

Privacy-Preserving Machine Learning Training in IoT Aggregation Scenarios

Liehuang Zhu, *Member, IEEE*, Xiangyun Tang, Meng Shen, *Member, IEEE*,
Jie Zhang, Xiaojiang Du, *Fellow Member, IEEE*

Abstract—To develop Smart City, the growing popularity of Machine Learning (ML) that appreciates high-quality training datasets generated from diverse IoT devices raises natural questions about the privacy guarantees that can be provided in such settings. Privacy-preserving ML training in an aggregation scenario enables a model demander to securely train ML models with the sensitive IoT data gathered from personal IoT devices. Existing solutions are generally server-aided, cannot deal with the collusion threat between the servers or between the servers and data owners, and do not match the delicate environments of IoT. We propose a privacy-preserving ML training framework named **Heda** that consists of a library of building blocks based on partial homomorphic encryption (PHE) enabling constructing multiple privacy-preserving ML training protocols for the aggregation scenario without the assistance of untrusted servers and defending the security under collusion situations. Rigorous security analysis demonstrates the proposed protocols can protect the privacy of each participant in the honest-but-curious model and defend the security under most collusion situations. Extensive experiments validate the efficiency of **Heda** which achieves the privacy-preserving ML training without losing the model accuracy.

Index Terms—IoT data, Machine Learning, Homomorphic Encryption, Secure Two-party Computation, Modular Sequential Composition

I. INTRODUCTION

INTERNET of Things (IoT) plays a remarkable role in all aspects of our daily lives, covering various fields including healthcare, industrial appliances, sports, homes, etc [1, 2]. The large data collected from IoT devices with machine learning (ML) technologies have been accelerating Smart City step and improving our daily lives. For a personal healthcare example, fitness records monitored by wearable IoT sensors can be feeded to a ML model provided by medical research institutions, for self-rated health measurement.

ML features data-driven [3]. The comprehensive training dataset is one of the critical factors for accomplishing accurate ML models. While the data collected from a single type of IoT devices is not comprehensive. Or some companies (e.g., the medical research institutions), desiring to develop a ML model to provide the smart services to users, own no training data generated from IoT devices. Mostly, the companies (model demanders) have to develop ML models on the training dataset gathered from multiple IoT data owners.

L. Zhu, X. Tang, M. Shen and J. Zhang are with School of Computer Science, Beijing Institute of Technology, Beijing, China. Email: {liehuangz, xiangyunt, shenmeng, 3120181068}@bit.edu.cn. Prof. Meng Shen is the corresponding author.

X. Du is with the Department of Computer and Information Sciences, Temple University, Philadelphia, USA. Email: dxj@ieee.org.

TABLE I
DIFFERENCES BETWEEN COLLABORATIVE SCENARIO AND AGGREGATION SCENARIO

Aspects	Differences Details
Model Demander	In aggregation scenarios: the company that desires ML models but has no training data is the model demander. In collaborative scenarios: every data owner is a model demander.
Computation Mode	In aggregation scenarios: the model demander interacts with the data owners for initiative training models. In collaborative scenarios: the data owners cooperating with each other to training models, servers is auxiliary.
Privacy Guarantee	In aggregation scenarios: the model demander learns nothing but the model; the data owners learn neither the model nor the data of other data owners. In collaborative scenarios: the data owners' datasets are confidential; the model is known by every participant.

However, the personal IoT data contains users' sensitive information. Privacy concerns and data protection laws surrounding data sovereignty and jurisdiction prevent IoT data owners from openly sharing users' data [4, 5]. Besides, the model demanders are unwilling to let others know about their personal models. This paper focuses on ML training phase and targets at the setting where a model demander learns nothing but a final model from the gathered IoT dataset, and each IoT data owner cannot learn any useful thing after sharing a protected version data with the model demander.

To train ML models upon gathered datasets securely, most existing works have explored the solutions under collaborative scenarios (e.g., Federated Learning [6, 7] and Multi-party Collaborative Learning [8, 9]), where a set of data owners share protected versions of their data with each other and jointly train a global model over these data for themselves. Our setting is different from them in some aspects. To distinguish from them, we name our target setting as Aggregation Scenario, the differences between the two scenarios are summarized in Table I. Specifically, in most of solutions for collaborative scenarios, the model is known by every data owner, which ignores the security requirement of model demanders [10]. PrivFL [11] fits Federated Learning setting and considers model privacy. But since it delegates most of heavy cryptographic computations to data owners, and IoT data owners are generally resource-constrained and cannot support the heavy cryptographic computations generally. PrivFL dose not match IoT setting. Besides, even though a method provides a separate

privacy-preserving solution for training one type of ML model in collaborative scenarios such as for Support Vector Machine (SVM) [9, 12], Linear Regression [13], Naive Bayesian (NB) [14], and K-means [15], other types of ML models remain unsolved, as well as the solutions for the aggregation scenario.

In our aggregation scenario, IoT data owners share protected versions of their data with the model demander and only allow to leak the information of the final model. To reduce the computing load at the IoT data owner side, the model demander shoulders most of the cryptographic computations. During the whole training process, the model demander performs computations on ciphertext to learn the model. Few works explored privacy-preserving ML training in the aggregation scenario. These works generally introduce untrusted servers to facilitate secure training and cannot defend the security of collusion situations [5, 10]. Once model demanders collude with data owners [10] or the servers [5], the sensitive data in the training dataset will be leaked in these methods. Privacy-preserving data aggregation is a kind of fundamental algorithm widely applied in IoT [16–18], which handles the scenario that resembles the aggregation scenario. Since privacy-preserving data aggregation solutions just attain simple operations such as secure summation and secure maximum, it cannot cope with the complex computations in ML training algorithms directly.

Given the limitations of existing schemes, designing a privacy-preserving ML training scheme in the aggregation scenario of IoT faces two main challenges. *First*, how to obtain the correct model without loss of accuracy on the premise of ensuring the security requirement in the aggregation scenario. Without server-aid, the model demander is forced to only get in touch with the ciphertext version of training data throughout the training process for developing ML models. While most ML training algorithms require iteratively updating model parameters using training datasets, and updating the model parameters using the protected version of datasets directly tend to cause a accuracy loss in models. *Second*, how to guarantee the security when the model demander colludes with data owners or data owners collude with each other. Most existing works limit the collusion situation such as prohibiting the collusion between the model demander and data owners, to meet the security requirements. While each participant has the motives for collusion and inferring the sensitive information of other participants. The complexity of the form of IoT privacy data in collusion situations increases the difficulty of privacy-preserving.

In this paper, we design a general framework that supports training three ML models, Logistic Regression (LR), SVM and NB, and allows the collusion between the model demander and IoT data owners and the collusion between data owners. Although practical deep learning models have sprung up and achieved excellent results, it cannot replace these traditional ML algorithms that are able to obtain accurate models from small training datasets [19–21]. And some deep learning applications employ traditional ML models (e.g., SVM and LR) for final prediction outputs, where neural networks are used to extract features [22, 23].

Contributions. To this end, we propose Heda, a general privacy-preserving framework supporting multiple ML train-

ing protocols that satisfy the security requirements in the aggregation scenario and the delicate environments of IoT. A thorough security analysis is provided, demonstrating the security of the proposed protocols in the honest-but-curious model. Extensive experiments on real-world datasets validate the proposed protocols achieve the privacy-preserving ML training without losing the model accuracy. The contributions of our paper can be summarized as follows.

1. In order to train ML models upon ciphertext without accuracy loss, we design a library of building blocks, based on the additively homomorphic encryption Paillier [37] and multiplicative homomorphic encryption Cloud-RSA [38]. Inspired by the idea of permutations and combinations that complex algorithms can be decomposed into several primitive operations, after identifying a set of core operations that underlie many ML training algorithms, we carefully design a library of building blocks supporting each of these core operations.

2. To guarantee the security under the collusion situations and meet the security requirements in the aggregation scenario, we design other two building blocks that enable an algorithm’s output to become the input of another algorithm. All building blocks are designed in a composable way and satisfy both functionality and security, where the security of the combinations between building blocks is ensured by Modular Sequential Composition [39].

3. We instantiate Heda to three privacy-preserving ML training protocols: LR, SVM, and NB, without the assistance of untrusted servers. To the best of our knowledge, we are the first to solve the non-linear function in privacy-preserving LR training without any approximate equation.

The rest of our paper is organized as follows. Section II provides our related work. Section III provides the system overview. In Section IV, we describe the background of PHE. Section V details the building blocks of Heda. Section VI presents the three training protocols instantiated from Heda. The evaluation results are provided in Section VII. Section VIII concludes this paper.

II. RELATED WORK

We devote to the privacy-preserving ML training in the aggregation scenario, while many studies exploring the privacy-preserving ML training fall in collaborative scenarios. More details about the differences between the aggregation scenario and collaborative scenarios can be found in Appendix A.

Our work is related to privacy-preserving ML which can be broadly divided into privacy-preserving prediction and privacy-preserving training. A series of excellent works have been developed for privacy-preserving prediction [7, 24–26]. Some representative works for privacy-preserving prediction are summarized in Table II. In this section, we give the literature review of privacy-preserving training in the aggregation scenario and collaborative scenarios.

In collaborative scenarios. Collaborative scenarios often occurs when multiple organizations have similar types of data, and they want to train a more accurate model on their joint their data [5, 9, 30, 40]. Mohassel et al. proposed a privacy-preserving training scheme based on Garbled Circuit and

TABLE II
SUMMARY OF EXISTING PRIVACY-PRESERVING MACHINE LEARNING SCHEMES

ML Phases	Target Algorithms	Solutions	Ref.
Prediction	Deep Learning	Differential Privacy	[7]
	Neural Network	Secure Multi-party Computation	[24]
	Linear Regression	Homomorphic Encryption	[13]
	Decision Trees, SVM and LR	Homomorphic Encryption and Secret Sharing	[25]
	Hyperplane Decision, NB, and Decision Trees	Homomorphic Encryption and Secret Sharing	[26]
Training	Collaborative Scenario	Deep Learning	Differential Privacy
		Decision Trees	Differential Privacy
		Linear Regression	Differential Privacy
		SVM	Homomorphic Encryption
		LR	Homomorphic Encryption
		NB	Homomorphic Encryption
	Aggregation Scenario	Linear Regression	Homomorphic Encryption
		Linear Regression, LR and Neural Network	Garbled Circuit and Secret Sharing
		Aggregate Statistics	Differential Privacy
		Multilayer Perceptron	Homomorphic Encryption
		Sums of vectors	Secret Sharing
		Quadratic Optimization Problem	Homomorphic Encryption
		k-means	Homomorphic Encryption

Secret Sharing where two untrusted non-colluding servers are introduced [5]. Many secure PHE-based algorithms have been developed for different specialized ML training algorithms such as SVM [9], LR [30], Linear Regression [31] and NB [14]. In order to handle complex non-linear function, PHE-based schemes usually depend on the untrusted servers [9], and use an approximate equation to simplify the complex iteration formula into a simple one¹ [5, 30]. Gonzlez et al. [9] developed a secure addition algorithm and a secure subtraction algorithm for constructing a secure SVM training algorithm, while some operations that are not supported by Paillier have to be implemented with the assistance of the untrusted servers. Mandal et al. proposed PrivFL [11], which guarantees data and model privacy and fits Federated Learning setting. But it delegates most of heavy cryptographic computations to data owners, which cannot match IoT setting where IoT data owners are usually resource-constrained.

In aggregation scenarios. Several works explored privacy-preserving aggregate statistics employing DP in the aggregation scenario [32, 33]. Training algorithms generally contain multiple iterations, thus noise-based DP is not a good choice for accuracy concern [7, 41]. Although, many efforts have been done for making Fully Homomorphic Encryption (FHE) practical, FHE is still unsuitable for general purpose applications [42]. Keith et al. [34] designed a protocol for secure aggregation of high-dimensional data. Their protocol allows a server to compute the sum of user-held data vectors from mobile devices. Shoukry et al. [35] considered a problem where multiple agents participate in solving a quadratic optimization problem. They proposed a PHE based protocol finding the optimal solution, where the privacy of the proposed protocol was analyzed by the zero-knowledge proofs. Mittal et al. [36] proposed a secure k-means data mining approach based on PHE.

Li et al. [10] proposed a server-aid framework for training multilayer perceptron in the aggregation scenarios. They intro-

duce an untrusted server to assist the secure training and ignore the collusion situation. Once the untrusted server colludes with model demanders or data owners, the confidentiality of models and datasets is not guaranteed. Mohassel et al. [5] proposed a privacy-preserving machine learning scheme with two untrusted but non-colluding servers. Their setting is similar to ours if we treat one server as the model demander and authorize it as the final model. But when an untrusted server is treated as the model demander, it will collude with the other server and figure out the plaintext training dataset.

Privacy-preserving data aggregation resembles the aggregation scenario, which is a kind of fundamental algorithm widely applied in Internet of Things [16], smart grid [17], wireless sensor networks [18], etc. Since privacy-preserving data aggregation achieves simple operations compared to ML training such as secure summation, it cannot handle the privacy-preserving ML training problem directly.

Although there are respectable studies on privacy-preserving training as listed in Table II, solutions for the aggregation scenario mainly rely on server-aid mode and cannot resist the threat of the collusion between the model demander and data owners. In this paper, we propose a general privacy-preserving framework, which can construct multiple privacy-preserving ML training protocols (including LR without simplification) that can guarantee security under the collusion situations.

III. SYSTEM OVERVIEW

This section presents the system model, the threat model, and the security definitions used in this paper.

A. System Model

We envision a data-driven IoT ecosystem, shown in Fig. 1, including IoT devices, IoT data owners and a model demander:

- **IoT devices** are responsible for sensing and transmitting valuable IoT data through wireless or wired networks.
- **Data owners** collect all pieces of the IoT data from the IoT devices within their own domains.

¹ $\log\left(\frac{1}{1+\exp(u)}\right) \approx \sum_{j=0}^k a_j \cdot u^j$

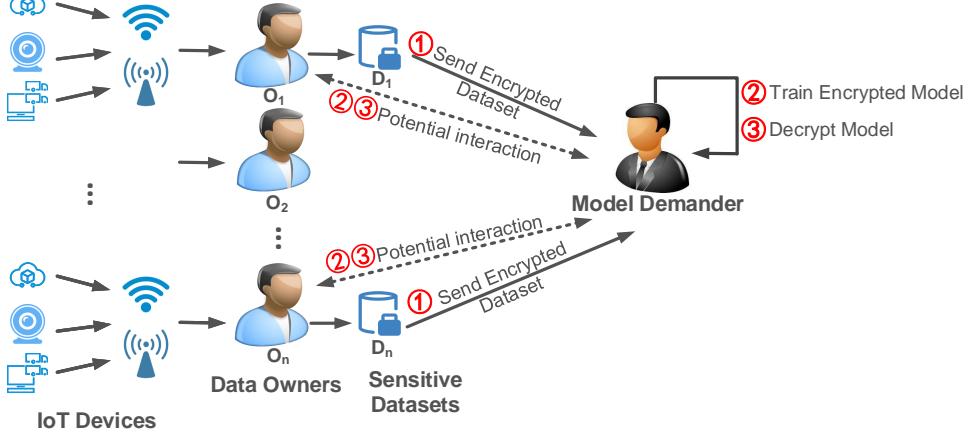


Fig. 1. Aggregation Scenario: a model demander learns the model only, and data owners neither know the model information nor other data owners' data.

- **Model demander** wants to training a ML model upon the dataset gathered from multiple data owners.

We assume that all participants have agreed upon the system of Heda to jointly train a model, and each data owner consents to releasing the model to the server. Every data owner generates its personal key pair to encrypted its data locally, and the model demander also holds his own key pair for model encryption.

Formally, our system consists of n data owners O_i ($i \in \{1, \dots, n\}$) and one untrusted model demander \mathcal{A} . Each data owner O_i holds a dataset D_i that contains users' sensitive information. This work considers *horizontal data sharing* [27, 43, 44], that is, the n datasets $\{D_i\}_{i=1}^n$ share the same feature space but different in samples. The model demander sequentially gathers the n encrypted data, and trains a ML model \mathcal{M} upon the dataset $\mathcal{D} := (D_1 \cup \dots \cup D_n)$, where $|\mathcal{D}| = \sum_{i=1}^n |D_i|$. After executing a privacy-preserving training protocol \mathcal{F} instantiated from Heda, the model demander obtains the desired model, i.e., the model parameters θ .

Security Goals: The privacy-preserving training protocol \mathcal{F} satisfies the following security requirements:

- The model demander cannot learn any sensitive information in the dataset \mathcal{D} .
- Every data owner cannot know the model parameters θ .
- Each data owner O_i know nothing about other data owners' sensitive information.

B. Threat Model

All participants in our model do not trust one another. Each data owner may try to learn as much other data owners' sensitive data and the model demander's model information as possible by honestly executing the pre-defined protocol. And the model demander follows the protocol honestly, but it tries to infer data owners' sensitive data as much as possible from the values he learns. Therefore, for any participant, we assume it is the passive (or honest-but-curious) adversary [45], that is, it does follow the protocol, but it tries to infer other participants' privacy as much as possible from the values they learn.

The proposed building blocks (except secure summation) are in two-party computation setting which should be ensured secure in the honest-but-curious model. While the privacy-preserving ML training protocols constructed from building blocks are multi-party protocols, where participants may collude with each other to acquire more information for inferring other participants' privacy. In our solution, we allow $(n - 1)$ data owners at most collude with each other to steal the privacy of other participants, and $(n - 2)$ data owners at most collude with the model demander to steal the privacy of other participants. Notice that when n data owners collude with each other, they can compute the model results on their joint dataset straightforward, and defending this extreme situation is meaningless.

Our model may encounter external adversaries that illegally obtain the data in the transmission process for their purposes by Internet eavesdropping or other means. While external adversary can be controlled by setting up a confidential and authentic channel using existing common technology like TSL.

Complementary directions. Since we assume every data owner agrees on the Heda to release the global model to the server, Heda dose not consider information leakage from the model parameters at the server. Employing DP could alleviate the information leakage, as the suggestion of existing works [46, 47]. While there are multiple attacks against ML. Protecting against these attacks is a complementary problem to that solved by Heda, and the corresponding solutions can be plugged into Heda.

C. Security Definition

To justify the security of two-party computation, we adapt Secure Two-party Computation framework [26, 31, 45]. To enable us to compose the building blocks into a privacy-preserving ML training protocol in a modular way securely, we invoke Modular Sequential Composition [39].

Secure Two-party Computation. For two-party protocols, to ensure security, we have to show that whatever A (B) can compute from its interactions with B (A) can be computed from its input and output, which leads to a commonly used definition, i.e., secure two-party computation [26, 31, 45].

Let $F = (f_A, f_B)$ be a (probabilistic) polynomial function. π is a protocol computing F . A and B want to compute $F(a, b)$ where a is A's input and b is B's input. The view of party A during the execution of π is the tuple $view_A^\pi(a, b) = (a, r, m_1, m_2, \dots, m_n)$ where m_1, m_2, \dots, m_n are the messages received from B, r is A's random tape. The view of B is defined similarly. Secure Two-party Computation is stated formally as follows:

Definition 1 (Secure Two-Party Computation [45]). *A two-part protocol π privately computes f if for all possible inputs (a, b) and simulators S_A and S_B hold the following properties:*

$$S_A(a, f_A(a, b)) \equiv_c view_A^\pi(a, b)$$

$$S_B(b, f_B(a, b)) \equiv_c view_B^\pi(a, b)$$

where \equiv_c denotes computational indistinguishability against Probabilistic Polynomial Time (PPT) adversaries with negligible advantage in the security parameter λ [37].

More details of computational indistinguishability can be found in Appendix B.

Modular Sequential Composition. Since all our protocols are designed and constructed in a modular way, we employ Modular Sequential Composition [39] for justifying the security proofs of our protocols, the detailed idea of which can be found in Appendix B.

Definition 2 (Modular Sequential Composition [39]). *Let f_1, \dots, f_n be two-party probabilistic polynomial time functionalities and ρ_1, \dots, ρ_n protocols that securely compute respectively f_1, \dots, f_n in the presence of semi-honest adversaries. Let F be a probabilistic polynomial time functionality and π a protocol that securely computes F with f_1, \dots, f_n in the presence of semi-honest adversaries. Then $\pi^{\rho_1, \rho_2, \dots, \rho_n}$ securely computes F in the presence of semi-honest adversaries.*

IV. PRELIMINARY

This section presents the PHE preliminaries used in this paper. ML preliminaries used in this paper can be found in Appendix C. Before presenting the main content, we summarize the notations used in paper as follows. A dataset \mathcal{D} is an unordered set with the size of $|\mathcal{D}|$. x denotes a scalar. $\mathbf{x} \in \mathbb{R}^d$ denotes a vector. $\mathbf{x}_i = [x_{i1}, x_{i2}, \dots, x_{id}]$ is the i-th record in dataset \mathcal{D} . Each record has d features. y_i is the class label correspond to \mathbf{x}_i . $X = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{|\mathcal{D}|}\}$, $Y = \{y_1, y_2, \dots, y_{|\mathcal{D}|}\}$. θ are the learnable parameters of ML models. $[m]_P$ denotes a message m encrypted by Paillier. $[m]_R$ denotes a message m encrypted by Cloud-RSA. $[m]$ denotes an encrypted message m that is encrypted with a non-specified cryptosystems. Important notations are present in Table III.

Public-key cryptosystems employ a pair of keys (PK, SK), the public key (PK, the encryption key) and the private key (SK, the decryption key). Some cryptosystems are gifted with a homomorphic property that can perform a set of operations on encrypted data without knowledge of the decryption key. Formalized definition of homomorphic can be found in Appendix L.

TABLE III
LIST OF NOTATIONS

Notation	Meaning
n	the number of data owners participating in scenario
\mathcal{D}_i	dataset from the i -th data owner
\mathcal{D}	training dataset gathered from multiple data owners
d	the number of features in \mathcal{D}
\mathbf{x}_i	the i -th record in training dataset \mathcal{D}
y_i	the class label correspond to \mathbf{x}_i
θ	learnable parameters of ML models
$[m]_P$	a message encrypted by Paillier
$[m]_R$	a message encrypted by Cloud-RSA
$[m]$	a message encrypted by a non-specified cryptosystems

Two public-key cryptosystems are employed in this paper: Paillier [37] and Cloud-RSA [38]. Paillier possesses additively homomorphic properties, and Cloud-RSA possesses multiplicative. Ciphertext indistinguishability against chosen plaintext attacks [37] ensures that no bit of information is leaked from ciphertexts. We prove the security of the proposed algorithms and protocols based on the semantic security [37] of Paillier and Cloud-RSA. Let GenModulus be a polynomial-time algorithm that, on input 1^n , outputs (N, p, q) where $N = pq$ and p and q are n-bit primes [37]. We restate the definitions of Paillier and Cloud-RSA as following.

Paillier. The security of Paillier is based on the Decisional Composite Residuosity assumption.

- Gen: run GenModulus(1^n) to obtain (N, p, q) . The public key is N , and the private key is $(N, \phi(N))$.
- Enc: on input a public key N and a message $m \in \mathbb{Z}_N$, choose an uniform $r \leftarrow \mathbb{Z}_N^*$ and output the ciphertext $c := [(1 + N)^m r^N \text{mod} N^2]$.
- Dec: on input a private key $(N, \phi(N))$ and a ciphertext c , output the message $m := [\frac{[c^{\phi(N)} \text{mod} N^2] - 1}{N} \phi(N)^{-1} \text{mod} N]$.

Assuming a pair of ciphertext (c_1, c_2) is (m_1, m_2) under the same Paillier encryption scheme, we have $c_1 \times c_2 = (1 + N)^{m_1+m_2} r^N \text{mod} N^2$, $m_1 + m_2 \in \mathbb{Z}_N$, i.e., $\text{Paillier.Enc}(m_1 + m_2) = \text{Paillier.Enc}(m_1) * \text{Paillier.Enc}(m_2)$

Cloud-RSA. RSA relies on the hardness of factoring assumption. Although RSA is commonly used for ensuring the authenticity of digital data, many attacks still threaten the security of RSA, such as Factorization attacks and Low private exponent attacks [48, 48, 49]. To strengthen RSA security, Optimal Asymmetric Encryption Padding scheme has been proposed in order to convert the RSA into a probabilistic encryption scheme and to achieve semantic security. But Optimal Asymmetric Encryption Padding scheme removes the multiplicative homomorphic property from RSA. To address the drawbacks of RSA, Khalid et al. [38] has proposed an enhanced encryption scheme named Cloud-RSA which keeps the multiplicative homomorphic property of the plain RSA and can resist the well-known attacks. Cloud-RSA encryption scheme (Gen, Enc, Dec) is given:

- Gen: run GenModulus(1^n) to obtain (N, p, q) . choose $e > 1$ such that $\text{gcd}(e, \phi(N)) = 1$. compute $d := [e^{-1} \text{mod} \phi(N)]$. The public key is (N) , and private key is (N, e, d) . Both the public key and private key of Cloud-RSA are hold by data owners.

- Enc: on input a message $m \in \mathbb{Z}_N^*$, output the ciphertext $c := [m^e \text{mod} N]$.
- Dec: on input a ciphertext $c \in \mathbb{Z}_N^*$, output the message $m := [c^d \text{mod} N]$.

For security proof details about Cloud-RSA, we refer the reader to [38]. Assuming a pair of ciphertext (c_1, c_2) is (m_1, m_2) under the same Cloud-RSA encryption scheme, we have $c_1 \times c_2 = (c_1 c_2)^e \text{mod} N$, $c_1 c_2 \in \mathbb{Z}_N^*$, i.e.,
 $\text{CloudRSA}.\text{Enc}(m_1 m_2) = \text{CloudRSA}.\text{Enc}(m_1) * \text{CloudRSA}.\text{Enc}(m_2)$

V. BUILDING BLOCKS BASED ON PARTIAL HOMOMORPHIC ENCRYPTION

This section details the design idea of Heda and the PHE-based library of building blocks. Table IV lists the different cases for each building block. For all building blocks, both parties cannot obtain other useful information except for the legal information.

Security Proofs. Formal cryptographic proofs of the building blocks requires space beyond the page limit. Hence, we provide the intuition behind the proofs, and delegate formal proofs to Appendix H.

A. Design Idea

Just as a mathematical formula can be decomposed into the permutation and combination of addition, subtraction, multiplication, and division, ML training algorithms can also be decomposed into a set of core primitive operations. Intuitively, we can design secure building blocks for each of core primitive operations and appropriately combine them into the desire ML training protocols that satisfy the security requirements in the aggregation scenario.

After analyzing the typical supervised learning algorithms (i.e., LR, SVM, and NB), we include addition, subtraction, multiplication, power function, and summation as the core primitive operations, see Table V for detail. Hence, we design secure building blocks targeting each of these core operations.

Nevertheless, using the above secure building blocks is inadequate for the security requirements in the aggregation scenario. Since there are n data owners in Heda, and each data owner has their own encryption schemes (i.e., a certain plaintext-ciphertext space with a pair of keys (PK,SK)). Data owners send the ciphertext data encrypted by its public key to the model demander. Homomorphic operations upon the ciphertext can only be operated in the same plaintext-ciphertext space. The model demander has to update the model parameters upon the encrypted data under different plaintext-ciphertext spaces.

To supplement and enable a building block's output to become the input of another, while maintaining the underlying plaintext, we design two building blocks for converting from the ciphertext under Cloud-RSA to under Paillier and converting the ciphertext under one data owner's Paillier encryption to the other data owner's Paillier encryption.

B. Building Blocks for Primitive Operations

Since it is plain to obtain the secure addition, subtraction and multiplication, we include them in the library of building blocks directly:

- Building Block 1: secure addition with Paillier.
- Building Block 2: secure subtraction with Paillier.
- Building Block 3: secure plaintext-ciphertext multiplication with Cloud-RSA.
- Building Block 4: secure ciphertext-ciphertext multiplication with Cloud-RSA.

Proposition V.1. *Building Block 1-4 is secure in the honest-but-curious model.*

Proof Intuition V.1 (for Proposition A.1). The security property of the four building blocks is straightforward by ciphertext indistinguishability against chosen plaintext attacks of Paillier and Cloud-RSA. See Appendix H for a complete proof. \square

Designing secure power function and secure summation is not straightforward. This paper novelly proposes secure power function and secure summation. From here onwards, we introduce our particularly designed building blocks.

Building Block 5 : Secure Power Function. The key to securely computing $\text{Sigmoid}(\beta^\top \mathbf{x}) = \frac{e^{\beta^\top \mathbf{x}}}{1 + e^{\beta^\top \mathbf{x}}}$ is to compute $e^{\beta^\top \mathbf{x}}$.

Supposing a data owner encrypts $e^{\mathbf{a}} = \{e^{a_1}, e^{a_2}, \dots, e^{a_d}\}$ by his Cloud-RSA public key and sends the ciphertext $[e^{\mathbf{a}}]_R$ to a model demander. The model demander has $\mathbf{b} = \{b_1, b_2, \dots, b_d\}$, and he wants to obtain $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$.

$$\begin{aligned} [e^{\mathbf{a} \cdot \mathbf{b}}]_R &= [e^{a_1 b_1 + a_2 b_2 + \dots + a_d b_d}]_R \\ &= \prod_{i=1}^d [e^{a_i b_i}]_R = \prod_{i=1}^d ([e^{a_i}]_R)^{b_i} \end{aligned} \quad (1)$$

Equation (1) specifies our secure power function. The key point is that $e^{a_i b_i}$ equals multiplying e^{a_i} multiplied by itself b_i times. Along this way, the model demander is able to obtain $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ by $(\sum_{i=1}^d b_i + d - 1)$ times multiplication.

Proposition V.2. *Secure power function is secure in the honest-but-curious model.*

Proof Intuition V.2 (for Proposition A.2). The data owner does not any message, his view only consists in its input. The model demander do computation on the ciphertext encrypted by the data owner's public key. By ciphertext indistinguishability against chosen plaintext attacks of Cloud-RSA, the model demander cannot learn any useful information. See Appendix H for a complete proof. \square

Building Block 6 : Secure Summation. There are n data owners. Each data owner \mathcal{O}_i holds a value a_i . Without decryption and revealing the values to the model demander, the model demander desire to obtain the summation of the n values $\{a_i\}_{i=0}^n$. Our secure summation solution is described Building Blocks 6.

Specifically, \mathcal{A} removes the encrypted noise $\sum_{i=1}^n r_i$ from res' that is obtained at the step 7 of Building Blocks 6 as following:

- (i) *From the first data owner to the last, \mathcal{A} sequentially computes $[\text{res}']_P^i := [\text{res}' - r_i]_P^i$ using secure subtraction, and converts $[\text{res}']_P^i$ to $[\text{res}']_P^{i+1}$ by Building Block 8.*
- (ii) *Finally, using Building Block 8, \mathcal{A} converts $[\text{res}]_P := \text{res}' - \sum_{i=1}^n r_i$ which is encrypted by the last data owner's Paillier public key to $[\text{res}]_P^A$ that is encrypted by itself.*

TABLE IV
THE CASES OF BUILDING BLOCKS

Algorithms	Input		Output
	Data Owner	Model Demander	
Secure addition	$(\text{SK}, \text{PK})_{\text{Paillier}}, [a]_P$	$[b]_P$	$[a + b]_P$
Secure subtraction	$(\text{SK}, \text{PK})_{\text{Paillier}}, [a]_P$	$[b]_P$	$[a - b]_P$
Secure plaintext-ciphertext multiplication	$(\text{SK}, \text{PK})_{\text{Paillier}}, [a]_P$	b	$[a * b]_P$
Secure plaintext-ciphertext dot product	$(\text{SK}, \text{PK})_{\text{Paillier}}, [a]_P$	\mathbf{b}	$[\mathbf{a} \cdot \mathbf{b}]_P$
Secure ciphertext-ciphertext multiplication	$(\text{SK}, \text{PK})_{\text{CloudRSA}}, [a]_R$	$[b]_R$	$[a * b]_R$
Secure power function	$(\text{SK}, \text{PK})_{\text{CloudRSA}}, [e^{\mathbf{a}}]_R$	\mathbf{b}	$[e^{\mathbf{a} \cdot \mathbf{b}}]_R$
Secure summation	$(\text{SK}, \text{PK})_{\text{Paillier}}, a_i$	$(\text{SK}, \text{PK})_{\text{Paillier}}^A$	$\sum_{i=1}^n a_i$
Converting $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ to $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$	$(\text{SK}, \text{PK})_{\text{Paillier}}, (\text{SK}, \text{PK})_{\text{CloudRSA}}$	$[e^{\mathbf{a} \cdot \mathbf{b}}]_R$	$[e^{\mathbf{a} \cdot \mathbf{b}}]_P$
Converting $[m]_P^1$ to $[m]_P^2$	$(\text{SK}, \text{PK})_{\text{Paillier}}^1, (\text{PK})_{\text{Paillier}}^2$	$[m]_P^1$	$[m]_P^2$

TABLE V
CORE OPERATION OF MACHINE LEARNING TRAINING

Operations	Add.	Sub.	Multi.	Pow	Comp.	Sum.
LR	✓	✓	✓	✓		
SVM	✓	✓	✓		✓	
NB	✓		✓			✓

Building Block 6: Secure Summation

Participants: n data owners, one model demander
Each Data Owner (\mathcal{O}) Input: $(\text{PK}, \text{SK})_{\text{Paillier}}^i$ and a_i
Model Demander (\mathcal{A}) Input : $(\text{PK}, \text{SK})_{\text{Paillier}}^A$
Model Demander (\mathcal{A}) Output: $\sum_{i=1}^n a_i$

```

1 for  $i = 1$  to  $n$  do
2    $\mathcal{O}_i$  uniformly picks  $r_i \in \mathbb{Z}_N$ ;
3    $\mathcal{O}_i$ :  $\hat{a}_i = a_i + r_i$ ;
4    $\mathcal{O}_i$ :  $[r_i]_P^i := \text{Paillier}^i.\text{Enc}(r_i)$ ;
5    $\mathcal{O}_i$  sends  $[r_i]_P^i$  and  $a_i + r_i$  to  $\mathcal{A}$ ;
6 end
7  $\mathcal{A}$ :  $\hat{r}_{\mathcal{E}} = \sum_{i=1}^n (a_i + r_i)$ ;
8  $\mathcal{A}$ :  $[\hat{r}_{\mathcal{E}}]_P^1 := \text{Paillier}^1.\text{Enc}(\hat{r}_{\mathcal{E}})$ ;
9 for  $i = 1$  to  $n - 1$  do
10   $\mathcal{A}$ :  $[\hat{r}_{\mathcal{E}}]_P^i := [\hat{r}_{\mathcal{E}}]_P^i * ([r_i]_P^i)^{(-1)}$  ;
11   $\mathcal{A}$ : converts  $[\hat{r}_{\mathcal{E}}]_P^i$  to  $[\hat{r}_{\mathcal{E}}]_P^{i+1}$  by Building Block 8;
12 end
13  $\mathcal{A}$ :  $[\hat{r}_{\mathcal{E}}]_P^n := [\hat{r}_{\mathcal{E}}]_P^n * ([r_n]_P^n)^{(-1)}$  ;
14  $\mathcal{A}$ : converts  $[\hat{r}_{\mathcal{E}}]_P^n$  to  $[\hat{r}_{\mathcal{E}}]_P^A$  by Building Block 8;
15  $\mathcal{A}$ :  $res := \text{Paillier}^A.\text{Dec}([\hat{r}_{\mathcal{E}}]_P^A)$             $\triangleright res = \sum_{i=1}^n a_i$ ;
16 return  $\sum_{i=1}^n a_i$  to  $\mathcal{A}$ .
```

Proposition V.3. *Secure summation is secure in the honest-but-curious model.*

Proof Intuition V.3 (for Proposition A.3). The data owners add random noise r_i to a_i , the random noise hides a_i in an information-theoretic way (it is an one-time pad). Even though the model demander receives $[r_i]_P^i$, the ciphertext indistinguishability against chosen plaintext attacks of Paillier prevents it figure out the a_i from $r_i + a_i$. Besides, the Building Block 8 is secure in the honest-but-curious model, we obtain the security of secure summation using the definition of Modular Sequential Composition.

As for the collusion situations, when $(n - 1)$ data owners collude with each other and the data owner \mathcal{O}_i dose not participate in the collusion, they can only figure out $a_i + r_i$ and $\sum_{c=1}^n a_c + r_i$ cannot obtain a_i or $\sum_{c=1}^n a_c$. When $(n - 2)$ data owners collude with the model demander, and \mathcal{O}_{i-1} and

\mathcal{O}_i do not participate in the collusion, they can only figure out $a_{i-1} + a_i$ cannot obtain a_i or a_{i-1} .

See Appendix H for a complete proof. \square

C. Building Blocks for Conversion

Since multiple encryption schemes are used in Heda, we developed two protocols for converting ciphertexts from one encryption scheme to another while maintaining the underlying plaintexts.

Building Block 7 : Converting Cloud – RSA to Paillier ($[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ to $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$).

The model demander holds a ciphertext $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ encrypted under a data owner's Cloud-RSA public key. For continuing to the subsequent ciphertext computations, the model demander needs to convert $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ to the ciphertext encrypted by the data owner's Paillier public key. During the conversion, $e^{\mathbf{a} \cdot \mathbf{b}}$ is confidential to the model demander and the data owner.

Building Block 7: Converting $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ to $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$

Data Owner (\mathcal{O}) Input: $(\text{PK}, \text{SK})_{\text{Paillier}}$ and $(\text{PK}, \text{SK})_{\text{CloudRSA}}$

Model Demander (\mathcal{A}) Input: $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$

Model Demander (\mathcal{A}) Output: $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$

```

1  $\mathcal{A}$  randomly picks  $r$ ;
2  $\mathcal{A}$ :  $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_R := [e^{\mathbf{a} \cdot \mathbf{b}}]_R * [e^r]_R$ ;
3  $\mathcal{A}$  sends  $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_R$  to  $\mathcal{O}$ ;
4  $\mathcal{O}$ :  $e^{\mathbf{a} \cdot \mathbf{b} + r} := \text{CloudRSA}.\text{Dec}([e^{\mathbf{a} \cdot \mathbf{b} + r}]_R)$ ;
5  $\mathcal{O}$ :  $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_P := \text{Paillier}.\text{Enc}(e^{\mathbf{a} \cdot \mathbf{b} + r})$ ;
6  $\mathcal{O}$  sends  $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_P$  to  $\mathcal{A}$ ;
7  $\mathcal{A}$ :  $[e^{\mathbf{a} \cdot \mathbf{b}}]_P := ([e^{\mathbf{a} \cdot \mathbf{b} + r}]_P)^{e^{-r}}$ ;
8 return  $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$  to  $\mathcal{A}$ ;
```

The correctness analysis is as follows: The model demander randomly picks a random noise r , generates $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_R$ by secure ciphertext-ciphertext multiplication. Then the data owner decrypts $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_R$ with its $\text{SK}_{\text{CloudRSA}}$ and encrypts it with its $\text{PK}_{\text{Paillier}}$, obtaining $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_P$. Using secure plaintext-ciphertext multiplication, the model demander multiplies $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_P$ by e^{-r} to remove e^r .

Proposition V.4. *Secure converting $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ to $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$ is secure in the honest-but-curious model.*

Proof Intuition V.4 (for Proposition A.4). Even though the data owner is able to decrypt and obtain $e^{\mathbf{a} \cdot \mathbf{b} + r}$, the random noise r hides $\mathbf{a} \cdot \mathbf{b}$ in an information-theoretic way (it is an one-time pad). See Appendix I for a complete proof. \square

Building Block 8 : Converting one Paillier to Another Paillier ($[m]_P^1$ to $[m]_P^2$).

Building Block 8: Converting $[m]_P^1$ to $[m]_P^2$

- Data Owner (O) Input:** $(\text{PK}, \text{SK})_{\text{Paillier}}^1$ and $(\text{PK}, \text{SK})_{\text{Paillier}}^2$
- Model Demander (A) Input:** $[m]_P^1$
- Model Demander (A) Output:** $[m]_P^2$
- 1 \mathcal{A} uniformly picks $r \in \mathbb{Z}_N$;
 - 2 $\mathcal{A} : [m+r]_P^1 := [m]_P^1 * [r]_P^1$;
 - 3 \mathcal{A} sends $[m+r]_P^1$ to \mathcal{O} ;
 - 4 $\mathcal{O} : m+r := \text{Paillier}^1.\text{Dec}([m+r]_P^1)$;
 - 5 $\mathcal{O} : [m+r]_P^2 := \text{Paillier}^2.\text{Enc}(m+r)$;
 - 6 \mathcal{O} sends $[m+r]_P^2$ to \mathcal{A} ;
 - 7 $\mathcal{A} : [m]_P^2 := [m+r]_P^1 * [r]_P^{-1}$;
 - 8 **return** $[m]_P^2$ to \mathcal{A} ;
-

The model demander holds a ciphertext $[m]_P^1$ encrypted by the Paillier encryption of data owner 1. He wants to convert $[m]_P^1$ to the ciphertext $[m]_P^2$ encrypted by another data owner's Paillier encryption. During the conversion, the message m is revealed to the data owners or the model demander. Building Block 8 achieves the switching of $[m]_P^1$ to $[m]_P^2$.

In Building Block 8, the model demander adds a random noise r to $[m]_P^1$ by secure addition, obtaining $[m+r]_P^1$. Then the data owner 1 decrypts the resulting value with his $\text{SK}_{\text{Paillier}}$ and encrypts it with the other data owner's Paillier key, obtaining $[m+r]_P^2$. The model demander is able to remove r from $[m+r]_P^2$ by using secure subtraction.

Proposition V.5. *Secure converting $[m]_P^1$ to $[m]_P^2$ is secure in the honest-but-curious model.*

Proof Intuition V.5 (for Proposition A.5). The model demander adds random noise to the ciphertext $[m]_P^1$. Even though the data owner is able to decrypt and obtain $m+r$, the random noise r hides m in an information-theoretic way (it is an one-time pad). See Appendix I for a complete proof. \square

VI. PRIVACY-PRESERVING MACHINE LEARNING TRAINING WITH HEDA

In this section, we detail how to construct the privacy-preserving ML training protocols using the proposed building blocks. Since these building blocks are designed in a modular way, so carrying the privacy-preserving ML training come down to invoking the right module.

For performing Stochastic Gradient Descent (SGD), the model demander randomly selects a small number of records from \mathcal{D} in each iteration. Since the dataset \mathcal{D} is gathered sequentially, the model demander is able to locate the data owner that the selected records belong to, which facilitates subsequent ciphertext computations, i.e., the model demander encrypts the correlative parameters using the picked data owner's public key. ML preliminaries used in this paper can be found in Appendix C.

Both Paillier and Cloud-RSA work with positive integers in a finite space, while the three ML training algorithms manipulate floating point numbers. Hence, after detailed secure training algorithms, we present the solution for dealing with floating point numbers.

A. Secure Support Vector Machine Training

This paper adopts Hinge Loss with SGD for solving SVM, which involves the less amount of vector multiplication than other optimization methods [50]. We restate the iteration equation:

$$\theta := \theta - \lambda(\alpha\theta - \alpha y_i \hat{\mathbf{x}}_i). \quad (2)$$

In iteration, the key points are two multiplication $\lambda\alpha y_i \hat{\mathbf{x}}_i$ and $\theta^\top y_i \hat{\mathbf{x}}_i$. From the perspective of the model demander, $\lambda\alpha y_i \hat{\mathbf{x}}_i$ and $\theta^\top y_i \hat{\mathbf{x}}_i$ belong to the plaintext-ciphertext multiplication, where $y_i \hat{\mathbf{x}}_i$ is unseen but $\lambda\alpha$ and θ are known. Thus, the two multiplications are coped with by secure plaintext-ciphertext multiplication. Fig. 2 specifies our secure SVM training protocol instantiated from Heda, which needs 3 interactions (i.e. interactions between the model demander and data owners) throughout each iteration.

Proposition VI.1. *Privacy-preserving SVM training protocol is secure in the honest-but-curious model.*

Proof Intuition VI.1 (for Proposition A.6). No collusion happen: Data owners do not receive any message in the protocol except for the auxiliary execution of secure building blocks. All the training data is ciphertext that is encrypted by corresponding data owners. The model demander can only infer the training data from the model parameters, which is a ciphertext-only attack with perfectly secret [37]. As Building Block used in this protocol are secure in the honest-but-curious model, we obtain the security using modular sequential composition.

As for the collusion situations, since the training data and model parameters are encrypted by corresponding data holders with their own public key. Without all the data owners participating in the collusion, data owners cannot figure out the complete model information. Without the corresponding private key, the ciphertext indistinguishability of Paillier ensures that no bit of information is leaked from ciphertexts of other data owners who do not participating in the collusion.

See Appendix B for a complete proof and the definition of ciphertext-only attack and perfectly secret. \square

B. Secure Logistic Regression Training

Here recalls the iteration equation of LR:

$$\theta_j := \theta_j - \lambda(x_{ij}y_i - \frac{x_{ij}}{1 + e^{-\theta^\top \mathbf{x}_i}}) \quad (3)$$

The complex part in Equation (12) is the Sigmoid function $\frac{x_i}{1 + e^{-\theta^\top \mathbf{x}_i}}$. By adapting secure power function, the model demander obtains $[e^{-\theta^\top \mathbf{x}_i}]_R$ first. Then, as specified in Fig. 3, the results in the operations of the model demander evolve as follows:

$$[e^{-\theta^\top \mathbf{x}_i}]_R \rightarrow [e^{-\theta^\top \mathbf{x}_i}]_p \rightarrow [e^{-\theta^\top \mathbf{x}_i} + 1]_p \rightarrow [e^{-\theta^\top \mathbf{x}_i + r} + e^r]_p$$

The model demander sends $[e^{-\theta^\top \mathbf{x}_i + r} + e^r]_p$ to data owners. The data owner carries on computations as following:

$$[e^{-\theta^\top \mathbf{x}_i + r} + e^r]_p \rightarrow e^{-\theta^\top \mathbf{x}_i + r} + e^r \rightarrow \frac{\mathbf{x}_i}{e^{-\theta^\top \mathbf{x}_i + r} + e^r}$$

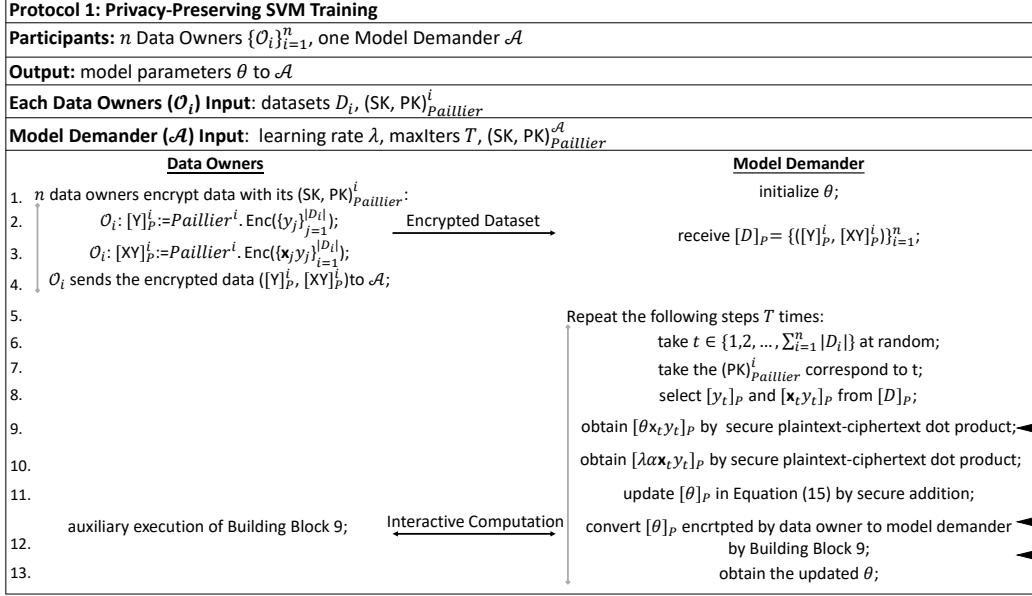


Fig. 2. Privacy-Preserving Support Vector Machine Training Protocol

The data owner returns the encrypted resulting value $[\frac{\mathbf{x}_i}{(e^{-\theta^T \mathbf{x}_i} + 1) * e^r}]_P$ to the model demander. Finally, removing the noise e^r , the model demander get $[\frac{\mathbf{x}_i}{1 + e^{-\theta^T \mathbf{x}_i}}]_P$. Fig. 3 specifies the privacy-preserving LR training protocol, which needs 4 interactions (i.e. interactions between the model demander and data owners) throughout each iteration.

Proposition VI.2. *Privacy-preserving LR training protocol is secure in the honest-but-curious model.*

Proof Intuition VI.2 (for Proposition A.7). No collusion happen: In the process of sigmoid function solution, even though the data owners is able to decrypt $e^{-\theta^T \mathbf{x}_i + r} + e^r$, the random noise r hides θ in an information-theoretic way (it is an one-time pad). All the training data is ciphertext that is encrypted by corresponding data owners. The model demander can only infer the training data from the model parameters, which is a ciphertext-only attack with perfectly secret. The collusion situations is similar as Protocol 1, so we do not repeat them here. See Appendix J for a complete proof. \square

C. Secure Naive Bayes Training

For learning a NB model from dataset \mathcal{D} , the model demander needs to compute the the class prior probability $P(y)$ and the conditional probability $P(\mathbf{x}_i|y)$.

$$P(\mathbf{x}_i|y) := \begin{cases} \frac{|\mathcal{D}^y(x_{ij})|}{m}, & \text{discrete attribute} \\ \frac{1}{\sqrt{2\pi}\sigma_{y,j}} \exp\left(-\frac{(x_{ij} - \mu_{y,j})^2}{2\sigma_{y,j}^2}\right), & \text{numeric attribute} \end{cases} \quad (4)$$

If the j -th attribute is a discrete attribute, the conditional probability is $P(x_{ij}|y) = \frac{|\mathcal{D}^y(x_{ij})|}{m}$, where the total number of records m is public [8] without loss of generality. $|\mathcal{D}^y(x_{ij})|$ is the number of records belonging to class y with the attribute value x_{ij} in \mathcal{D} . Since there are n data owners in the aggregation scenario, $|\mathcal{D}^y(x_{ij})| = \sum_{c=1}^n |\mathcal{D}_c^y(x_{ij})|$.

The class prior probability i.e., $P(y) = \frac{\sum_{c=1}^n |\mathcal{D}_c(y)|}{m}$ has a similar computation manner with the conditional probability of discrete attributes, where $|\mathcal{D}_c(y)|$ is the number of records belonging to class y in \mathcal{D}_c .

If the j -th attribute is a numeric attribute, we assume that the j -th attribute obeys normal distribution, where two parameters need to be estimated securely: mean $\mu_{y,j}$ and variance $\sigma_{y,j}^2$.

$$\begin{aligned} \mu_{y,j} &= \frac{\sum_{i=1}^{|\mathcal{D}|} x_{ij}}{m} \\ \sigma_{y,j}^2 &= \frac{\sum_{i=1}^{|\mathcal{D}|} (\mu_{y,j} - x_{ij})^2}{m} = \frac{\sum_{i=1}^{|\mathcal{D}|} (\mu_{y,j})^2 + (x_{ij}^2 - 2\mu_{y,j}x_{ij})}{m} \\ &= \frac{\sum_{i=1}^{|\mathcal{D}|} (\mu_{y,j})^2}{m} + \frac{\sum_{i=1}^{|\mathcal{D}|} (x_{ij})^2}{m} - 2\mu_{y,j} * \frac{\sum_{i=1}^{|\mathcal{D}|} (x_{ij})}{m} \end{aligned} \quad (5)$$

Employing secure summation protocol, we obtain $\sum_{c=1}^n |\mathcal{D}_c(y)|$, $\sum_{c=1}^n |\mathcal{D}_c^y(x_{ij})|$, $\sum_{i=1}^{|\mathcal{D}|} x_{ij}$ and $\sum_{i=1}^{|\mathcal{D}|} (x_{ij})^2$ securely. Fig. 4 specifies our privacy NB training protocol. Since the conditional probability of each feature can be figured out concurrently, the number of interactions is depended on the number of involved secure summation algorithm, e.i., $n + 1$ interactions.

Proposition VI.3. *Privacy-preserving NB training protocol is secure in the honest-but-curious model.*

Proof Intuition VI.3 (for Proposition A.8). No collusion happen: Data owners do not receive any message in the protocol except for the auxiliary execution of secure building blocks. All the training data is ciphertext that is encrypted by corresponding data holders. As Building Block used in this protocol are secure in the honest-but-curious model, we obtain the security using modular sequential composition. The collusion situations is similar as Protocol 1, so we do not repeat them here. See Appendix J for a complete proof. \square

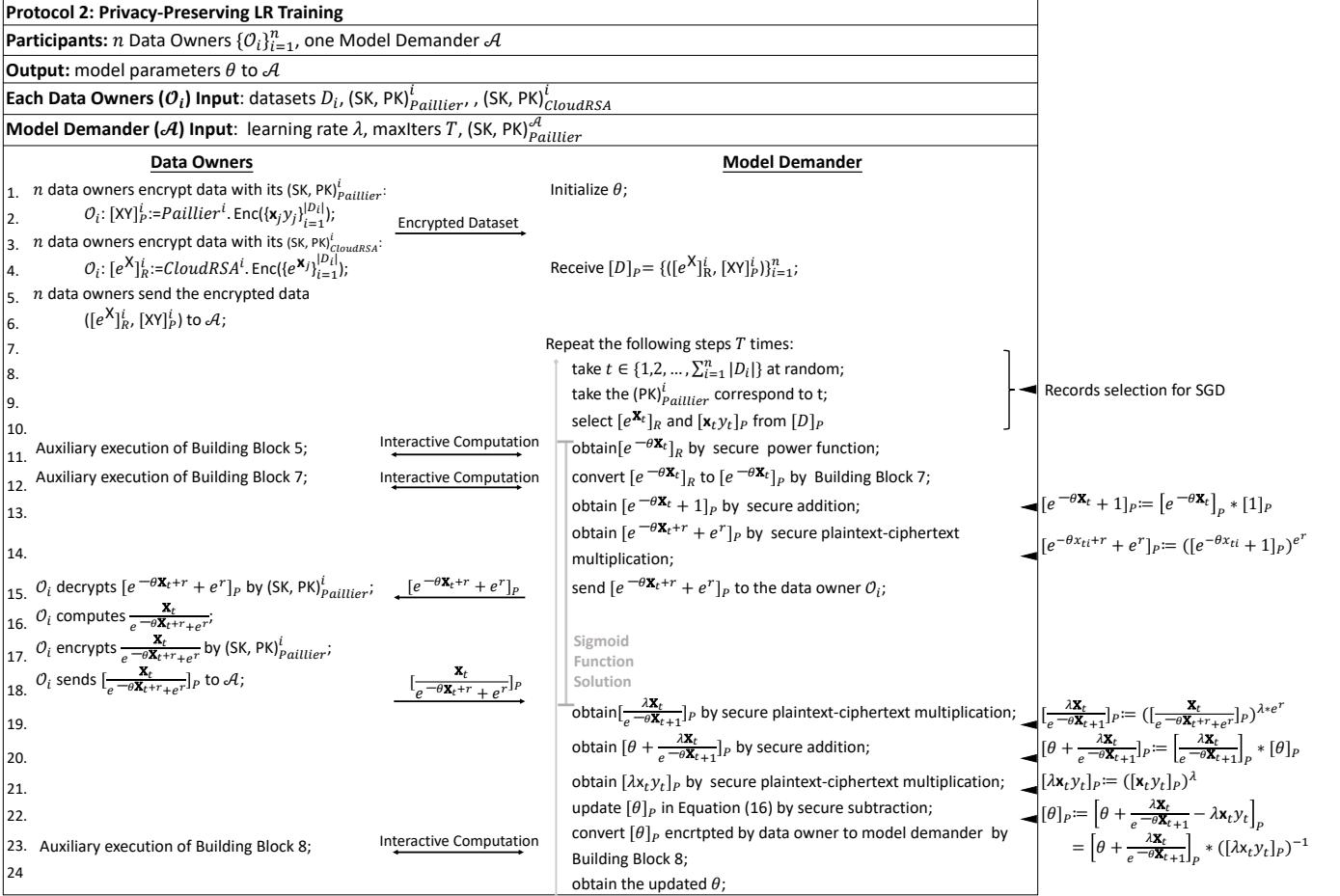


Fig. 3. Privacy-Preserving Logistic Regression Training Protocol

D. Dealing with Floating Point Numbers

The floating point number issues for PHE based secure ML training have been previously studied [9, 26]. Using similar idea, we perform the format conversion by multiplying each floating point value v by a big constant 10^e for fixed point representation. Empirically, we retained two decimal places (i.e., $e = 2$) for each floating point value involved in our implementation. Suppose v is a floating point number that is fixed to 2 decimal places in decimalism. Then,

$$(v)_{10} = \frac{(\hat{v})_{10}}{10^2}, \quad \hat{v} \in \mathbb{N}, \hat{v} > 0 \quad (6)$$

Without loss of generality, when facing the same training task, we assume that features of records in training dataset have been locally preprocessed and restricted in range $[0, 1]$. Despite the data standardization on training dataset, when the ciphertext is calculated many times, the \hat{v} may become very large integers, which might cause overflows errors. We must ensure $\log_{10} N > e^*$, where N denotes the modulus for Paillier or Cloud-RSA's cryptosystem, and e^* denotes $\log_{10} \hat{v}$. $\log_{10} N \approx 308$ when 1024-bit key length, and $\log_{10} N \approx 616$ when 2048-bit key length.

For Protocol 1. Referring to Fig. 2, at the end of each iteration, θ is refreshed with the format of Equation (6) ($e^* \leq 2$). There are 2 secure plaintext-ciphertext dot product for each

record throughout an iteration. 2048-bit key length is enough to control these computations.

For Protocol 2. Referring to Fig. 3, at the end of each iteration, θ is refreshed with the format of Equation (6) ($e^* \leq 2$). We discuss the situation of e^* in secure power function where $[e^{\mathbf{x}_i \cdot \theta}]_R$ is obtained by $(\sum_{i=1}^d \theta_i + d - 1)$ times multiplication of $[e^{\mathbf{x}_i}]_R$. Since, $e^* \leq 2$ for $[e^{\mathbf{x}_i}]_R$, we must ensure:

$$\log_{10} N > (\sum_{i=1}^d \theta_i + d - 1) * 2 \quad (7)$$

In the implementation of secure power function, we decompose θ_i into an integer part and a decimal part: $\theta_i = \theta_i^1 + \frac{\theta_i^2}{10^2}$, $\theta_i^1 \geq 0, 100 > \theta_i^2 \geq 1$. After obtaining $[e^{\mathbf{x}_i \cdot \theta_i^1}]_R$ and $[e^{\mathbf{x}_i \cdot \theta_i^2}]_R$, we merge the respective results for recovering: $e^{\theta_i \mathbf{x}_i} = e^{\theta_i^1 \mathbf{x}_i} * \sqrt[100]{e^{\theta_i^2 \mathbf{x}_i}}$. We provide a case study for explaining the recovering of $e^{\theta_i \mathbf{x}_i}$ from $[e^{\mathbf{x}_i \cdot \theta_i^1}]_R$ and $[e^{\mathbf{x}_i \cdot \theta_i^2}]_R$ in Appendix M. The key length of Cloud-RSA in Protocol 2 can be set appropriately according to Equation (7) and the number of features.

After secure power function, the e^* is refreshed to 2 in Building Block 8. Subsequent operations in an iteration, 3 secure plaintext-ciphertext multiplication, 2 secure addition, are controlled naturally.

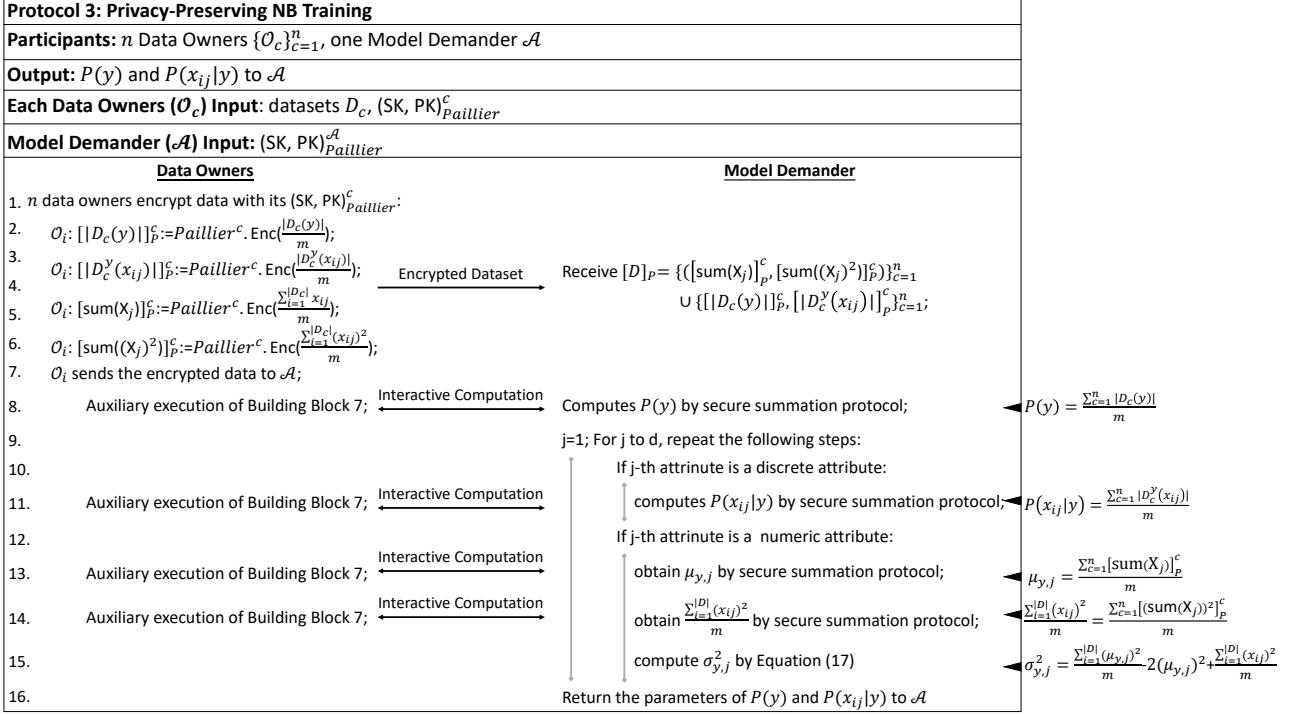


Fig. 4. Privacy-Preserving Logistic Regression Training Protocol

For Protocol 3. As shown in Fig. 4, the main computation focus on the 4 operations of secure summation. Referring to the 10 and 11 steps of Building Block 6, in secure summation e^* is refreshed to 2 once a secure addition’s computation ends. Therefor, 2048-bit key length is enough to control these computations.

VII. PERFORMANCE EVALUATION

In this section, we present the evaluation of Heda from the following aspects: (i) the performance overhead of Heda, (ii) the scalability of Heda.

A. Preparations

Implementations. In our design, each IoT data owner collects all pieces of data from the IoT devices in its own domain and then performs the following operations of Heda. Data owners and the model demander have adequate computing resources generally. Our experiments are run using a desktop computer with the configuration: single Intel i7 (i7-3770 64bit) processor for a total of 4 cores running at 3.40GHz and 8 GB RAM. We implement all the proposed protocols in Java Development Kit 1.8. Since multiple participants are involved in Heda, we mimic real network latency to be 30 ms for the round trip time of a packet.

Datasets. In our experiments, we use four datasets which are listed in Table VI from the UCI Machine Learning Repository.

Key length setting. The key length is not only related to the security guaranteed by cryptosystems but also to the plaintext space. The underlying plaintext operated in the proposed protocols should be limited in a finite plaintext space that is

TABLE VI
DATASETS USED IN OUR EXPERIMENTS

Datasets	Records	Attributes	Storage
BCWD	699	9	172KB
Adult	32561	14	11956KB
CAD	690	15	271KB
Car	1728	6	297KB

defined by the key length. As analyzed in Section VI-D, we use 2048-bit cryptographic keys in Paillier for the four datasets. We use 2048-bit cryptographic keys in Cloud-RSA for BCWD and Car datasets and 4096-bit cryptographic keys for Adult and CAD datasets.

B. Accuracy and Efficiency Evaluation of Heda

Heda consists of a set of building blocks supporting the fundamental operations that underlie many ML training algorithms. In this subsection, we present the performance of each building block first, following with the performance of the three privacy-preserving ML training protocols instantiated from Heda.

1) Performance of Building Blocks: We run 50 times per building blocks and report the averages, with 5-dimensional vectors. Table VII shows the results in terms of the time consumption at data owners \mathcal{O} and the model demander \mathcal{A} , the number of interactions (round trips) and the communication overhead. The total time consumption includes the time spend on encryption and decryption, the computation time consumption and the mimicked network latency. We observe that all

TABLE VII
BUILDING BLOCKS PERFORMANCE

algorithm	Computation \mathcal{O}	\mathcal{A}	Total Time	Inter.	Comm.
Addition	-	1ms	1ms	0	-
Subtraction	35ms	49ms	113ms	1	1.17kB
P-C Mult	-	150ms	150ms	0	-
Dot Product	-	630ms	630ms	0	-
C-C Mult	-	1ms	1ms	0	-
Power Function	23ms	3ms	56ms	1	0.33kB
Exchange 1	152ms	71ms	253ms	1	0.55kB
Exchange 2	1ms	16ms	47ms	1	0.55kB

protocols of Heda are efficient, with a runtime on the order of milliseconds.

2) *Performance of Privacy-preserving ML Training Protocols:* We instantiate Heda to three protocols to illustrate the power of Heda: *Heda-SVM* (Protocol 1), *Heda-LR* (Protocol 2) and *Heda-NB* (Protocol 3). We run these three protocols on datasets *BCWD*. Table VIII providers the overall performance. The accuracy is evaluated by a widely used criterion ($accuracy = \frac{\#correctly\ classified\ records}{\#total\ records}$). The total time consumption includes the time spend on encryption and decryption, the computation time consumption and the mimic network latency.

To observe whether Heda causes an accuracy loss when conducting privacy-preserving ML training, the standard implementations for LR, SVM and NB where models are trained non-privately using scikit-learn² are employed as the control group. By comparing the accuracy, it is clear that although the three protocols deal with the encrypted dataset, they have almost no loss of accuracy. Since the three protocols perform operations on ciphertext, the total time consumption is higher than the non-privacy ML training. But training a model is still in an acceptable time consumption, as shown in Table VIII. We believe Heda to be practical for sensitive applications.

The maximum number of iterations for Heda-LR and Heda-SVM are set to 1000 and 1000 respectively. The number of interactions is determined by the maximum number of iterations in these two protocols. The bandwidth can reach over 10MB/s in most practical application, thus the communication overhead shown in Table VIII is acceptable.

3) *Comparison with Prior Works:* We implement the three latest and effective solutions that considered using PHE to solve privacy-preserving ML training: secure LR training (PLR) [30], secure SVM training (PSVM) [9], and secure NB training (PNB) [51] where the privacy budget was set as 1 according to the authors' setting. The comparison results between the proposed protocols instantiated from Heda and the three solutions are reported in Table IX.

The first thing worth to mention is that PLR, PSVM, and PNB all need to introduce untrusted servers for completing the secure training computation, while there are only two types of roles in Heda, i.e., the data owner and the model demander. Additional roles may cause more communication delay and more privacy compromises because of the complex role scenarios.

PLR [30] handles the sigmoid function by an approximate equation, which causes a loss of accuracy. Heda-LR actually solve the sigmoid function without any approximate equation. Thus the accuracy of Heda-LR is higher than PLR [30]. Since the sigmoid function asks for the power operation, Heda-LR spends more time than PLR does. Actually, in many scenarios, accuracy is a more important standard than time consumption, such as in disease prediction system where experts are willing to obtain a more accurate prediction model at the expense of time consumption.

Heda-SVM and PSVM [9] both rely on PHE, thus there is little difference in accuracy. While Heda-SVM do not need untrusted servers, the overhead of communication and interactions is less than PSVM. Moreover, the secure multiplication protocol in PSVM [9] rely on the heavy interaction between the untrusted servers and data owners, which cause more communication delay. The model demander can complete the secure multiplication independently in our solution, after receiving the encrypted data.

PNB [51] protects the initial data by adding noise (i.e., DP mechanism), which inevitably reduces the accuracy of the trained model. Heda-NB does not harm for the accuracy, which is confirmed in Table IX.

C. Scalability Evaluation of Heda

We evaluate the scalability of Heda in the two aspects: (i) changing the number of participants, and keeping the number of records in training datasets unchanged. (ii) changing the number of records in training datasets, and keeping the number of participants unchanged.

1) *Changing Participant Number:* We divide dataset *Adult* into n equal parts to simulate n data owners participating in the same protocol, and varied the value of n . A series of experiments are carried out respecting to different n values. The number of records in training datasets remains unchanged, i.e., the whole dataset *Adult* was employed in each experiment. Experimental results are plotted in Fig. 5.

SGD is chose as the optimization method in Heda-LR and Heda-SVM. Theoretically, in these two protocols, after data owners send the encrypted datasets to the model demander, the time consumption is only related to the iteration number and the number of the training samples selected at each iteration, which is confirmed in Fig. 5(a) and 5(b). On the other hand, when the data quality is unchanged, the increasing number of data owners does not affect the accuracy of the trained model. A slight fluctuation of accuracy shown in Fig. 5(a) and Fig. 5(b) is ascribed to the random selection of initialization parameters and SGD.

In Heda-NB, after obtaining the noised summation, the model demander interacts with data owners to eliminate the noise in *Secure Summation*. Thus, with the increasing number of data owners, the time consumption increases in Heda-NB. As shown in Fig. 5(c), the increase in time consumption is not violent (more moderate than linear growth).

2) *Changing Record Number:* We vary the record number of training datasets from 5000 to 30000 at the interval of 5000, upon dataset *Adult*. Then, we conduct a series of experiments

²<http://scikit-learn.org>

TABLE VIII
PERFORMANCE OF PRIVACY-PRESERVING ML TRAINING PROTOCOLS INSTANTIATED FROM HEDA

Algorithms	Accuracy	Interactions	Comm.	Total Time	Time per participant	
					\mathcal{O}	\mathcal{A}
Heda-LR	96.52%	4000	514.01MB	2239.70s	1523.34s	626.36s
Heda-SVM	96.13%	3000	532.55MB	605.95s	193.57s	382.38s
Heda-NB	95.99%	30	7.92MB	4.80s	0.74s	3.15s

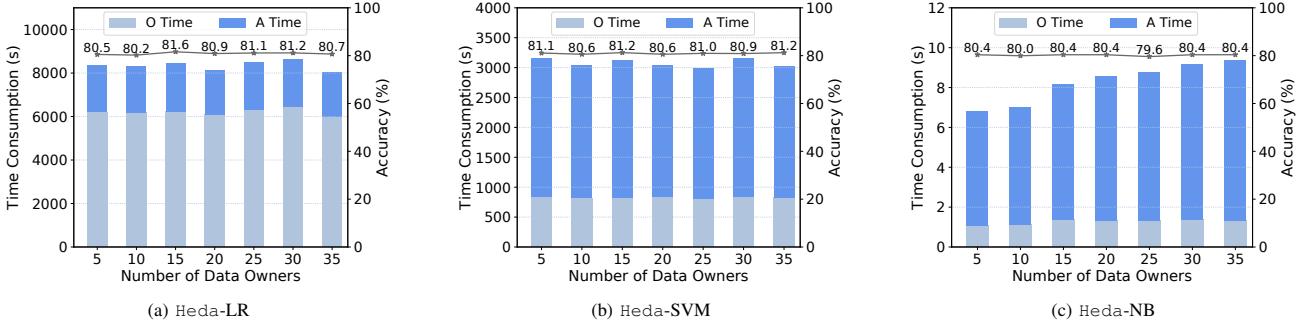


Fig. 5. Scalability evaluation of Heda when the number of participants changes, and the number of records in training datasets remains unchanged. The abscissa shows the changes in the number of \mathcal{O} . The bars represent the time consumption, and the line represents the accuracy.

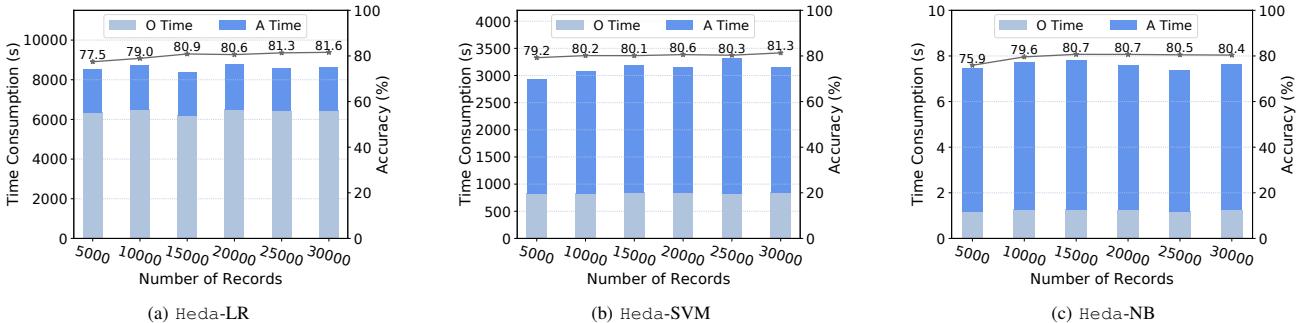


Fig. 6. Scalability evaluation of Heda when the number of records changes, the number of participants remains unchanged. The abscissa shows the changes in the number of records in training dataset, where \mathcal{O} 's number is fixed to 5. The bars and the line represent the time consumption and the accuracy respectively.

TABLE IX
PERFORMANCE COMPARISON WITH OTHER SCHEMES

(a) Logistic Regression

Dataset	Accuracy			Time Consumption	
	Original	Ours	PLR	Ours	PLR
BCWD	96.85%	96.85%	95.99%	2239.70s	1849.81s
Adult	81.44%	81.07%	78.87%	8539.36s	7581.73s
CAD	85.65%	86.23%	83.76%	4382.94s	3644.10s
Car	72.39%	71.99%	70.37%	1793.66s	1287.81

(b) Support Vector Machine

Dataset	Accuracy			Time Consumption	
	Original	Ours	PSVM	Ours	PSVM
BCWD	96.13%	96.85%	95.42%	605.95s	650.03s
Adult	81.62%	81.35%	81.00%	3132.15s	3269.03s
CAD	86.81%	86.23%	85.21%	1079.33s	1153.51s
Car	73.66%	73.03%	72.33%	389.70s	403.00s

(c) Naive Bayes

Dataset	Accuracy			Time Consumption	
	Original	Ours	PNB	Ours	PNB
BCWD	95.85%	95.27%	72.09%	5.01s	6.82s
Adult	80.38%	80.70%	70.02%	7.94s	9.14s
CAD	80.57%	82.17%	70.47%	8.96s	10.45s
Car	78.93%	77.31%	69.68%	2.81s	4.11s

respecting to these training datasets with different record numbers, where the number of data owners is fixed as 5 in these experiments. Experimental results are visualized in Fig. 6.

Experiment results confirm that supervised ML appreciates large and comprehensive training data [3]. As the number of records in training data increases, the accuracy of the trained model in Heda-LR and Heda-SVM increases to a certain extent. In Heda-NB, the time consumption is related to the number of data owners and the number of attributes, and in Heda-LR and Heda-SVM the time consumption is related to the number of iterations and the number of the training samples selected at each iteration, thus the changes in the record number does not affect the time consumption.

VIII. CONCLUSION

In this paper, we propose a novel privacy-preserving ML training framework named Heda for securely handling IoT data collected from diverse IoT devices. By applying Paillier and Cloud-RSA, we develop a library of building blocks based on partial homomorphic encryption to support training multiple ML models in the aggregation scenario of IoT. We demonstrate the efficiency and the security of Heda through

rigorous security analysis and extensive experiments. In the future work, we plan to explore a more outstanding solution enabling the balance between efficiency and accuracy for privacy-preserving ML training.

APPENDIX

A. Problem Description

We devote to the privacy-preserving ML training in aggregation scenario, while many studies exploring the privacy-preserving ML training fall in collaborative scenarios. This section presents the formal description of the aggregation scenario and collaborative scenario, followed with the differences description between the two.

In aggregation scenario, an untrusted model demander wishes to train a ML model over the training dataset gathered from multiple data owners (organizations). Each data owner sends the encrypted dataset encrypted by its own private key to the model demander. During the whole training process, the sensitive model information of the model demander is not revealed to the data owners. And the dataset of each data owner is also confidential for the model demander.

In collaborative scenarios, a set of data owners want to train ML models on their joint data. These data owners outsource the computation to several untrusted servers. During the training process, each data owner cannot learn the sensitive data of other data owners, but the model information is known to both the data owners and the untrusted servers.

More specifically, they differ in

- Different Model Demanders: the demander in aggregation scenario is the untrusted model demander, and in collaborative scenario is each data owner.
- Different Privacy Guarantee: in aggregation scenario, the untrusted model demander cannot learn anything about the data owners' sensitive data, and each data owner learn neither the model nor the sensitive data of other data owners; in collaborative scenario, the untrusted servers learning nothing about the data owners' sensitive data, while the model is known by every participant.
- Different Compute Mode: in aggregation scenario, the untrusted model demander interacts with the data owners for training models; in collaborative scenario, the data owners generally outsource part or all computations to the untrusted servers.

B. Security Definition

Definition 3 (Computational Indistinguishability [37]). *Two probability ensembles $\mathcal{X} = \{X_n\}_{n \in \mathbb{N}}$ and $\mathcal{Y} = \{Y_n\}_{n \in \mathbb{N}}$ are computationally indistinguishable, denoted $\mathcal{X} \equiv_c \mathcal{Y}$, if for every probabilistic polynomial-time distinguisher D there exists a negligible function negl such that:*

$$\Pr_{x \leftarrow X_n} [D(1^n, x) = 1] - \Pr_{y \leftarrow Y_n} [D(1^n, y) = 1] \leq \text{negl}(n)$$

For more details of probabilistic polynomial-time distinguisher and negligible function, we refer the reader to [37].

Modular Sequential Composition. Since all our protocols are designed and constructed in a modular way, we employ

Modular Sequential Composition [39] for justifying the security proofs of our protocols, the idea of which is that:

(i) A and B run a protocol π and use calls to an ideal functionality f . If we can show that π respects privacy in the honest-but-curious model and we have a protocol ρ that privately computes f in the same model, then we can replace the ideal calls for f by the execution of ρ in π ; The new protocol, denoted π^ρ is then secure in the honest-but-curious model.

(ii) A protocol π is a hybrid model that uses calls to f_1, \dots, f_n . The hybrid model with ideal access to f_1, \dots, f_n is augmented with an incorruptible trusted party T. The running of protocol π contains calls to T for the execution of one of f_1, \dots, f_n . Since the proposed protocols in this paper are considered as sequential composition, each party sends its input and wait until the trusted party sends the output back for each call. Let ρ_1, \dots, ρ_n be real protocols in the semi-honest model securely computing f_1, \dots, f_n . In $\pi^{\rho_1, \dots, \rho_n}$, f_i is replaced by a real execution of ρ_i . During the executing processes of $\pi^{\rho_1, \dots, \rho_n}$, if a participates P_i of $\pi^{\rho_1, \dots, \rho_n}$ has to compute f_j in the protocol f_i with input x_i , P_i halts, calling T for starting an execution of ρ_j with the other parties, and continues until T returns the results β_j .

C. Machine Learning Preliminary

On the input of an unencrypted training dataset, ML training algorithms output the ML model parameters θ . After the objective optimization function is given, ML training algorithms updates the model parameters θ through a certain parameter optimization strategy. In this paper, we employ Stochastic Gradient Descent (SGD) as the parameter optimization algorithm in SVM, LR and NB training algorithms.

D. Stochastic Gradient Descent

Gradient descent is an optimization algorithm for finding the local minimum of a function, which updates the parameters by using all the records in train dataset. Given a loss function $\mathcal{J}(\theta)$, the parameters updating equation of gradient descent is $\theta := \theta - \lambda \frac{\partial \mathcal{J}(\theta)}{\partial \theta}$, where λ is the learning rate and θ is the learnable parameters of models.

When the number of the records is large or the gradient calculation is time-consuming, the updating process using all samples is slow. Instead of using all samples, SGD randomly selects a small number of samples to update the gradient at each iteration, which is typically fast in practice [5]. This paper uses SGD as the optimization algorithm for LR and SVM model training.

E. Support Vector Machine

SVM gives the maximum-margin hyperplane that might classify the test data. The form of the hyperplane is expressed as $f(\mathbf{x}) = \theta^\top \hat{\mathbf{x}}$, $\hat{\mathbf{x}} := [\mathbf{x}; 1]$. For binary classification, if $\theta^\top \hat{\mathbf{x}} \geq 1$, the prediction label $y_i = +1$; otherwise the prediction label $y_i = -1$. The optimization problem of the primary of SVM as Equation (8). SVM can perform the non-linear classification by replacing the \mathbf{x} in $f(\mathbf{x}) = \theta^\top \hat{\mathbf{x}}$ with a kernel

trick $\kappa(\hat{\mathbf{x}})$. In this paper, we consider the plain type of SVM, i.e., $\kappa(\hat{\mathbf{x}}) := \hat{\mathbf{x}}$.

$$\begin{aligned} & \min_{\theta} \frac{1}{2} \|\theta\|^2 \\ & \text{s.t. } y_i (\theta^T \hat{\mathbf{x}}_i) \geq 1, \quad i = 1, 2, \dots, |D| \end{aligned} \quad (8)$$

Employing Hinge Loss, we define a differentiable loss function which is shown in Equation (9).

$$\min_{\theta} \sum_{i=1}^{|D|} \max(0, 1 - y_i \theta^T \hat{\mathbf{x}}_i) + \lambda \|\theta\|^2 \quad (9)$$

We use SGD for solving the parameter θ in Equation (9). For a records $\hat{\mathbf{x}}_i$ selected from the training dataset D , the iteration formula of SVM training algorithm is shown in Equation (10), where α is the regularization coefficient.

$$\theta := \begin{cases} \theta - \lambda(\alpha\theta - \alpha y_i \hat{\mathbf{x}}_i), & y_i \theta^T \hat{\mathbf{x}}_i < 1 \\ \theta - \lambda(\alpha\theta), & y_i \theta^T \hat{\mathbf{x}}_i \geq 1 \end{cases} \quad (10)$$

F. Logistic Regression

LR is a binary classifier that tries to learn parameters θ , where $\theta = [\theta_1, \theta_2, \dots, \theta_d]$ to satisfy $f\{\mathbf{x}_i\} = \theta^T \mathbf{x}_i$ and $f\{\mathbf{x}_i\} \cong y_i$. y_i is the probability that \mathbf{x}_i belongs to the positive class. LR uses the Sigmoid function to associate the true label y_i with the prediction label $f\{\mathbf{x}_i\}$: $h_\theta(\mathbf{x}_i) = \frac{e^{\theta^T \mathbf{x}_i}}{1 + e^{\theta^T \mathbf{x}_i}}$. Choosing Cross Entropy as the cost function $J(\theta)$.

$$J(\theta) = -\frac{1}{m} \left[\sum_{i=1}^m (y_i \log h_\theta(\mathbf{x}_i) + (1 - y_i) \log(1 - h_\theta(\mathbf{x}_i))) \right] \quad (11)$$

We update the parameters θ with SGD, solving the parameter values that can minimize $J(\theta)$. The iteration formula of LR training algorithm is shown in Equation (12).

$$\theta_j := \theta_j - \lambda x_{ij} (y_i - \frac{1}{1 + e^{-\theta^T \mathbf{x}_i}}) \quad (12)$$

G. Naive Bayes

The training process of NB is to compute the class prior probability $P(y)$ and the conditional probability $P(\mathbf{x}_i|y)$, where y denotes a certain class category in \mathcal{D} . The NB classifier is expressed as: $f(\mathbf{x}_i) = \operatorname{argmax}_y P(y) \prod_{j=1}^d P(\mathbf{x}_{ij}|y)$.

The class prior probability $P(y)$ can be obtained through the maximum likelihood estimation, i.e., $P(y) = \frac{|\mathcal{D}(y)|}{m}$, where $|\mathcal{D}(y)|$ is the number of the class y in \mathcal{D} .

For discrete attributes, the conditional probability for the discrete attributes is $P(x_{ij}|y) = \frac{|\mathcal{D}^y(x_{ij})|}{m}$ where $|\mathcal{D}^y(x_{ij})|$ is the number of the number of the j-th attribute having the value x_{ij} with the class y in \mathcal{D} .

As for the numeric attributes, probability density function is considered for computing the conditional probability $P(\mathbf{x}_i|y)$. Assuming that $P(x_{ij}|y)$ obeys normal distribution $N(\mu_{y,j}, \sigma_{y,j}^2)$, where $\mu_{y,j}$ and $\sigma_{y,j}^2$ are mean and variance respectively for the j-th attributes of the class y respectively. Then, the conditional probability $P(x_{ij}|y)$ can be obtained from Equation (13).

$$P(x_{ij}|y) = \frac{1}{\sqrt{2\pi}\sigma_{y,j}} \exp\left(-\frac{(x_{ij} - \mu_{y,j})^2}{2\sigma_{y,j}^2}\right) \quad (13)$$

H. Security Analysis for Building Blocks of Primitive Operations

When facing the honest-but-curious adversaries, we follow secure two-party computation for guaranteeing the security of the proposed building blocks. Here, we present our security proofs according to the ideas of secure two-party computation. That is, all the message that can be computed out by a participant from the intermediate result must be included in the message that can be computed from its input and output.

Proposition A.1. *Secure addition, secure subtraction, secure plaintext-ciphertext multiplication, and secure ciphertext-ciphertext multiplication is secure in the honest-but-curious model.*

Proof A.1 (for Proposition A.1). *The input of the data owner is $((\text{SK}, \text{PK})_{\text{Paillier}}, a)$. As the data owner does not receive any message and call to any other protocols or algorithms during the execution processes, his view only consists in its input. Hence, the simulator $S_{\mathcal{O}}$ simply generate random coins:*

$$S_{\mathcal{O}}(a) = (a, \text{coins}) = \text{view}_{\mathcal{O}}(a, b)$$

The input of the model demander is (b) . $\text{view}_{\mathcal{A}}(a, b) = \{b, [b], [a]; \text{Output}_{\mathcal{A}}\}$. $\text{Output}_{\mathcal{A}} = [f(a, b)]$. The simulator $S_{\mathcal{A}}$ does the following:

- Generates the random coins necessary for re-randomization and put them in coins .
- Generates an encryption using the public key of the data owner: $[c]$.
- Outputs $\{[b], [c], \text{coins}; [f(c, b)]\}$.

coins and coins come from the same distribution, independently from other parameters. Thus,

$$\{[b], [c], \text{coins}; [f(c, b)]\} = \{[b], [c], \text{coins}; [f(a, b)]\}$$

and by ciphertext indistinguishability against chosen plaintext attacks of Paillier,

$$\{[b], [c], \text{coins}; [f(c, b)]\} \equiv_c \{[b], [a], \text{coins}; [f(a, b)]\}$$

$[a]$ and $[f(a, b)]$ is encrypted by the public key of the data owner, the confidentiality of which are equivalent to the cryptosystem. By semantic security of Paillier, $S_{\mathcal{A}}(b, F(a, b)) \equiv_c \text{view}_{\mathcal{A}}(a, b)$. \square

Proposition A.2. *Secure power function is secure in the honest-but-curious model.*

Proof A.2 (for Proposition A.2). *The input of data owner is $((\text{SK}, \text{PK})_{\text{CloudRSA}}, e^a)$. As the data owner does not receive any message and call to any other protocols during the execution processes, his view only consists in its input. Hence, the simulator $S_{\mathcal{O}}$ simply generate random coins:*

$$S_{\mathcal{O}}(e^a) = (e^a, \text{coins}) = \text{view}_{\mathcal{O}}(e^a, \mathbf{b})$$

The input of model demander is (b) . $\text{view}_{\mathcal{A}}(a, b) = \{\mathbf{b}, [e^a]_R, \{\prod_{i=1}^j [e^{a_i b_i}]_R\}_{j=1}^d; \text{Output}_{\mathcal{A}}\}$. $\text{Output}_{\mathcal{A}} = [e^{a \cdot b}]_R$. The simulator $S_{\mathcal{A}}$ does the following:

- Picks $2d$ random numbers that are limited to \mathbb{Z}_N : $(\hat{a}_1, \dots, \hat{a}_d, c_1, \dots, c_d)$.

- Encrypts $(\hat{a}_1, \dots, \hat{a}_d)$ by $\text{PK}_{\text{CloudRSA}}$: $[e^{\hat{\mathbf{a}}}]_R := \{[\hat{a}_1]_R, \dots, [\hat{a}_d]_R\}$.
- Encrypts (c_1, \dots, c_d) by $\text{PK}_{\text{CloudRSA}}$.
- Generates the random coins necessary for re-randomization and put them in coins .
- Outputs $\{\mathbf{b}, [e^{\hat{\mathbf{a}}}]_R, \text{coins}, \{[c_i]_R\}_{i=1}^d; [e^{\hat{\mathbf{a}} \cdot \mathbf{b}}]_R\}$.

coins and $\hat{\text{coins}}$ come from the same distribution, independently from other parameters. Thus,

$$\begin{aligned} & \{\mathbf{b}, [e^{\hat{\mathbf{a}}}]_R, \text{coins}, \{[c_i]_R\}_{i=1}^d; [e^{\hat{\mathbf{a}} \cdot \mathbf{b}}]_R\} \\ &= \{\mathbf{b}, [e^{\hat{\mathbf{a}}}]_R, \text{coins}, \{[c_i]_R\}_{i=1}^d; [e^{\hat{\mathbf{a}} \cdot \mathbf{b}}]_R\} \end{aligned}$$

and by ciphertext indistinguishability against chosen plaintext attacks of Cloud-RSA,

$$\begin{aligned} & \{\mathbf{b}, [e^{\hat{\mathbf{a}}}]_R, \text{coins}, \{[c_i]_R\}_{i=1}^d; [e^{\hat{\mathbf{a}} \cdot \mathbf{b}}]_R\} \\ &\equiv_c \{\mathbf{b}, [e^{\mathbf{a}}]_R, \text{coins}, \{\prod_{i=1}^j [e^{a_i b_i}]_R\}_{j=1}^d; [e^{\mathbf{a} \cdot \mathbf{b}}]_R\} \\ &= \{\mathbf{b}, [e^{\mathbf{a}}]_R, \text{coins}, \{\prod_{i=1}^j [e^{a_i b_i}]_R\}_{j=1}^d; \text{Output}_{\mathcal{A}}\} \end{aligned}$$

$[e^{\mathbf{a}}]_R, \prod_{i=1}^d [e^{a_i b_i}]_R$ and $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ is encrypted by $\text{PK}_{\text{CloudRSA}}$, the confidentiality of which are equivalent to the cryptosystem. By semantic security of CloudRSA, $S_{\mathcal{A}} \equiv_c \text{view}_{\mathcal{A}}$

□

Proposition A.3. Secure summation is secure in the honest-but-curious model.

Proof A.3 (for Proposition A.3). We prove the security of the secure summation without collusion first.

For the first $n-1$ data owners:

The input of \mathcal{O}_i is $((\text{SK}, \text{PK})_{\text{Paillier}}^i; a_i, r_i, a_i + r_i, [r_i]_P^i)$. Each \mathcal{O}_i 's view is

$$\text{view}_{\mathcal{O}_i} = \{a_i, r_i, a_i + r_i, [r_i]_P^i; \text{out}_{\text{block9}}\}$$

where $\text{out}_{\text{block9}}$ means the received output from Building Blocks 8 in secure summation.

$$\text{out}_{\text{block9}} = (\sum_{c=1}^i a_c + \sum_{c=i}^n (a_c + r_c))$$

We construct a simulator $S_{\mathcal{O}}$ which runs as follows:

- Picks a random $c \in \mathbb{Z}_N$.
- Outputs $\{a_i, r_i, a_i + r_i, [r_i]_P^i; c\}$.

The distribution of c and $\sum_{c=1}^i a_c + \sum_{c=i}^n (a_c + r_c)$ are identical, so the real distribution $\{a_i, r_i, a_i + r_i, [r_i]_P^i; \text{out}_{\text{block9}}\}$ and the ideal distribution $\{a_i, r_i, a_i + r_i, [r_i]_P^i; c\}$ are statistically indistinguishable, i.e., $S_{\mathcal{O}} \equiv_c \text{view}_{\mathcal{O}_i}$.

For the last data owner \mathcal{O}_n :

The input of \mathcal{O}_n is $((\text{SK}, \text{PK})_{\text{Paillier}}^n; a_n, r_n, a_n + r_n, [r_n]_P^n)$. \mathcal{O}_n 's view is

$$\text{view}_{\mathcal{O}_n} = \{a_n, r_n, a_n + r_n, [r_n]_P^n; \text{out}_{\text{block9}}\}$$

$$\text{out}_{\text{block9}} = (\sum_{i=1}^n a_i + r_{\mathcal{A}})$$

We construct a simulator $S_{\mathcal{O}_n}$ which runs as follows:

- Picks a random $c \in \mathbb{Z}_N$;

- Outputs $\{a_n, r_n, a_n + r_n, [r_n]_P^n; c\}$.

The distribution of c and $\sum_{i=1}^n a_i + r_{\mathcal{A}}$ are identical, so the real distribution $\{a_n, r_n, a_n + r_n, [r_n]_P^n; \text{out}_{\text{block9}}\}$ and the ideal distribution $\{a_n, r_n, a_n + r_n, [r_n]_P^n; c\}$ are statistically indistinguishable, i.e., $S_{\mathcal{O}_n} \equiv_c \text{view}_{\mathcal{O}_n}$.

For the model demander \mathcal{A} :

The input of model demander \mathcal{A} is $(\text{SK}, \text{PK})_{\text{Paillier}}^{\mathcal{A}}$. The view of model demander is

$$\begin{aligned} \text{view}_{\mathcal{A}} &= \{r_{\mathcal{A}}, \{(a_i + r_i)\}_{i=0}^n, \{[r_i]_P^i\}_{i=0}^n, \\ &\quad \{[\sum_{i=0}^n a_i + \sum_{i=c}^n r_i]_P^c\}_{c=0}^n; \text{out}_{\text{block9}}\} \end{aligned}$$

where $\text{out}_{\text{block9}}$ means the received output from Building Blocks 8 in secure summation.

$$\text{out}_{\text{block9}} := \begin{cases} \{[\sum_{c=1}^i a_c + \sum_{c=i}^n (a_c + r_c)]_P^i, & 1 \leq i < n \\ \sum_{i=1}^n a_i, & i = n \end{cases}$$

We construct a simulator $S_{\mathcal{A}}$ which runs as follows:

- Picks $2n$ random numbers that are limited to \mathbb{Z}_N : $(\hat{a}_1, \dots, \hat{a}_n, \hat{r}_1, \dots, \hat{r}_n)$.
- Generates $\{(\hat{a}_i + \hat{r}_i)\}_{i=0}^n$.
- Generates the random coins necessary for re-randomization and put them in coins .
- Encrypts $\{\hat{r}_i\}_{i=1}^n$ by corresponding $\text{PK}_{\text{Paillier}}^i$.
- Encrypts $\{\sum_{i=0}^n \hat{a}_i + \sum_{c=1}^n \hat{r}_i\}_{c=1}^n$ by corresponding $\text{PK}_{\text{Paillier}}^i$.
- Generates $\sum_{i=0}^n \hat{a}_i$.
- Outputs:

$$\begin{aligned} & \{\text{coins}, \{(\hat{a}_i + \hat{r}_i)\}_{i=0}^n, \{[\hat{r}_i]_P^i\}_{i=0}^n, \{[\sum_{i=0}^n \hat{a}_i + \sum_{i=c}^n \hat{r}_i]_P^c\}_{c=0}^n \\ & \quad ; \{[\sum_{c=1}^i \hat{a}_c + \sum_{c=i}^n (\hat{a}_c + \hat{r}_c)]_P^i\}_{i=0}^{n-1}, \sum_{i=0}^n \hat{a}_i\} \end{aligned}$$

coins and $\hat{\text{coins}}$ come from the same distribution, independently from other parameters, and the distribution of $(\hat{a}_1, \dots, \hat{a}_n, \hat{r}_1, \dots, \hat{r}_n)$ and $(a_1, \dots, a_n, r_1, \dots, r_n)$ are identical, so the real distribution $(a_1, \dots, a_n, r_1, \dots, r_n)$ and the ideal distribution $(\hat{a}_1, \dots, \hat{a}_n, \hat{r}_1, \dots, \hat{r}_n)$ are statistically indistinguishable.

$$\begin{aligned} & \{\text{coins}, \{(\hat{a}_i + \hat{r}_i)\}_{i=0}^n, \{[\hat{r}_i]_P^i\}_{i=0}^n, \{[\sum_{i=0}^n \hat{a}_i + \sum_{i=c}^n \hat{r}_i]_P^c\}_{c=0}^n \\ & \quad ; \{[\sum_{c=1}^i \hat{a}_c + \sum_{c=i}^n (\hat{a}_c + \hat{r}_c)]_P^i\}_{i=0}^{n-1}, \sum_{i=0}^n \hat{a}_i\} \\ & \equiv_c \{\text{coins}, \{(a_i + r_i)\}_{i=0}^n, \{[\hat{r}_i]_P^i\}_{i=0}^n, \{[\sum_{i=0}^n a_i + \sum_{i=c}^n r_i]_P^c\}_{c=0}^n \\ & \quad ; \{[\sum_{c=1}^i a_c + \sum_{c=i}^n (a_c + r_c)]_P^i\}_{i=0}^{n-1}, \sum_{i=0}^n a_i\} \end{aligned}$$

by ciphertext indistinguishability against chosen plaintext attacks of Paillier

$$\begin{aligned} & \{\text{coins}, \{(a_i + r_i)\}_{i=0}^n, \{[\hat{r}_i]_P^i\}_{i=0}^n, \{[\sum_{i=0}^n \hat{a}_i + \sum_{i=c}^n \hat{r}_i]_P^c\}_{c=0}^n \\ & ; \{[\sum_{c=1}^i \hat{a}_c + \sum_{c=i}^n (\hat{a}_c + \hat{r}_c)]_P^i\}_{i=0}^{n-1}, \sum_{i=0}^n a_i\} \\ & \equiv_c \{\text{coins}, \{(a_i + r_i)\}_{i=0}^n, \{[r_i]_P^i\}_{i=0}^n, \{[\sum_{i=0}^n a_i + \sum_{i=c}^n r_i]_P^c\}_{c=0}^n \\ & ; \{[\sum_{c=1}^i a_c + \sum_{c=i}^n (a_c + r_c)]_P^i\}_{i=0}^{n-1}, \sum_{i=0}^n a_i\} \end{aligned}$$

i.e., $S_A \equiv_c \text{view}_A$.

Collusion situations.

■ We discuss the security when α ($\alpha \leq n-1$) data owners collude with each other to infer the summation $\sum_{i=0}^n a_i$ and other data owners' data. Considering the most extreme case, $\alpha = n-1$. The $n-1$ data owners have information:

$$\{\{a_i, r_i, a_i + r_i, [r_i]_P^i\}_{i=1}^{n-1}, \sum_{c=1}^{n-1} a_c + (a_n + r_n), a_n + r_n\}$$

It is straightforward that the random noise r_n in $\sum_{c=1}^{n-1} a_c + (a_n + r_n)$ hides $\sum_{i=0}^n a_i$ in an information-theoretic way (it is an one-time pad). Similarly, a_n cannot be figured out too.

■ We discuss the security when α ($\alpha \leq n-2$) data owners collude with model demander to infer other data owners' data. Considering the most extreme case, $\alpha = n-2$, where \mathcal{O}_{n-1} and \mathcal{O}_n do not participate in collusion.

The $n-2$ data owners have information:

$$\{\{a_i, r_i, a_i + r_i, [r_i]_P^i\}_{i=1}^{n-2}, \sum_{c=1}^{n-2} a_c + \sum_{c=n-2}^n (a_c + r_c)\} \quad (14)$$

The model demander have information:

$$\begin{aligned} & \{\{(a_i + r_i)\}_{i=0}^n, \{[r_i]_P^i\}_{i=0}^n, \{[\sum_{i=0}^n a_i + \sum_{i=c}^n r_i]_P^c\}_{c=0}^n, \\ & ; [\sum_{c=1}^i a_c + \sum_{c=i}^n (a_c + r_c)]_P^i\}_{i=0}^n \} \quad (15) \end{aligned}$$

Combining Equation (14) and Equation (15), we obtain:

$$\{(a_n + a_{n-1}), (a_{n-1} + r_{n-1}), (a_n + r_n), [r_{n-1}]_P^{n-1}, [r_n]_P^n\}$$

Ciphertext indistinguishability against chosen plaintext attacks of Paillier ensures that no bit of information is leaked from $[r_{n-1}]_P^{n-1}, [r_n]_P^n$. The random noise r_n and r_{n-1} hides a_n and a_{n-1} respectively in an information-theoretic way (it is an one-time pad).

The model demander and data owners may try to infer a_n and a_{n-1} from $a_n + a_{n-1}$. In this case, we see $a_n + a_{n-1}$ as a ciphertext, where the model demander and data owners infer information by observing $a_n + a_{n-1}$.

That is, the model demander and data owners just observes a ciphertext $a_n + a_{n-1}$ and attempts to determine information about the underlying plaintext (or plaintexts), which is a ciphertext-only attack. Observing $a_n + a_{n-1}$ has no effect on the knowledge regarding the actual message that was sent. \square

I. Security Analysis for Building Blocks of Conversion

Proposition A.4. Secure converting $[e^{\mathbf{a} \cdot \mathbf{b}}]_R$ to $[e^{\mathbf{a} \cdot \mathbf{b}}]_P$ is secure in the honest-but-curious model.

Proof A.4 (for Proposition A.4). The input of data owner is $\{(\text{SK}, \text{PK})_{\text{Paillier}}, (\text{SK}, \text{PK})_{\text{CloudRSA}}\}$. \mathcal{O} 's view is

$$\text{view}_\mathcal{O} = (e^{\mathbf{a} \cdot \mathbf{b} + r}, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_P)$$

We construct a simulator $S_\mathcal{O}$ which runs as follows:

- Picks two random vectors $(\hat{\mathbf{a}}, \hat{\mathbf{b}})$.
- Picks a random c , computes $e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}$.
- Generates the random coins necessary for re-randomization and put them in coins .
- Encrypts $e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}$ under $\text{PK}_{\text{Paillier}}$ and $\text{PK}_{\text{CloudRSA}}$ respectively.
- Outputs $(e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_P, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_R, \text{coins})$.

coins and $\hat{\text{coins}}$ come from the same distribution, independently from other parameters,

$$\begin{aligned} & (e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_P, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_R, \hat{\text{coins}}) \\ & = (e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_P, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_R, \text{coins}) \end{aligned}$$

The distribution of $(\mathbf{a} \cdot \mathbf{b} + r)$ and $(\hat{\mathbf{a}} \cdot \hat{\mathbf{b}} + c)$ are identical, so the real distribution $(e^{\mathbf{a} \cdot \mathbf{b} + r}, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_P)$ and the ideal distribution $(e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_P, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_R)$ are statistically indistinguishable,

$$\begin{aligned} & (e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_P, [e^{c+\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}}]_R) \\ & \equiv_c (e^{\mathbf{a} \cdot \mathbf{b} + r}, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_P) \end{aligned}$$

Thus, $S_\mathcal{O} \equiv_c \text{view}_\mathcal{O}$.

The input of model demander is $\{e^{\mathbf{a} \cdot \mathbf{b}}\}$.

$$\text{view}_A = (r, [e^{\mathbf{a} \cdot \mathbf{b}}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_P, [e^{\mathbf{a} \cdot \mathbf{b}}]_P)$$

We construct a simulator S_A which runs as follows:

- Picks 2 random numbers that are limited to \mathbb{Z}_N : c_1, c_2 .
- Generates $e^{c_2}, e^{c_1+c_2}$.
- Generates the random coins necessary for re-randomization and put them in coins .
- Encrypts $e^{c_1+c_2}$ by $\text{PK}_{\text{Paillier}}$.
- Encrypts e^{c_2} by $\text{PK}_{\text{Paillier}}$.
- Encrypts $e^{c_1+c_2}$ by $\text{PK}_{\text{CloudRSA}}$.
- Encrypts e^{c_2} by $\text{PK}_{\text{CloudRSA}}$.
- Outputs $(\text{coins}, c_1, [e^{c_2}]_R, [e^{c_1+c_2}]_R, [e^{c_1+c_2}]_P, [e^{c_2}]_P)$.

coins and $\hat{\text{coins}}$ come from the same distribution, independently from other parameters, and by ciphertext indistinguishability against chosen plaintext attacks of Paillier and Cloud-RSA,

$$\begin{aligned} & (c_1, [e^{c_2}]_R, [e^{c_1+c_2}]_R, [e^{c_1+c_2}]_P, [e^{c_2}]_P) \\ & \equiv_c (r, [e^{\mathbf{a} \cdot \mathbf{b}}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_P, [e^{\mathbf{a} \cdot \mathbf{b}}]_P) \end{aligned}$$

$[e^{\mathbf{a} \cdot \mathbf{b}}]_R, [e^{\mathbf{a} \cdot \mathbf{b} + r}]_R, [e^{\mathbf{a} \cdot \mathbf{b}}]_P$ and $[e^{\mathbf{a} \cdot \mathbf{b} + r}]_P$ are encrypted by data owners' public key, the confidentiality of which is equivalent to the cryptosystem. Thereby $S_A \equiv_c \text{view}_A$. \square

Proposition A.5. Secure converting $[m]_P^1$ to $[m]_P^2$ is secure in the honest-but-curious model.

Proof A.5 (for Proposition A.5). *The input of data owner is $\{(\text{SK}, \text{PK})_{\text{Paillier}}^1, (\text{PK})_{\text{Paillier}}^2\}$. \mathcal{O} 's view is*

$$\text{view}_{\mathcal{O}_n} = (m + r, [m + r]_P^1, [m + r]_P^2)$$

We construct a simulator $S_{\mathcal{O}}$ which runs as follows:

- Picks a random $c, c \in \mathbb{Z}_N$.
- Encrypts c under $\text{PK}_{\text{Paillier}}^1$ and $\text{PK}_{\text{Paillier}}^2$ respectively.
- Outputs $(c, [c]_P^1, [c]_P^2)$.

The distribution of c and $m + r$ are identical, so the real distribution $(m + r, [m + r]_P^1, [m + r]_P^2)$ and the ideal distribution $(c, [c]_P^1, [c]_P^2)$ are statistically indistinguishable,

$$(m + r, [m + r]_P^1, [m + r]_P^2) \equiv_c (c, [c]_P^1, [c]_P^2)$$

Thus, $S_{\mathcal{O}} \equiv_c \text{view}_{\mathcal{O}}$.

The input of model demander is $\{[m]_P^1\}$.

$$\text{view}_{\mathcal{A}} = \{r, [m]_P^1, [m]_P^2, [m + r]_P^1, [m + r]_P^2\}$$

$[m]_P^1, [m + r]_P^1, [m]_P^2, [m + r]_P^2$ are encrypted by data owners' public key, the confidentiality of which is equivalent to the cryptosystem. Thereby $S_{\mathcal{A}} \equiv_c \text{view}_{\mathcal{A}}$. \square

J. Security Analysis for ML Training Protocols

Definition 4 (Ciphertext-only Attack [37]). *This is the most basic attack, and refers to a scenario where the adversary just observes a ciphertext (or multiple ciphertexts) and attempts to determine information about the underlying plaintext (or plaintexts).*

Definition 5 (Perfectly Secret [37]). *An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ with message space M is perfectly secret if for every probability distribution over M , every message $m \in M$, and every ciphertext $c \in C$ for which $\Pr[C = c] > 0$:*

$$\Pr[M = m | C = c] = \Pr[M = m]$$

Recalling that our security goal is achieving keeping privacy of each participant and computing model parameters securely when facing honest-but-curious adversaries. Both the model of model demander \mathcal{A} and the sensitive datasets from n data owners \mathcal{O}_i are confidential throughout the execution of secure ML training protocols. This section gives the security analyses for the three privacy-preserving ML training protocols instantiated from Heda .

We follow the ides of Modular Sequential Composition to present the security proofs. If we can show that a protocol π respects privacy in the honest-but-curious model using calls to a series of ideal functionalities, and these ideal functionalities can be replaced by real secure protocols in the semi-honest model, π is secure in the honest-but-curious model. Then we discuss the security in situations of collusion.

Proposition A.6. *Privacy-preserving SVM training protocol is secure in the honest-but-curious model.*

Proof A.6 (for Proposition A.6). *We prove the security without collusion first. Because the model demander and n data owner perform interactive computations in turn, we analyze the security according to definition of Secure Two-party Computation.*

For each data owner \mathcal{O}_i ,

After sending the encrypted dataset to model demander, the data owner does not receive any message and call to any other protocols during the execution processes, his view only consists in its input. The input of the data owner is $((\text{SK}, \text{PK})_{\text{Paillier}}^i, \mathcal{D}_i)$. We use the trivial simulator that just outputs its inputs for the proof of security. Hence, $S_{\mathcal{O}_i} = (\mathcal{D}_i, \text{coins}) = \text{view}_{\mathcal{O}_i}$.

For model demander \mathcal{A} .

The input of the model demander is the initialized model parameters (θ) . The model demander's view is

$$\begin{aligned} \text{view}_{\mathcal{A}} = \{&\theta, [\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i, [\theta \mathbf{x}_t \mathbf{y}_t]_P^i, [\lambda \alpha \mathbf{x}_t \mathbf{y}_t]_P^i; \\ &\text{out}_{\text{block}9}\} \end{aligned}$$

where $\text{out}_{\text{block}9}$ denote the received outputs from Building Blocks 7 respectively.

We construct a simulator $S_{\mathcal{A}}$ which runs as follows:

- Uniformly picks a value v from $\{1, 0\}$.
- Picks a random $\hat{\theta}$.
- Picks 4 random numbers $c_1, c_2, c_3, c_4, c_i \in \mathbb{Z}_N$.
- Encrypts c_1, c_2, c_3, c_4 by $\text{PK}_{\text{Paillier}}^i$.
- Outputs $\{\theta, [c_1]_P^i, [c_2]_P^i, [c_3]_P^i, [c_4]_P^i; \hat{\theta}, v\}$.

by ciphertext indistinguishability against chosen plaintext attacks of Paillier:

$$\begin{aligned} \{[c_1]_P^i, [c_2]_P^i, [c_3]_P^i, [c_4]_P^i\} \equiv_c \\ \{[\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i, [\theta \mathbf{x}_t \mathbf{y}_t]_P^i, [\lambda \alpha \mathbf{x}_t \mathbf{y}_t]_P^i\} \end{aligned}$$

The distribution of $\{v, \hat{\theta}\}$ and $\{(1 >? [\theta \mathbf{x}_t \mathbf{y}_t]_P^i), \text{update}(\theta)\}$ are come from the same distribution, independently from other parameters:

$$\{v, \hat{\theta}\} \equiv_c \{(1 >? [\theta \mathbf{x}_t \mathbf{y}_t]_P^i), \text{update}(\theta)\}$$

The model demander may try to infer data owners' data from θ or $\text{update}(\theta)$. In this case, we see $(\theta, \text{update}(\theta))$ as a ciphertext, where model demander infers information by observing $(\theta, \text{update}(\theta))$.

That is the model demander just observes a ciphertext $(\theta$ and $\text{update}(\theta))$ and attempts to determine information about the underlying plaintext (or plaintexts) in training dataset D , which is a ciphertext-only attack. Besides, observing θ and $\text{update}(\theta)$ have no effect on the the model demander's knowledge regarding the actual message that was sent. For every probability data in training dataset $x_i \in D$, and every ciphertext θ and $\text{update}(\theta)$:

$$\Pr[M = x_i | C = \theta \text{ or } \text{update}(\theta)] = \Pr[M = x_i]$$

Thus, inferring data owners' data from θ or $\text{update}(\theta)$ is a ciphertext-only attack with perfectly secret. Thereby $S_{\mathcal{A}} \equiv_c \text{view}_{\mathcal{A}}$.

In particular, secure addition, secure plaintext-ciphertext dot product and Building Block 8 are secure in the honest-but-curious model. We obtain the security of privacy-preserving SVM training protocol using Modular Sequential Composition.

Collusion situations.

■ We discuss the security when α ($\alpha \leq n - 1$) data owners collude with each other to infer the model parameters θ and other data owners' data. Considering the most extreme case, $\alpha = n - 1$. The $n - 1$ data owners have information:

$$\{([\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i)_{i=1}^{n-1}\}$$

Since the $n - 1$ data owners didn't receive the complete θ , and θ is encrypted by the model demander's public key. It is straightforward that θ cannot be figured out.

Without the corresponding private key of the data owner who do not participating in the collusion, the ciphertext indistinguishability of Paillier ensures that no bit of information is leaked from ciphertexts of other data owners who do not participating in the collusion.

■ We discuss the security when α ($\alpha \leq n - 2$) data owners collude with the model demander to infer other data owners' data. Considering the most extreme cases, $\alpha = n - 2$.

The $n - 2$ data owners have information:

$$\{([\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i)_{i=1}^{n-2}\} \quad (16)$$

The model demander have information:

$$\{\theta, ([\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i, [\theta \mathbf{x}_t y_t]_P^i, [\lambda \alpha \mathbf{x}_t y_t]_P^i)_{i=0}^n\} \quad (17)$$

Combining Equation (16) and Equation (17), we deduce that:

$$\begin{aligned} & \{\theta, (\mathbf{Y}, \mathbf{XY}, \theta \mathbf{x}_t y_t, \lambda \alpha \mathbf{x}_t y_t)_{i=0}^{n-2}\} \text{ with} \\ & ([\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i, [\theta \mathbf{x}_t y_t]_P^i, [\lambda \alpha \mathbf{x}_t y_t]_P^i)_{i=n-1}^n \end{aligned}$$

Without the corresponding private key, they cannot figure out $([\mathbf{Y}]_P^i, [\mathbf{XY}]_P^i)_{i=n-1}^n$. \square

Proposition A.7. Privacy-preserving LR training protocol is secure in the honest-but-curious model.

Proof A.7 (for Proposition A.7). We prove the security without collusion first. Because model demander and each data owner perform interactive computations in turn, we analyze the security according to definition of Secure Two-party Computation.

For each data owner \mathcal{O}_i .

The input of the data owner is $((\mathbf{SK}, \mathbf{PK})_{\text{Paillier}}^i, (\mathbf{SK}, \mathbf{PK})_{\text{CloudRSA}}^i, \mathcal{D}_i)$. The data owner does not call to any other protocols or algorithms during the execution processes.

$$\text{view}_{\mathcal{O}_i} = (\mathcal{D}_i, [e^{\theta \mathbf{x}_t + r} + e^r]_P, \frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}, [\frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}]_P) \quad (18)$$

We construct a simulator $S_{\mathcal{O}_i}$ which runs as follows:

- Uniformly picks a value c .
- Picks a random $\hat{\theta}$.
- Picks a record $\hat{\mathbf{x}}_t$ from \mathcal{D}_i .
- Generates $\frac{\mathbf{x}_t}{e^{\theta \hat{\mathbf{x}}_t + c} + e^c}$ and $e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c$.
- Encrypts $\frac{\mathbf{x}_t}{e^{\theta \hat{\mathbf{x}}_t + c} + e^c}$ and $e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c$ by $\mathbf{PK}_{\text{Paillier}}^i$.
- Outputs $([\frac{\mathbf{x}_t}{e^{\theta \hat{\mathbf{x}}_t + c} + e^c}]_P, [e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c]_P, e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c)$.

The real distribution $(r, \theta, \mathbf{x}_t)$ and the ideal distribution $(c, \hat{\theta}, \hat{\mathbf{x}}_t)$ are come from the same distribution, independently from other parameters,

$$\begin{aligned} & ([e^{\theta \mathbf{x}_t + r} + e^r]_P, \frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}, [\frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}]_P) \\ & \equiv_c ([\frac{\mathbf{x}_t}{e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c}]_P, [e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c]_P, e^{\hat{\theta} \hat{\mathbf{x}}_t + c} + e^c) \end{aligned}$$

Hence, $S_{\mathcal{O}_i} \equiv_c \text{view}_{\mathcal{O}_i}$.

For model demander \mathcal{A} .

The input of model demander the initialized model parameters (θ) . The model demander's view is

$$\begin{aligned} \text{view}_{\mathcal{A}} = & \{\theta, [\mathbf{xy}_t]_P, [e^{\mathbf{x}_t}]_R, r, [e^{-\theta \mathbf{x}_t + r} + e^r]_P, [\lambda \mathbf{x}_t y_t]_P, \\ & [\frac{\mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r}]_P, [\frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta]_P, [\frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta]_P; \\ & \text{out}_{\text{block}5}; \text{out}_{\text{block}8}; \text{out}_{\text{block}9}\} \\ \text{out}_{\text{block}5} = & [e^{-\theta \mathbf{x}_t}]_R; \text{out}_{\text{block}8} = [e^{-\theta \mathbf{x}_t}]_P; \\ \text{out}_{\text{block}9} = & \text{update}(\theta) \end{aligned}$$

As you can see, except for the model parameters θ , all other data are encrypted by data owners public key. As Paillier and Cloud-RSA's cryptosystem is semantically secure, model demander can only infer training dataset information from θ or $\text{update}(\theta)$.

In this case, we see $(\theta, \text{update}(\theta))$ as a ciphertext, where model demander infers information by observing $(\theta, \text{update}(\theta))$. But the model demander just observes a ciphertext $(\theta, \text{update}(\theta))$ and attempts to determine information about the underlying plaintext (or plaintexts) of training dataset \mathcal{D} , which is a ciphertext-only attack. Besides, observing θ and $\text{update}(\theta)$ have no effect on the the model demander's knowledge regarding the actual message that was sent. That is for every probability data in training dataset $x_i \in \mathcal{D}$, and every ciphertext θ and $\text{update}(\theta)$:

$$\Pr[M = x_i | C = \theta \text{ or } \text{update}(\theta)] = \Pr[M = x_i]$$

Thus, inferring data owners' data from θ or $\text{update}(\theta)$ is a ciphertext-only attack with perfectly secret. Thereby $S_{\mathcal{A}} \equiv_c \text{view}_{\mathcal{A}}$.

In particular, secure power function, Biling Block 8, secure addition, secure plaintext-ciphertext multiplication, secure subtraction, and Building Block 8 are secure in the honest-but-curious model. We obtain the security of privacy-preserving LR training protocol using Modular Sequential Composition.

Collusion situations.

■ We discuss the security when α ($\alpha \leq n - 1$) data owners collude with each other to infer the model parameters θ and other data owners' data. Considering the most extreme case, $\alpha = n - 1$. The $n - 1$ data owners have information:

$$\{(\mathcal{D}_i, [e^{\theta \mathbf{x}_t + r} + e^r]_P, \frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}, [\frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}]_P)_{i=0}^{n-1}\}$$

This case is almost the same as Equation (18) where each data owner without collusion, the security of which that we have proved above. Thus, θ cannot be figured out.

Without the corresponding private key of the data owner who do not participating in the collusion, the ciphertext indistinguishability of Paillier ensures that no bit of information is leaked from ciphertexts of other data owners who do not participating in the collusion.

■ We discuss the security when α ($\alpha \leq n - 2$) data owners collude with model demander to infer other data owners' data. Considering the most extreme cases, $\alpha = n - 2$.

The $n - 2$ data owners have information:

$$\{(\mathcal{D}_i, [e^{\theta \mathbf{x}_t + r} + e^r]_P, \frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}, [\frac{\mathbf{x}_t}{e^{\theta \mathbf{x}_t + r} + e^r}]_P)_{i=0}^{n-2}\} \quad (19)$$

The model demander have information:

$$\begin{aligned} & \{\theta, ([\mathbf{x}_t y_t]_P^i, [e^{\mathbf{x}_t}]_R^i, r, [e^{-\theta \mathbf{x}_t + r} + e^r]_P^i, [\lambda \mathbf{x}_t y_t]_P, \\ & [\frac{\mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r}]_P^i, [\frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta]_P^i, [\frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta]_P^i, \\ & [e^{-\theta \mathbf{x}_t}]_R^i, [e^{-\theta \mathbf{x}_t}]_P^i)_{i=0}^n \} \end{aligned} \quad (20)$$

Combining Equation (19) and Equation (20), we obtain:

$$\begin{aligned} & \{\theta, (\mathbf{x}_t y_t, e^{\mathbf{x}_t}, r, e^{-\theta \mathbf{x}_t + r} + e^r, \lambda \mathbf{x}_t y_t, \\ & \frac{\mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r}, \frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta, \frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta, \\ & e^{-\theta \mathbf{x}_t}, e^{-\theta \mathbf{x}_t})_{i=0}^{n-2} \} \text{ with} \\ & ([\mathbf{x}_t y_t]_P^i, [e^{\mathbf{x}_t}]_R^i, r, [e^{-\theta \mathbf{x}_t + r} + e^r]_P^i, [\lambda \mathbf{x}_t y_t]_P, \\ & [\frac{\mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r}]_P^i, [\frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta]_P^i, [\frac{\lambda \mathbf{x}_t}{e^{-\theta \mathbf{x}_t + r} + e^r} + \theta]_P^i, \\ & [e^{-\theta \mathbf{x}_t}]_R^i, [e^{-\theta \mathbf{x}_t}]_P^i)_{i=n-1}^n \end{aligned}$$

Without the corresponding private key, they cannot figure out $([\mathbf{x}_t y_t]_P^i, [e^{\mathbf{x}_t}]_R^i)_{i=n-1}^n$. Therefor, α data owners collude with model demander cannot infer other data owners' data. \square

Proposition A.8. Privacy-preserving NB training protocol is secure in the honest-but-curious model.

Proof A.8 (for Proposition A.8). We prove the security without collusion first.

For each data owner \mathcal{O}_i .

After sending the encrypted dataset to model demander, the data owner does not receive any message and call to any other protocols during the execution processes, his view only consists in its input. The input of the data owner is $((\text{SK}, \text{PK})_{\text{Paillier}}, \mathcal{D}_i)$. We use the trivial simulator that just outputs its inputs for the proof of security. Hence, $S_{\mathcal{O}_i} = (\mathcal{D}_i, \text{coins}) = \text{view}_{\mathcal{O}_i}$.

For model demander \mathcal{A} . The input of model demander is $((\text{SK}, \text{PK})_{\text{Paillier}}^{\mathcal{A}})$. The model demander's view is

$$\begin{aligned} \text{view}_{\mathcal{A}} = & \{ \\ & \mu_{y,j}, \sigma_{y,j}^2, \sum_{c=1}^n |\mathcal{D}_c(y)|, \sum_{c=1}^n |\mathcal{D}_c^y(x_{ij})|, \sum_{i=1}^{|\mathcal{D}|} x_{ij}, \sum_{i=1}^{|\mathcal{D}|} (x_{ij})^2 \} \end{aligned} \quad (21)$$

$$\begin{aligned} \mu_{y,j} &= \frac{\sum_{i=1}^{|\mathcal{D}|} x_{ij}}{m} \\ \sigma_{y,j}^2 &= \frac{\sum_{i=1}^{|\mathcal{D}|} (\mu_{y,j})^2}{m} + \frac{\sum_{i=1}^{|\mathcal{D}|} (x_{ij})^2}{m} - 2\mu_{y,j} * \frac{\sum_{i=1}^{|\mathcal{D}|} (x_{ij})}{m} \end{aligned}$$

Model demander may try to infer data owners' data from his view. In this case, we see the message in Equation (21) as a ciphertext, where model demander infers information of \mathcal{D} by observing these message. The model demander just observes the message in Equation (21) and attempts to determine information about the underlying plaintext (or plaintexts), which is a ciphertext-only attack.

Observing the message in Equation (21) have no effect on the the model demander's knowledge regarding the actual message that was sent. That is for every probability data in training dataset $x \in \mathcal{D}_{n-1} \cup \mathcal{D}_n$, and every ciphertext $c \in$ Equation (24):

training dataset $x \in \mathcal{D}$, and every ciphertext $c \in$ Equation (21):

$$\Pr[M = x | C = c] = \Pr[M = x]$$

Thus, inferring data owners' data from message in Equation (21) is a ciphertext-only attack with perfectly secret. Thereby $S_{\mathcal{A}} \equiv_c \text{view}_{\mathcal{A}}$.

In particular, secure summation protocol is secure in the honest-but-curious model. We obtain the security of privacy-preserving SVM training protocol using Modular Sequential Composition.

Collusion situations.

■ We discuss the security when α ($\alpha \leq n-1$) data owners collude with each other to infer the model parameters $P(y)$ and $P(\mathbf{x}_i | y)$ and other data owners' data. Considering the most extreme case, $\alpha = n-1$. The $n-1$ data owners have information:

$$\{(\mathcal{D}_i)_{i=1}^{n-1}\}$$

Since the $n-1$ data owners didn't even receive other information during Protocol 3,. It is straightforward that $P(y)$ and $P(\mathbf{x}_i | y)$ cannot be figured out. Without the corresponding private key of the data owner who do not participating in the collusion, the ciphertext indistinguishability of Paillier ensures that no bit of information is leaked.

■ We discuss the security when α ($\alpha \leq n-2$) data owners collude with the model demander to infer other data owners' data. Considering the most extreme cases, $\alpha = n-2$.

The $n-2$ data owners have information:

$$\{(\mathcal{D}_i)_{i=1}^{n-2}\} \quad (22)$$

The model demander have information:

$$\{\mu_{y,j}, \sigma_{y,j}^2, \sum_{c=1}^n |\mathcal{D}_c(y)|, \sum_{c=1}^n |\mathcal{D}_c^y(x_{ij})|, \sum_{i=1}^{|\mathcal{D}|} x_{ij}, \sum_{i=1}^{|\mathcal{D}|} (x_{ij})^2\} \quad (23)$$

Combining Equation (16) and Equation (17), we can figure out:

$$\{(|\mathcal{D}_{n-1}(y)| + |\mathcal{D}_n(y)|), (|\mathcal{D}_{n-1}^y(x_{ij})| + |\mathcal{D}_n^y(x_{ij})|), \sum_{x_{ij} \in \mathcal{D}_{n-1} \cup \mathcal{D}_n} x_{ij}, \sum_{x_{ij} \in \mathcal{D}_{n-1} \cup \mathcal{D}_n} (x_{ij})^2\} \quad (24)$$

Model demander and data owners try to infer $x_{ij}, y_i \in \mathcal{D}_{n-1} \cup \mathcal{D}_n$ from Equation 24.

In this case, we see the message in Equation (24) as a ciphertext. The model demander just observes a ciphertext and attempts to determine information about the underlying plaintext (or plaintexts), which is a ciphertext-only attack.

Observing the message in Equation (24) have no effect on the the model demander's knowledge regarding the actual message that was sent. That is for every probability data in training dataset $x \in \mathcal{D}_{n-1} \cup \mathcal{D}_n$, and every ciphertext $c \in$ Equation (24):

$$\Pr[M = x | C = c] = \Pr[M = x]$$

Thus, inferring data owners' data from message in Equation (21) is a ciphertext-only attack with perfectly secret.

Therefor, α data owners collude with model demander cannot infer other data owners' data. \square

K. Complexity Analysis

Let l be the length of attribute value. Supposing n is the number of data owners, and T is the maximum number of iterations.

It is straightforward that the number of ciphertext computation included in the following building blocks is constant: secure addition, secure subtraction, secure plaintext-ciphertext multiplication, secure ciphertext-ciphertext multiplication secure summation and two converting building blocks. Therefore, the time complexity of the above building blocks is $\mathcal{O}(1)$.

The number of the outermost loop is d in secure power function and secure plaintext-ciphertext dot product, which processes one attribute at each loop. The time complexity of secure power function is $\mathcal{O}(ld)$.

Privacy-preserving SVM training protocol employs secure plaintext-ciphertext dot product in each iteration. Thus, the time complexity is $\mathcal{O}(Tld)$.

Privacy-preserving LR training protocol adopts secure power function in each iteration. Hence, the time complexity is $\mathcal{O}(Tld)$.

Privacy-preserving NB training protocol calls for other building blocks than secure power function and secure plaintext-ciphertext dot product. And the number of the outermost loop of it is d . Therefor, the time complexity of it is $\mathcal{O}(d \cdot ld)$.

L. Homomorphic Definition

Formalized definition of homomorphic is given in Definition 6.

Definition 6 (Homomorphic [37]). A public-key encryption scheme (Gen , Enc , Dec) is homomorphic if for all n and all (PK, SK) output by $Gen(1^n)$, it is possible to define groups \mathbb{M} , \mathbb{C} (depending on PK only) such that:

- 1) The message space is \mathbb{M} , and all ciphertexts output by Enc_{PK} are elements of \mathbb{C} .
- 2) For any $m_1, m_2 \in \mathbb{M}$, any c_1 output by $Enc_{PK}(m_1)$, and any c_2 output by $Enc_{PK}(m_2)$, it holds that $Dec_{SK}(o(c_1, c_2)) = \sigma(m_1, m_2)$.

M. A Case Study of Secure Power Function

This section provides a case study for explicating the recovering of $e^{\theta_i x_i}$ from $[e^{x_i \theta_i^1}]_R$ and $[e^{x_i \theta_i^2}]_R$. The input of the data owner is:

$$\mathbf{x} = \{0.1, 0.2\}, \quad e^{\mathbf{x}} = \{1.10517091808, 1.22140275816\}$$

$$e^{\hat{\mathbf{x}}} = \{110, 122\}; \quad [e^{\hat{\mathbf{x}}}]_R = \{[110]_R, [122]_R\}$$

The input of model demander is:

$$\theta = \{1.31, 2.42\}, \quad \hat{\theta} = \{(1, 31), (2, 42)\}$$

\triangle *Secure power function.* The data owner sends $[e^{\hat{\mathbf{x}}}]_R$ to the model demander. The model demander computes:

$$\begin{aligned} & \{([110]_R^1, [110]_R^{31}), ([122]_R^2, [122]_R^{42})\} \Leftrightarrow \\ & \{([110]_R, [1.9194342e + 63]_R), ([14884]_R, [4.237531e + 87]_R)\} \\ & \rightarrow \{[1637240]_R, [8.133662e + 150]_R\} \end{aligned}$$

At this time, the model demander has finished a secure power function $([1637240]_R * [\sqrt[100]{8.133662e + 150}]_R = [e^{\hat{\mathbf{x}}\theta}]_R)$. In our privacy-preserving LR training protocol, the model demander continues to Bilding Block 8.

\triangle *Conversion protocol (Bilding Block 8) for recovering.* The model demander picks a $r = -2$ randomly, and computes:

$$e^{-2} = 0.13533528323; \quad e^{-2} = 1353; \quad [e^{-2}]_R = [1353]_R$$

$$[e^{\mathbf{x}\theta + \hat{1.01}r}]_R = \{[2215185720]_R, [1.100484e + 154]_R\}$$

The model demander sends $([e^{\mathbf{x}\theta + \hat{1.01}r}]_R, (1+2)*2+4, (31+42)*2+4)$ to the data owner. The data owner computes:

$$\begin{aligned} [e^{\mathbf{x}\theta + \hat{1.01}r}]_R \rightarrow e^{\mathbf{x}\theta + \hat{1.01}r} &= \frac{2215185720}{1e + 10} * \sqrt[100]{\frac{1.100484e + 154}{1e + 150}} \\ &= 0.221518572 * 0.97817337451 = 0.21668356909 \end{aligned}$$

$$0.21668356909 \rightarrow 22 \rightarrow [22]_P$$

The data owner sends $[22]_P$ to the model demander. $e^{2.02} = 7.53832493366 \rightarrow (7, 54)$ The model demander obtains $[e^{\hat{\mathbf{x}}\theta}]_P$ by:

$$\begin{aligned} \{([22]_P^7, 2 * 7), ([22]_P^{54}, 2 * 54 + 2)\} \Leftrightarrow \\ \{([154]_P, 2), ([1188]_P, 4)\} \end{aligned}$$

Bilding Block 8 is end at here, where the plaintext of $\{([154]_P, 2), ([1188]_P, 4)\}$ is $\frac{154}{100} + \frac{1188}{10000} = 1.6588 \approx e^{0.1*1.31+0.2*2.42} = 1.83$.

REFERENCES

- [1] M. binti Mohamad Noor and W. H. Hassan, “Current research on internet of things (iot) security: A survey,” *Computer Networks*, vol. 148, pp. 283 – 294, 2019. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128618307035>
- [2] M. Ammar, G. Russello, and B. Crispo, “Internet of things: A survey on the security of iot frameworks,” *Journal of Information Security and Applications*, vol. 38, pp. 8 – 27, 2018. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S2214212617302934>
- [3] C. Sun, A. Shrivastava, S. Singh, and A. Gupta, “Revisiting unreasonable effectiveness of data in deep learning era,” in *2017 IEEE International Conference on Computer Vision (ICCV)*, Oct 2017, pp. 843–852.
- [4] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*. Springer, 2017.
- [5] P. Mohassel and Y. Zhang, “Secureml: A system for scalable privacy-preserving machine learning,” in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 19–38.
- [6] J. Konen, B. McMahan, F. X. Yu, and D. B. Peter Richtrik, Ananda Theertha Suresh, “Federated learning: Strategies for improving communication efficiency,” *CoRR*, vol. abs/1610.05492, 2016.
- [7] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, “Deep learning with differential privacy,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’16. New York, NY, USA: ACM, 2016, pp. 308–318.
- [8] J. Vaidya, M. Kantarcioglu, and C. Clifton, “Privacy-preserving naive bayes classification,” *The VLDB Journal*, vol. 17, no. 4, pp. 879–898, Jul. 2008.
- [9] F.-J. Gonzlez-Serrano, n. Navia-Vzquez, and A. Amor-Martn, “Training support vector machines with privacy-protected data,” *Pattern Recogn.*, vol. 72, pp. 93–107, Dec. 2017. [Online]. Available: <https://doi.org/10.1016/j.patcog.2017.06.016>
- [10] T. Li, J. Li, X. Chen, Z. Liu, W. Lou, and T. Hou, “Npmml: A framework for non-interactive privacy-preserving multi-party machine learning,” *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [11] K. Mandal and G. Gong, “Privfl: Practical privacy-preserving federated regressions on high-dimensional data over mobile networks,” in *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*, 2019, pp. 57–68.

- [12] Y. Rahulamathavan, R. C. W. Phan, S. Veluru, K. Cumanan, and M. Rajarajan, "Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 5, pp. 467–479, Sept 2014.
- [13] T. Graepel, K. Lauter, and M. Naehrig, "ML confidential: Machine learning on encrypted data," in *Information Security and Cryptology – ICISC 2012*, T. Kwon, M.-K. Lee, and D. Kwon, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–21.
- [14] X. Liu, R. Lu, J. Ma, L. Chen, and B. Qin, "Privacy-preserving patient-centric clinical decision support system on naive bayesian classification," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 2, pp. 655–668, March 2016.
- [15] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Efficient privacy preserving k-means clustering," in *Intelligence and Security Informatics*, H. Chen, M. Chau, S.-h. Li, S. Urs, S. Srinivasa, and G. A. Wang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 154–166.
- [16] T. Li, C. Gao, L. Jiang, W. Pedrycz, and J. Shen, "Publicly verifiable privacy-preserving aggregation and its application in iot," *Journal of Network and Computer Applications*, vol. 126, pp. 39–44, 2019.
- [17] S. Li, K. Xue, Q. Yang, and P. Hong, "Ppma: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462–471, 2017.
- [18] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2016, pp. 341–350.
- [19] N. G. Paterakis, E. Mocanu, M. Gibescu, B. Stappers, and W. van Alst, "Deep learning versus traditional machine learning methods for aggregated energy demand prediction," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6.
- [20] N. Prakash, A. Manconi, and S. Loew, "Mapping landslides on eo data: Performance of deep learning models vs. traditional machine learning models," *Remote Sensing*, vol. 12, no. 3, p. 346, 2020.
- [21] C. Stanik, M. Haering, and W. Maalej, "Classifying multilingual user feedback using traditional machine learning and deep learning," in *2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)*, 2019, pp. 220–226.
- [22] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, pp. 580–587.
- [23] G. Chérion, I. Laptev, and C. Schmid, "P-cnn: Pose-based cnn features for action recognition," in *Proceedings of the IEEE international conference on computer vision*, 2015, pp. 3218–3226.
- [24] W. Wang, C.-M. Vong, Y. Yang, and P.-K. Wong, "Encrypted image classification based on multilayer extreme learning machine," *Multidimensional Syst. Signal Process.*, vol. 28, no. 3, pp. 851–865, Jul. 2017.
- [25] M. D. Cock, R. Dowsley, C. Horst, R. Katti, A. Nascimento, S. Truex, and W.-S. Poon, "Efficient and private scoring of decision trees, support vector machines and logistic regression models based on pre-computation," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2017.
- [26] R. Bost, R. A. Popa, S. Tu, and S. Goldwasser, "Machine learning classification over encrypted data," in *Network and Distributed System Security Symposium*, 2014.
- [27] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: ACM, 2015, pp. 1310–1321. [Online]. Available: <http://doi.acm.org/10.1145/2810103.2813687>
- [28] G. Jagannathan, K. Pillaiapakkamatt, and R. Wright, "A practical differentially private random decision tree classifier," in *2009 IEEE International Conference on Data Mining Workshops*, Dec 2009, pp. 114–121.
- [29] Y. Aono, T. Hayashi, L. T. Phong, and L. Wang, "Input and output privacy-preserving linear regression," *IEICE TRANSACTIONS on Information and Systems*, vol. 100, no. 10, pp. 2339–2347, 2017.
- [30] Y. AONO, T. HAYASHI, L. T. PHONG, and L. WANG, "Privacy-preserving logistic regression with distributed data sources via homomorphic encryption," *IEICE Transactions on Information and Systems*, vol. E99.D, no. 8, pp. 2079–2089, 2016.
- [31] M. d. Cock, R. Dowsley, A. C. Nascimento, and S. C. Newman, "Fast, privacy preserving linear regression over distributed datasets based on pre-distributed data," in *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, ser. AISec '15. New York, NY, USA: ACM, 2015, pp. 3–14.
- [32] E. Shi, H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Annual Network & Distributed System Security Symposium (NDSS)*. Internet Society., 2011.
- [33] G. Acs and C. Castelluccia, "I have a dream! (differentially private smart metering)," in *Information Hiding*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 118–132.
- [34] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: ACM, 2017, pp. 1175–1191. [Online]. Available: <http://doi.acm.org/10.1145/3133956.3133982>
- [35] Y. Shoukry, K. Gatsis, A. Alanwar, G. Pappas, S. Seshaia, M. Srivastava, and P. Tabuada, "Privacy-aware quadratic optimization using partially homomorphic encryption," in *2016 IEEE 55th Conference on Decision and Control (CDC)*, Dec 2016, pp. 5053–5058.
- [36] D. Mittal, D. Kaur, and A. Aggarwal, "Secure data mining in cloud using homomorphic encryption," in *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, Oct 2014, pp. 1–7.
- [37] J. Katz and Y. Lindell, *Introduction to modern cryptography*, ser. CRC Cryptography and Network Security Series. CRC press, 2014.
- [38] K. El Makkaoui, A. Ezzati, and A. Beni-Hssane, "Cloud-rsa: An enhanced homomorphic encryption scheme," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Cham: Springer International Publishing, 2017, pp. 471–480.
- [39] R. Canetti, "Security and composition of multiparty cryptographic protocols," *Journal of Cryptology*, vol. 13, no. 1, pp. 143–202, Jan 2000. [Online]. Available: <https://doi.org/10.1007/s001459910006>
- [40] C. Juvekar, V. Vaikuntanathan, and A. Chandrakasan, "Gazelle: A low latency framework for secure neural network inference," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, 2018, pp. 1651–1669. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity18/presentation/juvekar>
- [41] Z. Zhang, B. I. Rubinstein, C. Dimitrakakis *et al.*, "On the differential privacy of bayesian inference," in *AAAI*, 2016, pp. 2365–2371.
- [42] P. Martins, L. Sousa, and A. Mariano, "A survey on fully homomorphic encryption: An engineering perspective," *ACM Comput. Surv.*, vol. 50, no. 6, pp. 83:1–83:33, Dec. 2017. [Online]. Available: <http://doi.acm.org/10.1145/3124441>
- [43] Y. Aono, T. Hayashi, L. Trieu Phong, and L. Wang, "Scalable and secure logistic regression via homomorphic encryption," in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '16. New York, NY, USA: ACM, 2016, pp. 142–144.
- [44] Y. Aono, T. Hayashi, L. Wang, S. Moriai *et al.*, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333–1345, 2017.
- [45] O. Goldreich, *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.
- [46] E. Roth, D. Noble, B. H. Falk, and A. Haeberlen, "Honeycrisp: large-scale differentially private aggregation without a trusted core," in *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, 2019, pp. 196–210.
- [47] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 308–318.
- [48] A. Nitaj and T. Rachidi, "Factoring rsa moduli with weak prime factors," in *Codes, Cryptology, and Information Security*, S. El Hajji, A. Nitaj, C. Carlet, and E. M. Soudi, Eds. Cham: Springer International Publishing, 2015, pp. 361–374.
- [49] D. Boneh, "Twenty years of attacks on the rsa cryptosystem," *NOTICES OF THE AMS*, vol. 46, pp. 203–213, 1999.
- [50] Z. Wang, K. Crammer, and S. Vucetic, "Breaking the curse of kernelization: Budgeted stochastic gradient descent for large-scale svm training," *J. Mach. Learn. Res.*, vol. 13, no. 1, pp. 3103–3131, Oct. 2012. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2503308.2503341>
- [51] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private naive bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89 – 104, 2018.

Excellent Talents in University from Ministry of Education, P.R. China. His research interests include Internet of Things, Cloud Computing Security, Internet and Mobile Security.

Xiangyun Tang received the B.Eng degree in computer science from Minzu University of China, Beijing, China in 2016. Currently she is a Ph.D student in the Department of Computer Science, Beijing Institute of Technology. Her research interests include Differential Privacy and Secure Multi-party Computation.

Meng Shen received the B.Eng degree from Shandong University, Jinan, China in 2009, and the Ph.D degree from Tsinghua University, Beijing, China in 2014, both in computer science. Currently he serves in Beijing Institute of Technology, Beijing, China, as an associate professor. His research interests include privacy protection for cloud and IoT, blockchain applications, and encrypted traffic classification. He received the Best Paper Runner-Up Award at IEEE IPCCC 2014. He is a member of the IEEE.

Jie Zhang received the B.Eng degree in computer science from China University of Mining and Technology, Jiangsu, China in 2018. Currently he is a master student in the Department of Computer Science, Beijing Institute of Technology. His research interests include blockchain applications and machine learning privacy.

Xiaojiang Du (S'99-M'03-SM'09-F'20) is a tenured professor in the Department of Computer and Information Sciences at Temple University, Philadelphia, USA. Dr. Du received his B.S. and M.S. degree in electrical engineering from Tsinghua University, Beijing, China in 1996 and 1998, respectively. He received his M.S. and Ph.D. degree in electrical engineering from the University of Maryland College Park in 2002 and 2003, respectively. His research interests are wireless communications, wireless networks, security, and systems. He has authored over 400 journal and conference papers in these areas, as well as a book published by Springer. Dr. Du has been awarded more than \$5 million US dollars research grants from the US National Science Foundation (NSF), Army Research Office, Air Force, NASA, the State of Pennsylvania, and Amazon. He won the best paper award at IEEE GLOBECOM 2014 and the best poster runner-up award at the ACM MobiHoc 2014. He serves on the editorial boards of three international journals. Dr. Du is a Fellow of IEEE and a Life Member of ACM.