High Throughput Asymmetric 3PC: A Secure Prediction Framework

Harsh Chaudhari, Ashish Choudhury, Arpita Patra and Ajith S.
Indian Institute Of Science, Bangalore

Abstract

We use our asymmetric 3PC setting in the regime of secure server-aided machine-learning (ML) inference for a range of prediction functions– linear regression, linear SVM regression, logistic regression, and linear SVM classification. Our setting considers a model owner with trained model parameters and a client with a query, with the latter willing to learn the prediction of her query based on the model parameters of the former. The inputs and computation is outsourced to a set of three non-colluding servers. The security is provided against an adversary who may control one of the servers and one amongst the model owner and the client, either semi-honestly or maliciously. Our constructions catering to both semi-honest and malicious world and over rings and fields, invariably perform better than the existing constructions.

Introduction

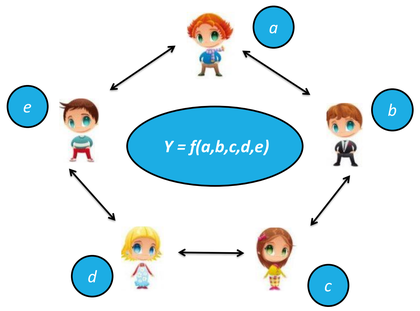
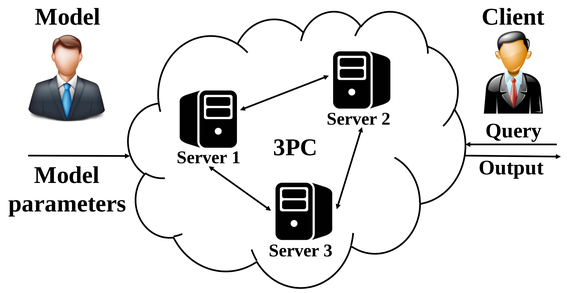


Figure 1. Multiparty Computation

Multiparty Computation (MPC) : Secure Multi-party computation(MPC), introduced by Andew Chi Chi Yao, is arguably regarded as the most fundamental problem in cryptography and it can model any task in cryptography. MPC can be viewed as the computation of the value of a public function upon the private inputs of a set of distrusting parties. To do so the parties engage in a protocol, by exchanging messages, and thus obtain the output of the desired function. The goal is that the output of the protocol is just the value of the function, and nothing else is revealed. The distrust among the parties is formalized by having an adversary that may corrupt some of the parties. A passive/semi-honest adversary simply acts as an observer. It eavesdrops the corrupted parties and tries to gain more information than allowed from the protocol transcript. But it follows the prescribed protocol. In contrary, an active/malicious adversary takes full control over the corrupted parties. As such it can deviate at will from the prescribed protocol.

PPML Setup



In this section, we describe our setup for secure prediction. A model-owner Pm, holding a vector of trained model parameters, would like to offer ML prediction service to a client Pc holding a query vector as per certain prediction function. In the server-aided setting, Pc and Pm outsource their respective inputs in shared fashion to three untrusted but non-colluding servers {P0,P1,P2} who perform the computation in shared fashion via techniques developed for our 3PC protocols and reconstruct the output to the client alone. The client learns the output and nothing beyond. We assume a computationally bounded adversary A, who can corrupt at most one of the servers {P0,P1,P2} and one of {Pm,Pc} in either semi-honest or malicious fashion. The security against an adversary $\mathcal{A}$ corrupting parties in both sets {P0,P1,P2} and {Pm,Pc} semi-honestly and likewise maliciously reduces to the semi-honest and respectively malicious security of our 3PC protocols.

Function	Mapping	P_m's input	P_c's input
Linear Regression	Π^{p}_{re} / Π^{m}_{re}	$\vec{p} = \vec{w}, v = b$	$\vec{q} = \vec{z}$
SVM Regression	Π^{p}_{re} / Π^{m}_{re}	$\vec{p} = (p_1, \ldots, p_d)$, where $p_i = \sum_{j=1}^{k} \alpha_j y_j x_{ji}$ and $v = b$	$\vec{q} = \vec{z}$
Logistic Regression	Π^{p}_{cl} / Π^{m}_{cl}	$\vec{p} = \vec{w}, v = b - \ln(\frac{t}{1-t})$	$\vec{q} = \vec{z}$
SVM Classification	Π^{p}_{cl} / Π^{m}_{cl}	$\vec{p} = (p_1, \ldots, p_d)$, where $p_i = \sum_{j=1}^{k} \alpha_j y_j x_{ji}$ and $v = b$	$\vec{q} = \vec{z}$

Table 1. Mapping to ML Algorithms to 3PC Protocols

Results

Work	Π^{p}_{re}		Π^{m}_{re}		Π^{p}_{cl}		Π^{m}_{cl}	
	Offline	Online	Offline	Online	Offline	Online	Offline	Online
ABY^3 [51]	31.19	0.47	63.35	1.41	31.19	3.78	63.35	5.67
ABY^3-opt	0.00		0.95		0.00		0.97	
This	0.47	0.00	2.11	0.94	0.48	1.79	2.16	2.98
LAN setting (*ms*)								
ABY^3 [51]	15.16	0.23	30.78	0.69	15.16	1.84	30.78	2.76
ABY^3-opt	0.00		0.46		0.00		0.46	
This	0.23	0.00	1.00	0.46	0.23	0.65	1.00	1.41
WAN setting (*s*)								
ABY^3 [51]	0.11	0.03	74.17	55.15	0.11	0.08	74.46	55.29
ABY^3-opt	0.00	0.02	73.5	55.13	0.00	0.07	73.69	55.26
This	0.01	0.00	128.63	12.27	0.04	0.05	129.12	12.36
Communication (KB)								

Table 2. Time taken to process one Clinet's query

Protocol	Bandwidth	Semi-honest			Malicious		
		ABY^3 [51] / ABY^3-opt	**This**	Gain	ABY^3 [51] / ABY^3-opt	**This**	Gain
Reg.	BW-1	0.66 M	8 M	**12.21**×	278.64	417.96	**1.5**×
	BW-2	0.16 M		**48.83**×	69.66		**6**×
Clas.	BW-1	0.10 M	0.21 M	**2.08**×	277.93	416.90	**1.5**×
	BW-2	0.05 M		**3.98**×	69.48		**6**×
LAN setting (#queries/sec); 'M' denotes million							
Protocol	Bandwidth	Semi-honest			Malicious		
		ABY^3 [51] / ABY^3-opt	**This**	Gain	ABY^3 [51] / ABY^3-opt	**This**	Gain
Reg.	BW-1	0.104 M	480 M	**4600**×	0.010 M	0.031 M	**3**×
	BW-2				0.002 M		**15**×
Clas.	BW-1	0.013 M	0.037 M	**2.83**×	0.009 M	0.016 M	**1.8**×
	BW-2				0.002 M		**7.5**×
WAN setting (#queries/min); 'M' denotes million							

Table 3. Number of queries processed per second / min

Contact

Harsh Chaudhari
Indian Institute Of Science, Bangalore
Email : chaudharim@iisc.ac.in
Phone : +918879023240

References

1. [MR18] MOHASSEL .P and RINDAL.P, ABY3 : A Mixed Protocol Framework for Machine Learning, In ACM CCS (2018).
2. [MZ17] MOHASSEL .P and ZHANG.Y, SecureML: A system for scalable privacy preserving machine learning, In IEEE S&P (2017).
3. [RTSSK18] RIAZI.M. S, WEINERT.C, TKACHENKO.O, SONGHORI.E.M, SCHNEIDER.T, and KOUSHANFAR.F, Chameleon: A hybrid secure computation framework for machine learning applications. In AsiaCCS (2018).
4. [NNOB12] WAGH .S, GUPTA.D and CHANDRAN.N, SecureNN: Efficient and private neural network training. IACR Cryptology ePrint Archive (2018).