 输出 P_2'

1) S_1 和 S_2 协同执行 $\theta_1 \leftarrow \text{SComp}(s_1, s_2, 6, 6)$
2) S_1 和 S_2 分别计算 $P_1 \leftarrow s_1\theta_1$ 和 $P_2 \leftarrow s_2\theta_1$，若 $P_1 = 0$ 和 $P_2 = 0$，则 $P_1 \leftarrow 6$，$P_2 \leftarrow 6$
3) S_1 和 S_2 协同执行 $\theta_2 \leftarrow \text{SComp}(P_1, P_2, 0, 0)$，然后，$S_1$ 和 S_2 分别在本地计算 $\rho \leftarrow 1-\theta_2$
4) S_1 计算并返回 $P_1' \leftarrow P_1\rho$，S_2 计算并返回 $P_2' \leftarrow P_2\rho$，满足 $P' \leftarrow P_1'+P_2'$

3.4 安全全局平均池化与安全全连接层

在安全全局平均池化中，不需要 S_1 和 S_2 协同执行，由此提出了 S_1 和 S_2 分别在本地线性计算求和与除法操作的 SGAP 协议。在单通道情况下，假设加法分量 1 和 2 得到求和的值为 ∂_1 和 ∂_2，已知该图像特征某一通道值的数量为 λ_1 和 λ_2，S_1 和 S_2 分别在本地执行 $z_1 = \frac{\partial_1}{\lambda_1}$ 和 $z_2 = \frac{\partial_2}{\lambda_2}$，池化结果为 $z_1 + z_2 = \frac{\partial}{\lambda}$。

PPCF 的安全全连接计算与安全卷积计算类似，涉及安全点乘计算，本文提出 SFC 协议。已知 S_1 和 S_2 接收到输入 η_1 和 η_2，权重和偏置 $\overline{w}_1, \overline{w}_2$ 和 $\overline{b}_1, \overline{b}_2$，满足 $\eta = \eta_1 + \eta_2$，$\overline{w} = \overline{w}_1 + \overline{w}_2$，$\overline{b} = \overline{b}_1 + \overline{b}_2$。$S_1$ 和 S_2 协同执行 SecDotMul 协议得 $\psi_1, \psi_2 = \text{SecDotMul}(\eta_1, \eta_2, \overline{w}_1, \overline{w}_2)$，满足 $\psi = \psi_1 + \psi_2$。然后，S_1 和 S_2 分别在本地与偏置 $\overline{b}_1, \overline{b}_2$ 执行加法计算 $\psi_1' = \psi_1 + \overline{b}_1$ 和 $\psi_2' = \psi_2 + \overline{b}_2$，满足 $\psi' = \psi_1' + \psi_2'$。

4 理论分析

4.1 正确性分析

已知输入图像数据 η' 被随机拆分成 η_1' 和 η_2'，S_1 和 S_2 协同执行 PPCF 后输出目标分类结果 $\overline{f}_1$ 和 $\overline{f}_2$，满足 $\overline{f} = \overline{f}_1 + \overline{f}_2$。在 PPCF 中，图像数据 η' 经过一系列的安全计算层，计算层的安全性又依赖于安全计算协议的安全性。之前的工作[17-18,23-24]已经证明 SDiv 协议、SMul 协议、SSqr 协议和 SecDotMul 协议的正确性。在本文中，输入的 2 个图像分量 η_1' 和 η_2' 由 S_1 和 S_2 协同执行 SConv 协议完成卷积计算，得到结果 $\overline{y}_1, \overline{y}_2$，满足 $\overline{y} = \overline{y}_1 + \overline{y}_2$。然后，SBN 协议完成安全批量归一化，使输出结果满足正态分布。此过程中，S_1 和 S_2 协同执行 SSqr 协议、SDiv 协议、SMul 协议以及本地操作，以正确计算 SBN 协议输出的结果 p_1' 和 p_2'，满足 $p = p_1' + p_2'$。接着由 SRU6 协议完成安全激活计算，S_1 和 S_2 对输入 p_1' 和 p_2' 执行 2 次 SComp 协议，以及 3 次本地计算，正确地比较 p_1'、p_2' 和 6 及 0 的大小。通过符号位的结果，从而确定将输入 p_1' 和 p_2' 置为 0 还是 6，或者保持不变。在 SMP 协议中，S_1 和 S_2 协同执行 $a \times a - 1$ 次交互操作，$a \times a$ 为卷积核大小，求出最大值 Γ_1 和 Γ_2，满足 $\Gamma = \Gamma_1 + \Gamma_2$。然后，$S_1$ 和 S_2 分别在本地执行 SGAP 协议，即简单的求和及除法操作，得到结果 z_1 和 z_2，满足 $z = z_1 + z_2$。接着执行 SFC 协议，S_1 和 S_2 对输入 z_1 和 z_2 协同执行 SecDotMul 协议，得到输出结果 ψ_1', ψ_2'，满足 $\psi' = \psi_1' + \psi_2'$。显然，通过这一系列安全计算协议可以保证 PPCF 在理论上是完全正确性的。

4.2 安全性分析

在半可信模型中，假设存在一个与边缘服务器计算资源一样的概率多项式时间模拟器 $\hat{S}$，能够独立地通过某个算法模拟一组视图，且模拟出来的视图与真实视图让敌手 $\mathcal{A}$ 无法区分，则说明本文提出的计算协议是安全的。为了证明本文提出的协议是安全的，将引入下述引理[25-26]。

引理 1 如果一个协议的所有子协议是完全可模拟的，那么该协议是完全可模拟的。

引理 2 如果一个随机元素 $\overline{t}$ 均匀分布在 $\mathbb{Z}_n$，并且独立于任意变量 $t\overline{t} \in \mathbb{Z}_n$，那 $\overline{t} \pm t\overline{t}$ 也是均匀随机且与 $t\overline{t}$ 互相独立。

关于引理 1 和引理 2 的证明，可以参考文献[25-26]。根据引理 1 所述，PPCF 的安全性可以归结于 SConv 协议、SBN 协议、SRU6 协议、SGAP 协议和 SFC 协议的安全性证明，以上协议又依赖于 SMul 协议、SSqrt 协议、SDiv 协议和 SecDotMul 协议，这些子协议的安全性在文献[17,23-24]中已得到证明。

定理 1 在半可信模型中，SBN 协议是安全的。

证明 在 SBN 协议中，S_1 的真实视图是

$\{n_1, w_1', b_1', \delta_1, \mu_1, q_1, q_2, o_1, y_1'', y_2'', o_1', o_1'', p_1'\}$，$S_1$ 在本地计算得到 $q_1 \leftarrow \delta_1 + (1e-5)$ 不需要传递给 S_2，与 S_2 协同执行 SSqr 协议、SDiv 协议和 SMul 协议得到的 o_1，o_1' 和 o_1'' 同样也不能直接发送给 S_2。然后，S_1 只需在本地计算 o_1'' 和 b_1' 的加值，得到 $p_1' \leftarrow o_1'' + b_1'$。模拟器 $\hat{S}$ 为 S_1 模拟生成均匀随机分布的模拟视图，敌手 $\mathcal{A}$ 无法区分真实视图和模拟视图。同理，敌手 $\mathcal{A}$ 也无法区分 S_2 真实视图 $\{n_2, w_2', b_2', \delta_2, \mu_2, q_1, q_2, o_2, y_1'', y_2'', o_2', o_2'', p_2'\}$ 及模拟试图。此外，根据引理 1，SBN 协议的安全性可由 SSqr 协议、SDiv 协议和 SMul 协议所保证。因此，SBN 协议是安全的。

证毕。

定理 2　在半可信模型中，SRU6 协议是安全的。

证明　在 SRU6 协议中，S_1 的真实视图是 $\{s_1, \theta_1, p_1, \theta_2, \rho, p_1'\}$，由 2 次 SComp 协议得到符号位 θ_1 和 θ_2 是均匀分布的随机值，由引理 2 知，该值若被公开不会泄露隐私数据的隐私。模拟器 $\hat{S}$ 为 S_1 模拟生成均匀随机分布的模拟视图，敌手 $\mathcal{A}$ 无法与真实视图区分。同理，敌手 $\mathcal{A}$ 无法区分 S_2 的真实视图 $\{s_2, \theta_1, p_1, \theta_2, \rho, p_2'\}$ 和模拟试图。由于 SComp 协议已被证明是安全的，因此，SRU6 协议是安全的。

证毕。

定理 3　在半可信模型中，SGAP 协议、SConv 协议和 SFC 协议是安全的。

证明　在 SGAP 协议中，S_1 的真实视图是 $\{\chi_1, \partial_1, \lambda_1, z_1\}$，其中 ∂_1, λ_1 和 z_1 是本地计算得到的值，计算过程不需要跟 S_2 有任何交互，故敌手 $\mathcal{A}$ 无法窃取到任何数据，因此，SGAP 协议是安全的。在 SConv 协议中，S_1 的真实视图是 $\{t_1, w_1, y_1\}$，y_1 是 S_1 和 S_2 协同执行 SecDotMul 协议后的结果，该结果不能直接发送给 S_2。模拟器 $\hat{S}$ 为 S_1 模拟生成均匀的模拟视图，敌手 $\mathcal{A}$ 无法与真实视图进行区分。同理，敌手 $\mathcal{A}$ 也无法区分 S_2 的真实视图 $\{t_2, w_2, y_2\}$，而且 SecDotMul 协议有所保证。可见，SConv 协议是安全的。同样地，SFC 协议中，S_1 的真实视图是 $\{\eta_1, \overline{w}_1, \overline{b}_1, \psi_1, \psi_1'\}$，$\psi_1$ 是 S_1 和 S_2 协同执行 SecDotMul 协议后的结果，ψ_1' 是本地计算的结果。模拟器 $\hat{S}$ 为 S_1 模拟生成均匀的模拟视图，敌手 $\mathcal{A}$ 无法与真实视图进行区分。同理，敌手 $\mathcal{A}$ 也无法区分 S_2 的真实视图 $\{\eta_2, \overline{w}_2, \overline{b}_2, \psi_2, \psi_2'\}$。因此，SFC 协议也是安全的。

证毕。

4.3　复杂性分析

本节对计算和通信两方面进行复杂性分析，评估本文提出的 PPCF 效率。相比于明文环境下的 ResNet，本文引入安全计算协议，显然会增加计算复杂度。在 SConv 协议中，引入了一次 SecDotMul 协议计算，此协议与 SMul 协议计算方式都是顺序执行的，其计算复杂度为 $O(N)$。在 SBN 协议中，基于顺序结构执行 SSqr 协议、SDiv 协议和 SMul 协议，并且采用互相传递本地计算得到的参数方式，计算复杂度为 $O(N)$。然后，PPCF 基于 2 次 SComp 协议完成 SRU6 协议计算，不需要多次循环操作，其计算复杂度是 $O(N)$，然而文献[20]的安全激活函数只执行了一次 SComp 操作，那么执行 2 次 SComp 的复杂度则需要 $O(2N\log l)$。对于 SGAP 协议，在本地执行求和及除法计算，计算复杂度为常数阶 $O(1)$。基于 SecDotMul 执行的 SFC 协议，其计算复杂度也为 $O(N)$，计算复杂度如表 1 所示。表 1 中，N 表示输入数组大小；l 表示整数环大小。

表 1　安全计算协议的计算复杂度

协议	ResNet[21]	FALCON[20]	PPCF
SConv	$O(N)$	$O(N)$	$O(N)$
SFC	$O(N)$	$O(N)$	$O(N)$
SGAP	$O(1)$	—	$O(1)$
SBN	$O(N)$	$O(3N)$	$O(N)$
SRU6	$O(N)$	$O(2N\log l)$	$O(N)$

对于通信复杂度而言，安全计算协议的通信开销与通信轮数和传递内容的长度大小有关，底层的 SMul 协议、SSqrt 协议、SDiv 协议、SecDotMul 协议和 SComp 协议分别需要一轮、3 轮、3 轮、一轮和 3 轮的通信开销。在 PPCF 的 SConv 协议中，S_1 和 S_2 协同执行一次 SecDotMul 协议，通信开销为一轮。在 SBN 协议中，执行各一次的 SSqr 协议、SDiv 协议、SMul 协议，均需要 7 轮通信开销，与文献[20]的多轮迭代近似方法相比，远远小于 $(1+4l+14N)r\|N\|$ 的通信开销，其中，$\|N\|$ 表示传递消息的大小，r 表示迭代次数。在 SRU6 协议中，包含 2 次 SComp 协议，即需要 6 轮通信开销。SGAP 协议无数据交互传递，均不需要通信开销。对于 SFC 协议，同样包含一次 SecDotMul 协议，则需要一轮通信开销，通信复杂度如表 2 所示。

表 2 安全计算协议的通信复杂度

安全计算协议	通信轮数/轮	通信开销
SConv	1	$2N\|N\|$
SBN	7	$13N\|N\|$
SRU6	6	$8N\|N\|$
SF	1	$2N\|N\|$

5 性能评估

本节实验使用 A100-SXM4-40GB 的 GPU，其硬件配置为 132 GB 的内存、32 核的处理器和 940 GB 的硬盘，在 Visual Studio Code 仿真平台上完成实验。利用 Numpy 工具完成多维浮点数数组的创建、传递和计算。接下来，本文先从提出的安全计算协议和隐私保护分类框架 PPCF 的计算误差讨论，然后从计算和通信开销方面对两者做性能评估。在本文隐私计算中，本文采用明文训练、密文推理方式，输入输出及计算均采用 4 B 的浮点数组，每个数组元素的计算形式一致。随机选择多维数组 κ_1，取值范围在 $(-2^8,2^8)$ 之间，得到另一分量 $\kappa_2=\kappa-\kappa_1$。

5.1 误差分析

计算误差即明文输出结果与利用安全计算协议执行密文计算输出结果的最大差值，它对框架分类精度具有关键作用。本文主要讨论误差与安全计算协议输入数组大小的关系，为使实际的误差结果足够客观，将输入数组大小设定为 1×10^5 内，并保留 8 位小数参与误差计算。在 SMul 协议、SDiv 协议、SComp 协议、SecDotMul 协议基础上设计的 SConv 协议、SRU6 协议、SFC 协议可以达到近似零误差，具有优良的计算性能。此外，SGAP 协议没有涉及数据消息的交互传递，也能达到近似零误差。然而由于数值精度等原因，实际计算中的 SBN 协议存在误差，但随着输入数组增大，计算误差仍维持在 1×10^{-4} 不变，此细微误差在可接受范围之内。

5.2 计算开销

计算开销即运行时间的大小，通过断点测试方法，利用安全计算协议的运行时间量化计算开销，安全计算协议的性能如图 6 所示。从图 6 可知，运行时间随输入数组的增大而增加，横坐标是输入数组大小，纵坐标是以毫秒为单位的时间戳浮点数。相比于明文环境下的 SConv 协议、SBN 协议、SRU6 协议、SFC 协议在处理大小为 1×10^3 内的输入数组时，计算开销可忽略不计。进而，在处理大小为 1×10^4 内的输入数组，计算开销没有明显增长。即使处理大小为 1×10^5 内的输入数组，SConv 协议、SBN 协议、SRU6 协议和 SFC 协议的计算开销也能控制在 350 ms、120 ms、70 ms、11 ms 内。此结果与表 1 计算复杂度一致，由于在执行 2 轮 SComp 协议上设计的 SRU6 协议不需要引入依赖于 l 的循环结构，只需要执行 2 轮 STAM 协议和线性计算，但 SRU6 协议计算开销仍不及基于 SSqr 协议、SDiv 协议和 SMul 协议设计的 SBN 协议计算开销大，因为 SSqr 协议、SDiv 协议和 SMul 协议都要执行 STMA 协议和 STAM 协议各一次和线性计算。此外，基于一次 SecDotMul 协议的 FC 协议没有涉及 STAM 协议或者 STMA 协议，只执行一些点乘运算，其计算开销最低。然而基于一次 SecDotMul 协议的 SConv 协议计算开销最大，SConv 协议产生的计算开销约为 SBN 协议的 3 倍，因为该协议还在本地执行大量的线性乘法和除法等计算。对于 SGAP 协议，没有涉及数据交互传递，无论在哪个输入范围，其运行时间都能保持在 0.3 ms 内，计算差值可忽略不计。

5.3 通信开销

PPCF 的实际开销与传递数据的大小和通信轮数有关，随输入数组的增大而增加。以最大输入数组 $N=1\times10^5$ 为例，图像尺寸为 $180\times180\times3$，该大小足够适用于大多数深度学习模型的输入长度。由图 6(f) 可以看出，SConv 协议和 SFC 协议的通信开销一致，两者都只涉及 SecDotMul 协议，无其他数据传递，两者协议的通信开销基本一致。特别地，当 SBN 协议、SRU6 协议、SConv 协议和 SFC 协议处理大小为 1×10^3 内的输入数组时，其通信开销可以忽略不计。对于大小为 1×10^4 内的输入数组，其通信开销均控制在 0.5 MB、0.3 MB 及 0.083 MB 内。对于大小为 1×10^5 内的输入数组，基于 SSqr 协议、SDiv 协议和 SMul 协议基础上设计的 SBN 协议通信轮数频繁地达到 7 轮。该协议涉及的基础协议数量较多，由于 STAM 协议和 STMA 协议各需 2 轮和一轮的通信开销，因此基于 STAM 协议和 STMA 协议的 SSqr 协议、SDiv 协议和 SMul 协议各需要 3 轮、3 轮、一轮的通信开销，即 SBN 协议的通信开销最大，但能控制在 5 MB 内，在可接受范围内。

5.4 目标分类结果

本文采用自定义的分类数据集进行试验，从互联网上获取 3 670 张 RGB 图像，其中训练数据有

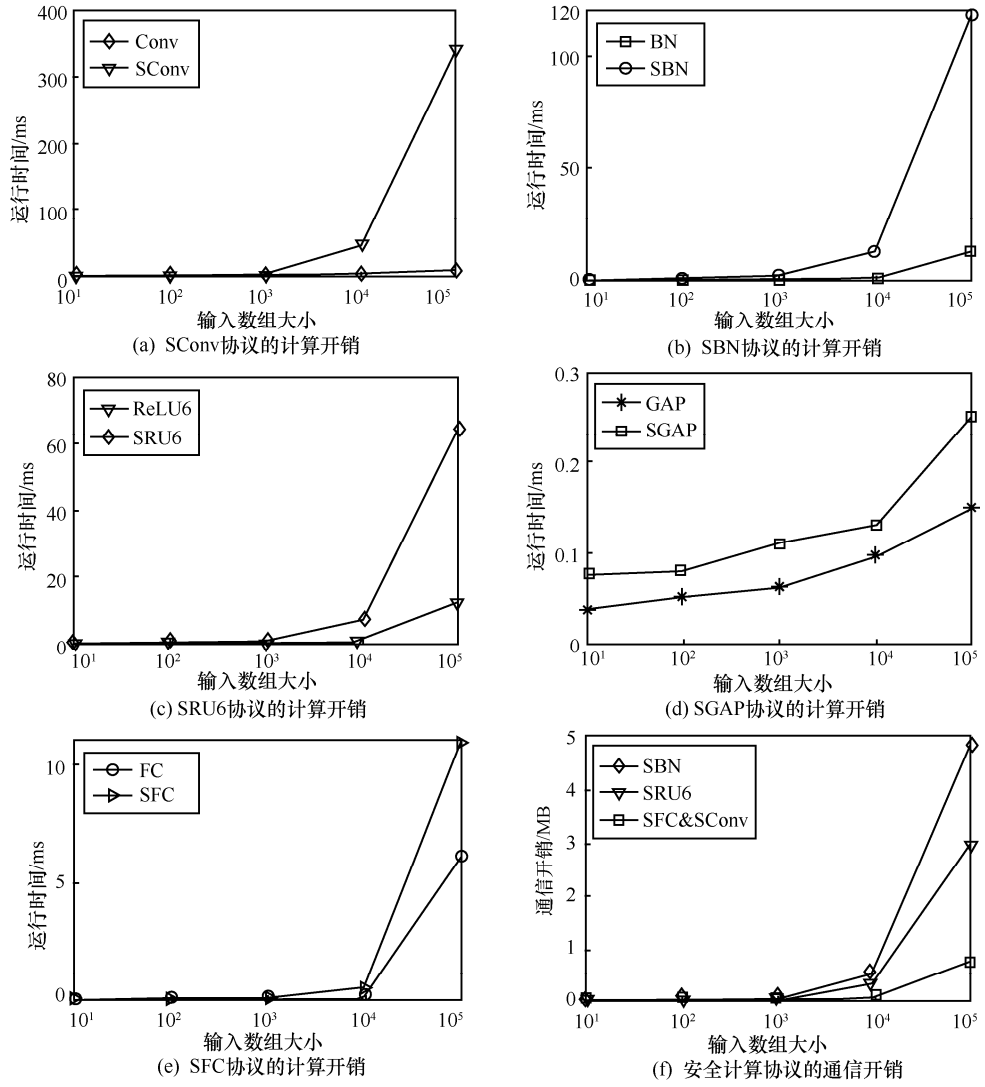


图 6　安全计算协议的性能

3 306 张，测试数据有 364 张，包含 5 个类别。考虑到实际的网联自动驾驶应用场景，采用先进的 18 层分类网络 ResNet 进行图像分类。把输入大小为 1×10^5 的图像随机拆分为 2 个加法分量，S_1 和 S_2 利用本文提出的安全计算协议执行 PPCF，首先执行 SConv 协议需要 341 ms，SBN 协议需要 120ms，相应的 SRU6 协议需要 70 ms，接下来 3×3 的 SMP 协议需要 20 ms。同时，SFC 协议也仅耗时 11 ms，以上的安全计算协议均可达到毫秒级别。综上所述，PPCF 实际产生的计算开销约为 5s，这对于实时性需求苛刻的自动驾驶场景来说具有可观的应用场景。在 PPCF 中，计算误差主要由 SBN 协议带来，但无论输入图像大小是多少，计算误差保持 1×10^{-4} 量级不变，且最高的通信开销也保持在 145.3 MB 内，PPCF 与明文 ResNet 的性能比较结果如表 3 所示。此外，理论分析证明 PPCF 的正确性、安全性和高效性，PPCF 与其他隐私深度学习框架的比较如表 4 所示。

表 3　PPCF 与明文 ResNet 的性能比较

模型	计算开销/s	通信开销/MB	分类精度
ResNet[21]	1.06	—	99.83%
PPCF	5.10	145.3	99.83%

表 4　PPCF 与其他隐私深度学习框架比较

协议	文献[17]	文献[19]	文献[20]	PPCF
SConv	√	√	√	√
SGAP	—	—	—	√
SFC	√	√	√	√
SBN	—	—	√	√
SRU6	—	—	—	√
保护训练参数	—	√	√	√

6 结束语

本文对感知图像数据在信道传输、边缘节点分类过程和分类后结果的隐私安全和计算效率问题进行研究，考虑到复杂多变的网络环境、低时延和低开销的强需求，基于加性秘密共享技术设计了一系列安全计算协议，并实现了一种边缘协同的轻量级隐私保护分类框架 PPCF。理论分析了安全计算协议和 PPCF 的正确性和安全性，在整个隐私计算中，两台边缘服务器和敌手均不能窃取到完整的图像特征和网络参数。仿真结果证明，PPCF 兼备良好的分类性能和计算效率优势，且达到与明文环境等同的分类精度。

参考文献：

[1] NGUYEN K X, RYU T, ZHANG J, et al. CoConv: learning dynamic cooperative convolution for image recognition[C]//Proceedings of 2021 IEEE International Conference on Multimedia and Expo. Piscataway: IEEE Press, 2021: 1-6.

[2] YANG Q, FU S, WANG H G, et al. Machine-learning-enabled cooperative perception for connected autonomous vehicles: challenges and opportunities[J]. IEEE Network, 2021, 35(3): 96-101.

[3] GUO J D, CARRILLO D, TANG S H, et al. CoFF: cooperative spatial feature fusion for 3-D object detection on autonomous vehicles[J]. IEEE Internet of Things Journal, 2021, 8(14): 11078-11087.

[4] XIONG J B, BI R W, TIAN Y L, et al. Towards lightweight, privacy-preserving cooperative object classification for connected autonomous vehicles[J]. IEEE Internet of Things Journal, 3573, PP(99): 1.

[5] LIN L, LIAO X F, JIN H, et al. Computation offloading toward edge computing[J]. Proceedings of the IEEE, 2019, 107(8): 1584-1607.

[6] YANG S Z, GONG Z, YE K, et al. EdgeCNN: convolutional neural network classification model with small inputs for edge computing[J]. arXiv Preprint, arXiv: 1909.13522, 2019.

[7] WANG Y B, HONG K J, ZOU J, et al. A CNN-based visual sorting system with cloud-edge computing for flexible manufacturing systems[J]. IEEE Transactions on Industrial Informatics, 2020, 16(7): 4726-4735.

[8] WONG A, LIN Z Q, CHWYL B. AttoNets: compact and efficient deep neural networks for the edge via human-machine collaborative design[C]//Proceedings of 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. Piscataway: IEEE Press, 2019: 684-693.

[9] HESAMIFARD E, TAKABI H, GHASEMI M, et al. Privacy-preserving machine learning as a service[J]. Proceedings on Privacy Enhancing Technologies,2018, 2018(3): 123-142.

[10] GILAD-BACHRACH R, DOWLIN N, LAINE K, et al. CryptoNets: applying neural networks to encrypted data with high throughput and accuracy[C]//Proceedings of the 33rd International Conference on Machine Learning. Saarland: DBLP, 2016: 201-210.

[11] CHOU E, BEAL J, LEVY D, et al. Faster CryptoNets: leveraging sparsity for real-world encrypted inference[J]. arXiv Preprint, arXiv: 1811.09953, 2018.

[12] AL-BADAWI A, JIN C, LIN J, et al. Towards the AlexNet moment for homomorphic encryption: HCNN, the first homomorphic CNN on encrypted data with GPUs[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(3): 1330-1343.

[13] ZHANG Q C, YANG L T, CHEN Z K. Privacy preserving deep computation model on cloud for big data feature learning[J]. IEEE Transactions on Computers, 2016, 65(5): 1351-1362.

[14] ROUHANI B D, RIAZI M S, KOUSHANFAR F. DeepSecure: scalable provably-secure deep learning[C]//Proceedings of 2018 55th ACM/ESDA/IEEE Design Automation Conference. Piscataway: IEEE Press, 2018: 1-6.

[15] LIU J, JUUTI M, LU Y, et al. Oblivious neural network predictions via MiniONN transformations[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 619-631.

[16] RIAZI M S, WEINERT C, TKACHENKO O, et al. Chameleon: a hybrid secure computation framework for machine learning applications[C]//Proceedings of the 2018 on Asia Conference on Computer and Communications Security. New York: ACM Press, 2018: 707-721.

[17] HUANG K, LIU X M, FU S J, et al. A lightweight privacy-preserving CNN feature extraction framework for mobile sensing[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1441-1455.

[18] 熊金波, 毕仁万, 陈前昕, 等. 边缘协作的轻量级安全区域建议网络[J]. 通信学报, 2020, 41(10): 188-201.
XIONG J B, BI R W, CHEN Q X, et al. Towards edge-collaborative, lightweight and secure region proposal network[J]. Journal on Communications, 2020, 41(10): 188-201.

[19] WAGH S, GUPTA D, CHANDRAN N. SecureNN: 3-party secure computation for neural network training[J]. Proceedings on Privacy Enhancing Technologies, 2019, 2019(3): 26-49.

[20] WAGH S, TOPLE S, BENHAMOUDA F, et al. Falcon: honest-majority maliciously secure framework for private deep learning[J]. Proceedings on Privacy Enhancing Technologies, 2021, 2021(1): 188-208.

[21] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2016: 770-778.

[22] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[23] 毕仁万, 陈前昕, 熊金波, 等. 面向深度神经网络的安全计算协议设计方法[J]. 网络与信息安全学报, 2020, 6(4): 130-139.
BI R W, CHEN Q X, XIONG J B, et al. Design method of secure computing protocol for deep neural network[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 130-139.

[24] LIU Y, MA Z, LIU X M, et al. Privacy-preserving object detection for medical images with faster R-CNN[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 69-84.

[25] BOGDANOV D, NIITSOO M, TOFT T, et al. High-performance secure multi-party computation for data mining applications[J]. International Journal of Information Security, 2012, 11(6): 403-418.

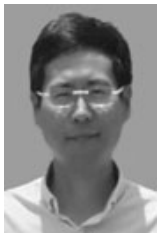
[26] XIONG J B, BI R W, ZHAO M F, et al. Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles[J]. IEEE Wireless Communications, 2020, 27(3): 24-30.

[作者简介]

熊金波（1981– ），男，湖南益阳人，博士，福建师范大学教授、博士生导师，主要研究方向为安全深度学习、移动群智感知、隐私保护技术等。

周永洁（1996– ），女，贵州镇远人，贵州大学硕士生，主要研究方向为安全深度学习、隐私保护技术等。

毕仁万（1996– ），男，湖南常德人，福建师范大学博士生，主要研究方向为安全深度学习、安全多方计算等。



万良（1974– ），男，贵州铜仁人，博士，贵州大学教授、硕士生导师，主要研究方向为网络空间安全等。

田有亮（1982– ），男，贵州六盘水人，博士，贵州大学教授、博士生导师，主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护、区块链与电子货币等。