Qiang Wang, Fu-cai ZHOU, Tie-min MA, Zi-feng XU, 2018. Faster fog-aided private set intersection with integrity preserving. *Frontiers of Information Technology & Electronic Engineering,* 19(12):1558-1568. https://doi.org/10.1631/FITEE.1800518

Faster fog-aided private set intersection with integrity preserving

Key words: Private set intersection; Fog computing; Verifiable; Data privacy

Corresponding author: Fu-cai ZHOU
E-mail: fczhou@mail.neu.edu.cn
ORCID: Qiang WANG, http://orcid.org/0000-0003-4480-9314

Motivation

1. With the development of fog computing, the need has arisen to delegate PSI on outsourced datasets to the fog.

2. The existing PSI schemes are based on either fully homomorphic encryption (FHE) or pairing computation. To the best of our knowledge, FHE and pairing operations consume a huge amount of computational resource.

3. These PSI schemes cannot be applied to fog computing due to some inherent problems such as unacceptable latency and lack of mobility support.

Main contributions in theoretical aspect

(1) We introduce the concept of FFPSI and give its system model and security model.

(2) Taking advantage of the Rivest-Shamir-Adleman (RSA) cryptosystem, we design an efficient FFPSI protocol and prove itssecurity against the untrusted fog.

(3) We assess the performance of the proposed scheme through theoretical analysis and simulation, and compare the results with those of the state-of-the-art schemes in terms of computation overhead and communication overhead. Theoretical analysis and simulation show that our proposed scheme is more efficient and practical.

Main Contributions in practical aspect

(1) high checkability of the correctness of computation results;

(2) strong privacy for the data owner in the process of outsourcing and delegated computation;

(3) low computational burden for the data owner by eliminating FHE and pairing operations either when the fog identifies the common dataset or when the data owner checks the integrity of delegated computation.

Architecture

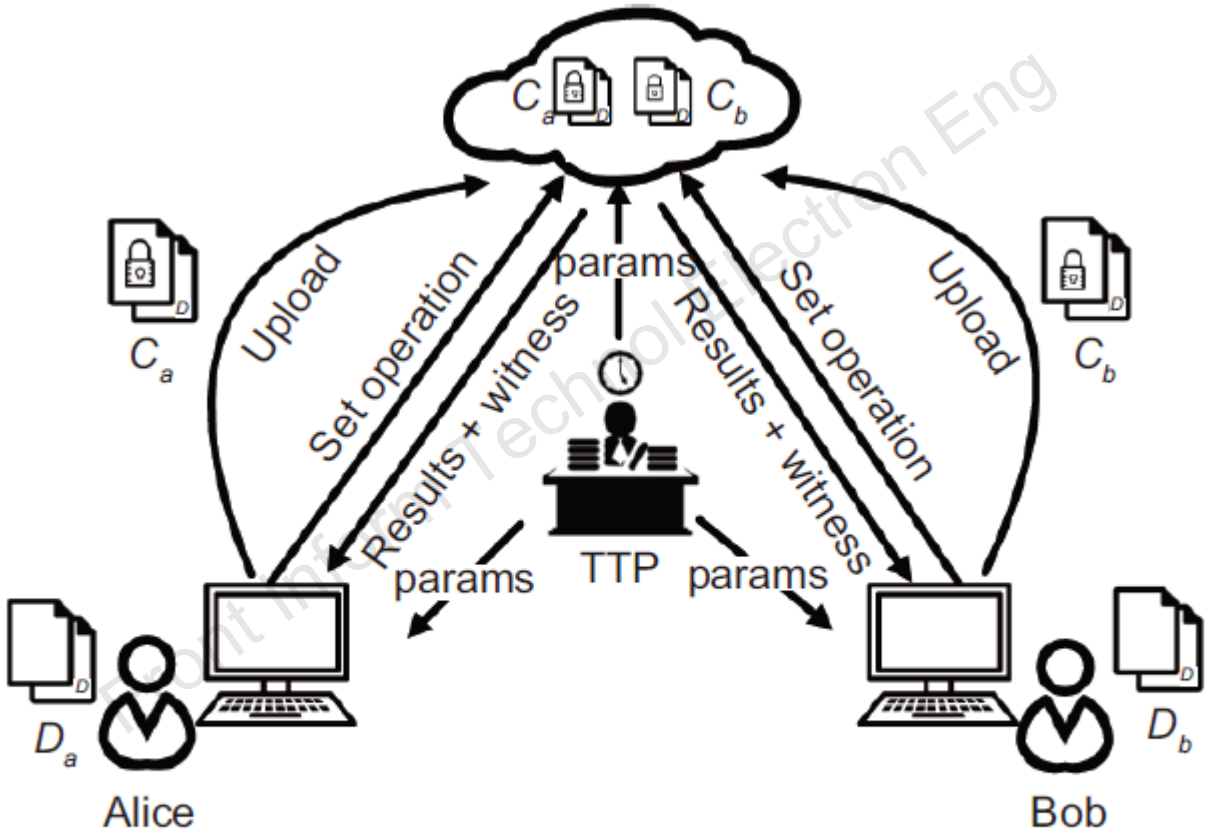

Fig. 1 Architecture of the faster fog-aided private set intersection with the integrity preserving protocol

Major results

Table 2 Comparison of communication cost between our proposed scheme and state-of-the-art schemes

Phase	Communication cost					
	VDSI (Zheng and Xu, 2015)		VDPSI (Abadi et al., 2016)		Our scheme	
	Alice	Cloud	Alice	Cloud	Alice	Fog
Outsourcing	$(3n+1)Z_p^* + 1G$	$(3n+3m+2)Z_p^* + 2G$	$(10d+20)Z_p^*$	$(8d+12)Z_p^*$	$(2n+2)Z_p^*$	$(2n+2m+4)Z_p^*$
Intersection	$3kZ_p^* + 4G$	$3kZ_p^* + 4G$	$(2d+3)Z_p^*$	$(2d+3)Z_p^*$	$(2k+5)Z_p^*$	$(2k+5)Z_p^*$

$1G$ denotes one element of bilinear group G and $1Z_p^*$ denotes one item of Z_p^*

Table 3 Comparison of computation cost between our proposed scheme and state-of-the-art schemes

Algorithm	Computation cost		
	VDSI (Zheng and Xu, 2015)	VDPSI (Abadi et al., 2016)	Our scheme
Enc	$3n$Exp+nPairing	N/A	$3n$Exp
Dec	$2n$Exp	N/A	nExp
AuGen	4Exp	$(2d+3)$FHE.E + $(6d+9)$Exp	3Exp
SetI	$3(n+m)$Pairing	$(2d+3)$FHE.E + $(2d+3)$Exp	$(n+m)$Exp
Verify	$(3k+2)$Exp + $(k+7)$Pairing	$(2d+3)$FHE.D	$2k$Exp

Exp: cost time of exponentiation; Pairing: cost time of bilinear pairing; FHE.E: cost time of fully homomorphic encryption; FHE.D: cost time of fully homomorphic decryption

Table 4 Development environment

Scheme	Security parameter size (bit)	Library	Hardware environment
VDSI (Zheng and Xu, 2015)	160	OpenSSL, GMP, PBC, NTL	CPU: Intel Core i7
VDPSI (Abadi et al., 2016)	1024	OpenSSL, GMP, NTL	Physical memory: 8 GB
Our scheme	1024	OpenSSL, NTL	OS: Ubuntu 18.04 LTS

Major results

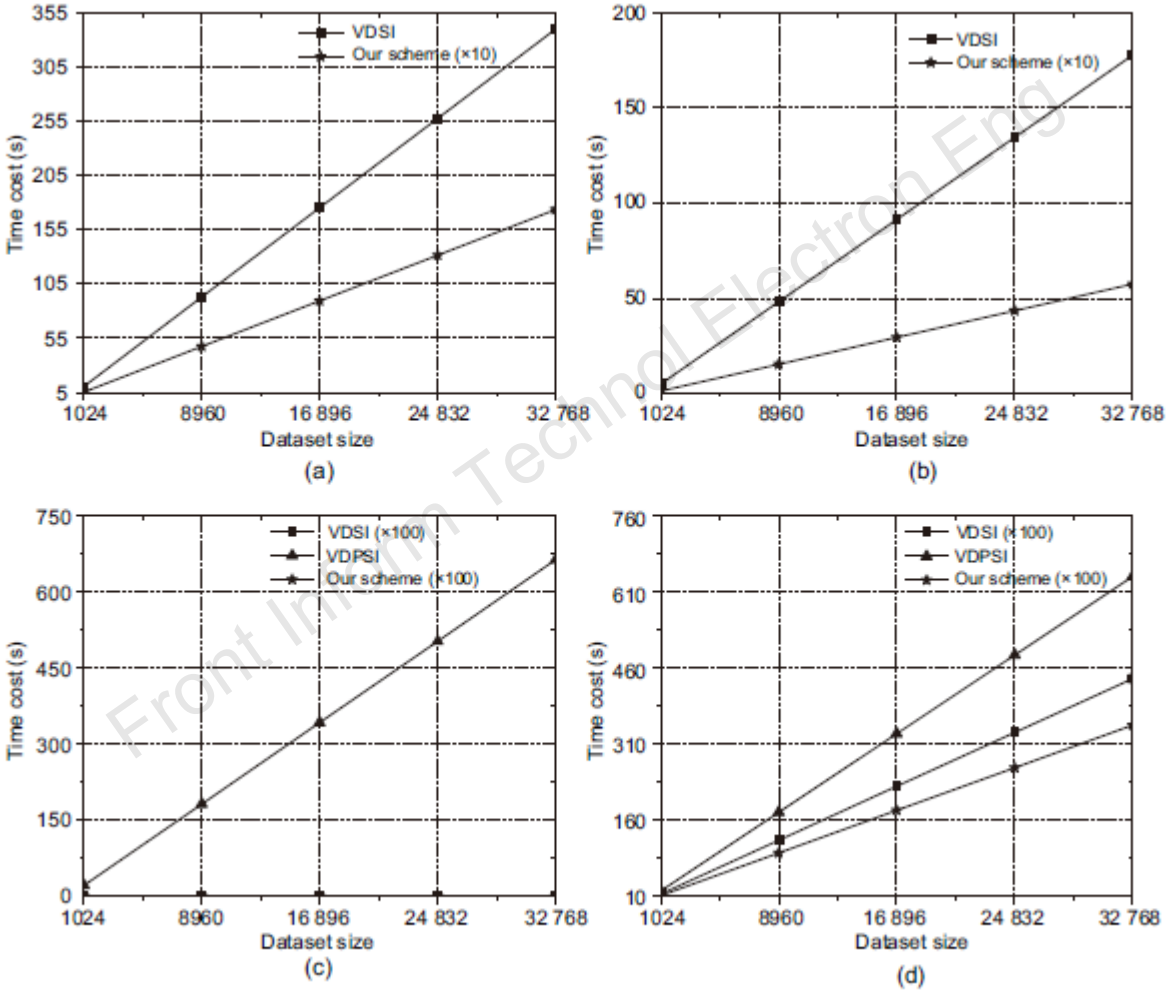

Fig. 2 Computation cost comparison among common algorithms: (a) Enc; (b) Dec; (c) AuGen; (d) SetI

Major results

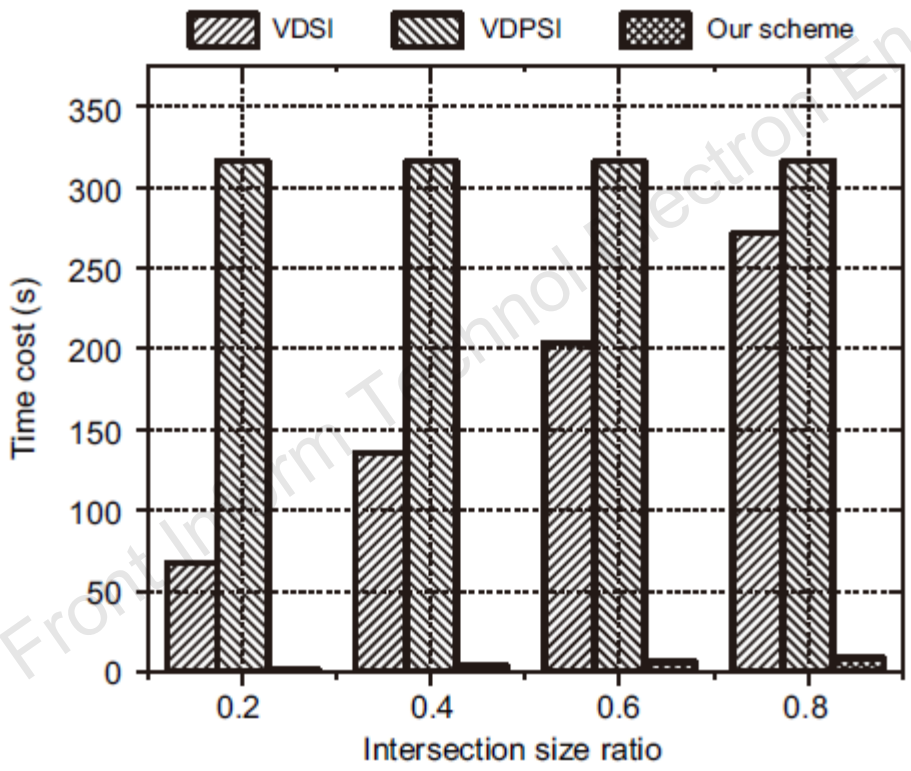

Fig. 3 Computation cost at dataset size $n = 32\,768$

Conclusions

1. we proposed a new primitive called “faster fog-aided private set intersection with integrity preserving (FFPSI),” where the fog conducts delegated intersection over encrypted data without the decryption capacity.
2. One of our technical highlights is to reduce the computation cost greatly by eliminating the pairing computation.
3. We have made a detailed theoretical analysis and simulation between our scheme and several state-of-the-art schemes in two directions: communication overhead and computation overhead. Theoretical analysis and simulation showed that our scheme is more efficient and practical.