LaTeX Example Doc

Bikash Thapa
CS 800

Current draft: 2/9/26 at 3:34pm EDT

Look at the source main.tex to see how this is done.

1 URIs

This is a formatted, clickable link to my webpage: `https://www.cs.odu.edu/~cs_bthap004/`

2 Images

All figures must have a caption and must be referenced in the text. See the example below.

Figure 1 shows an original PNG with no scaling or cropping. The original dimensions are 1919 x 802 (or, 6.4in x 2.67in). Figure 2 shows an example of cropping the image using the `trim, clip` options to `includegraphics`.

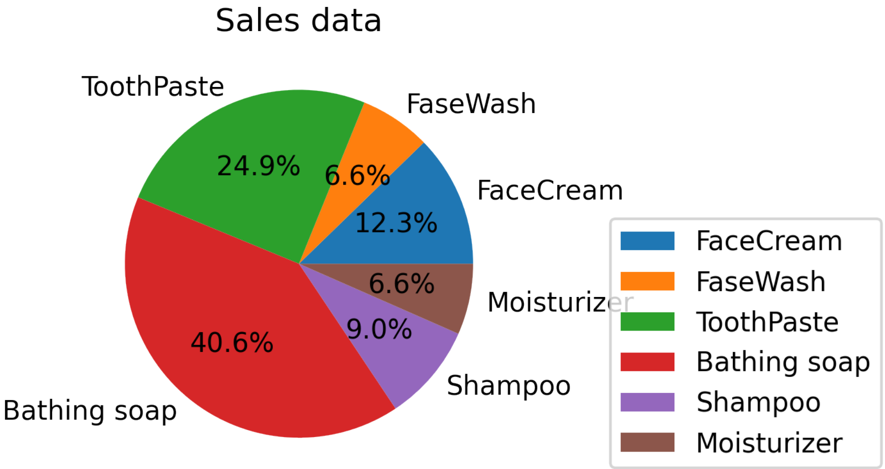


Figure 1: Original PNG

Figure 3 shows the same cropping as Figure 2 but scaled up. It’s a bit blurry because the original image (Figure 1 was a low resolution.)

We can insert PDFs into the document in the same way as images. Figure 4 is the first page of an academic paper. I’ve added the `\frame` command to show where the boundaries are. Figure 5 shows the margins trimmed off so that the text can be larger (scaled up).

3 Quotation Marks

Quotation marks are weird in LaTeX. Here, we have used one: ”Where there’s a will, there’s a way”. *Not quite right.* Here’s the proper way “Where there’s a will, there’s a way”. It’s two

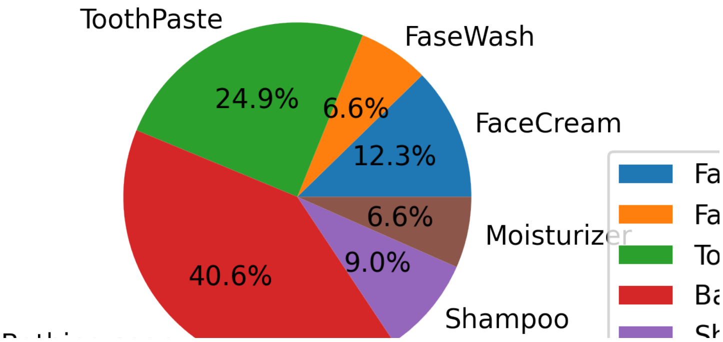


Figure 2: Cropped PNG - 0.25in from left, 0.5in from bottom, 1in from right, 0.3in from top

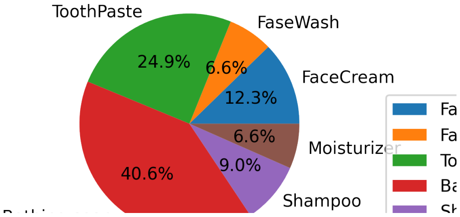


Figure 3: Cropped and scaled PNG

backticks and two single quotes: ‘‘Where there’s a will, there’s a way’’

4 Tables

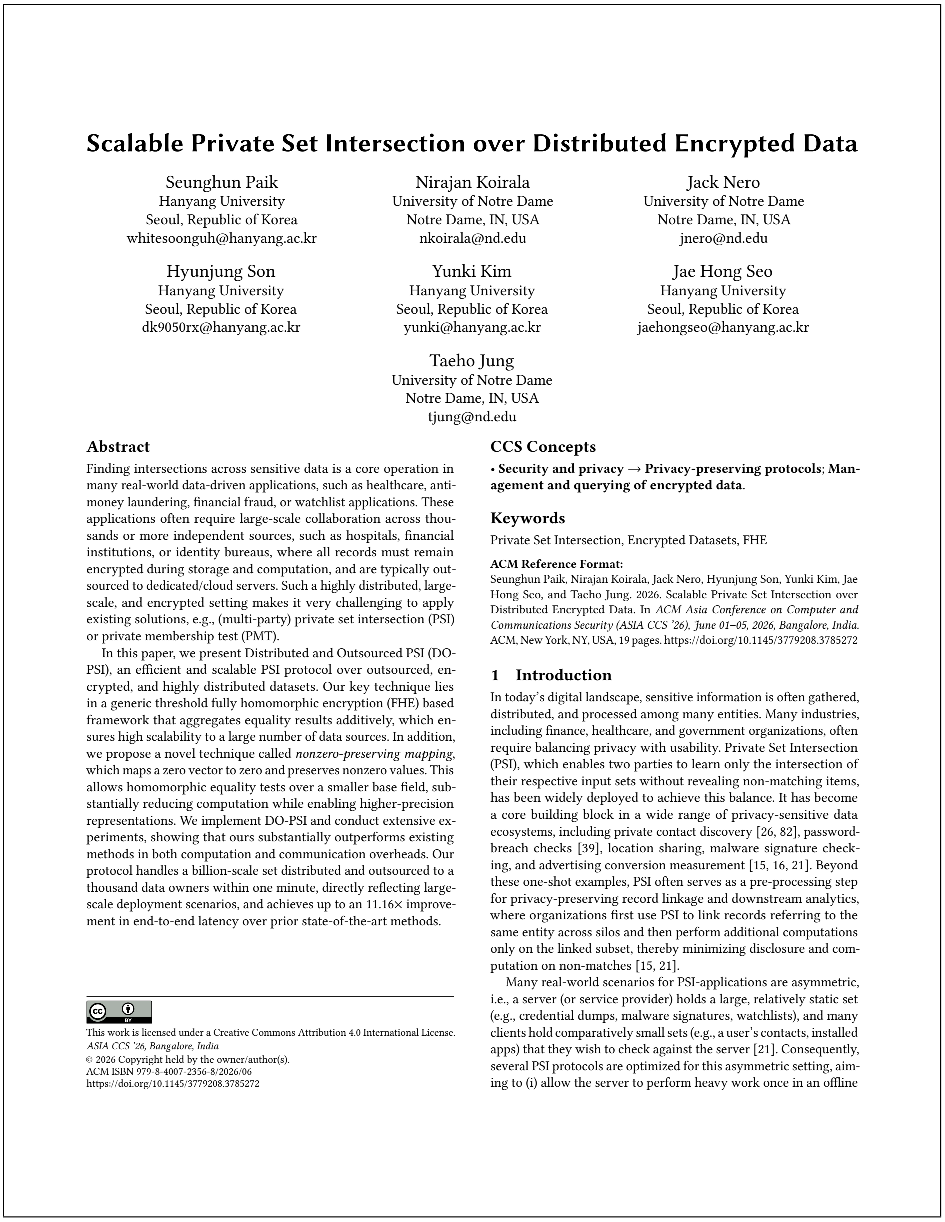
Table 1 shows a simple example table of evaluating a function value for certain input range. Table 2 shows types of Homomorphic Encryption which is captioned below unlike the first one. Table 2 employs toprule, midrule and bottomrule feature that gives the horizontal straight line to the table.

Table 1: $\tanh(x)$ function evaluation for $x \in \{-5, \ldots, 5\}$

x	$\tanh(x)$
-5	-0.9999
-4	-0.9993
-3	-0.9951
-2	-0.9640
-1	-0.7616
0	0
1	0.7616
2	0.9640
3	0.9951
4	0.9993
5	0.9999

Types	**Supported Operations**	**Number of Operations**
Partially Homomorhic Encryption	Either × or +	Unlimited
Somewhat Homomorhic Encryption	Both × or +	Limited
Fully Homomorhic Encryption	Both × or +	Unlimited

Table 2: Types of Homomorphic Encryption



Scalable Private Set Intersection over Distributed Encrypted Data

Seunghun Paik
Hanyang University
Seoul, Republic of Korea
whitesoonguh@hanyang.ac.kr

Nirajan Koirala
University of Notre Dame
Notre Dame, IN, USA
nkoirala@nd.edu

Jack Nero
University of Notre Dame
Notre Dame, IN, USA
jnero@nd.edu

Hyunjung Son
Hanyang University
Seoul, Republic of Korea
dk9050rx@hanyang.ac.kr

Yunki Kim
Hanyang University
Seoul, Republic of Korea
yunki@hanyang.ac.kr

Jae Hong Seo
Hanyang University
Seoul, Republic of Korea
jaehongseo@hanyang.ac.kr

Taeho Jung
University of Notre Dame
Notre Dame, IN, USA
tjung@nd.edu

Abstract

Finding intersections across sensitive data is a core operation in many real-world data-driven applications, such as healthcare, anti-money laundering, financial fraud, or watchlist applications. These applications often require large-scale collaboration across thousands or more independent sources, such as hospitals, financial institutions, or identity bureaus, where all records must remain encrypted during storage and computation, and are typically outsourced to dedicated/cloud servers. Such a highly distributed, large-scale, and encrypted setting makes it very challenging to apply existing solutions, e.g., (multi-party) private set intersection (PSI) or private membership test (PMT).

In this paper, we present Distributed and Outsourced PSI (DO-PSI), an efficient and scalable PSI protocol over outsourced, encrypted, and highly distributed datasets. Our key technique lies in a generic threshold fully homomorphic encryption (FHE) based framework that aggregates equality results additively, which ensures high scalability to a large number of data sources. In addition, we propose a novel technique called *nonzero-preserving mapping*, which maps a zero vector to zero and preserves nonzero values. This allows homomorphic equality tests over a smaller base field, substantially reducing computation while enabling higher-precision representations. We implement DO-PSI and conduct extensive experiments, showing that ours substantially outperforms existing methods in both computation and communication overheads. Our protocol handles a billion-scale set distributed and outsourced to a thousand data owners within one minute, directly reflecting large-scale deployment scenarios, and achieves up to an 11.16× improvement in end-to-end latency over prior state-of-the-art methods.

ASIA CCS '26, Bangalore, India

ACM ISBN 979-8-4007-2356-8/2026/06
https://doi.org/10.1145/3779208.3785272

CCS Concepts

• **Security and privacy** → **Privacy-preserving protocols**; **Management and querying of encrypted data**.

Keywords

Private Set Intersection, Encrypted Datasets, FHE

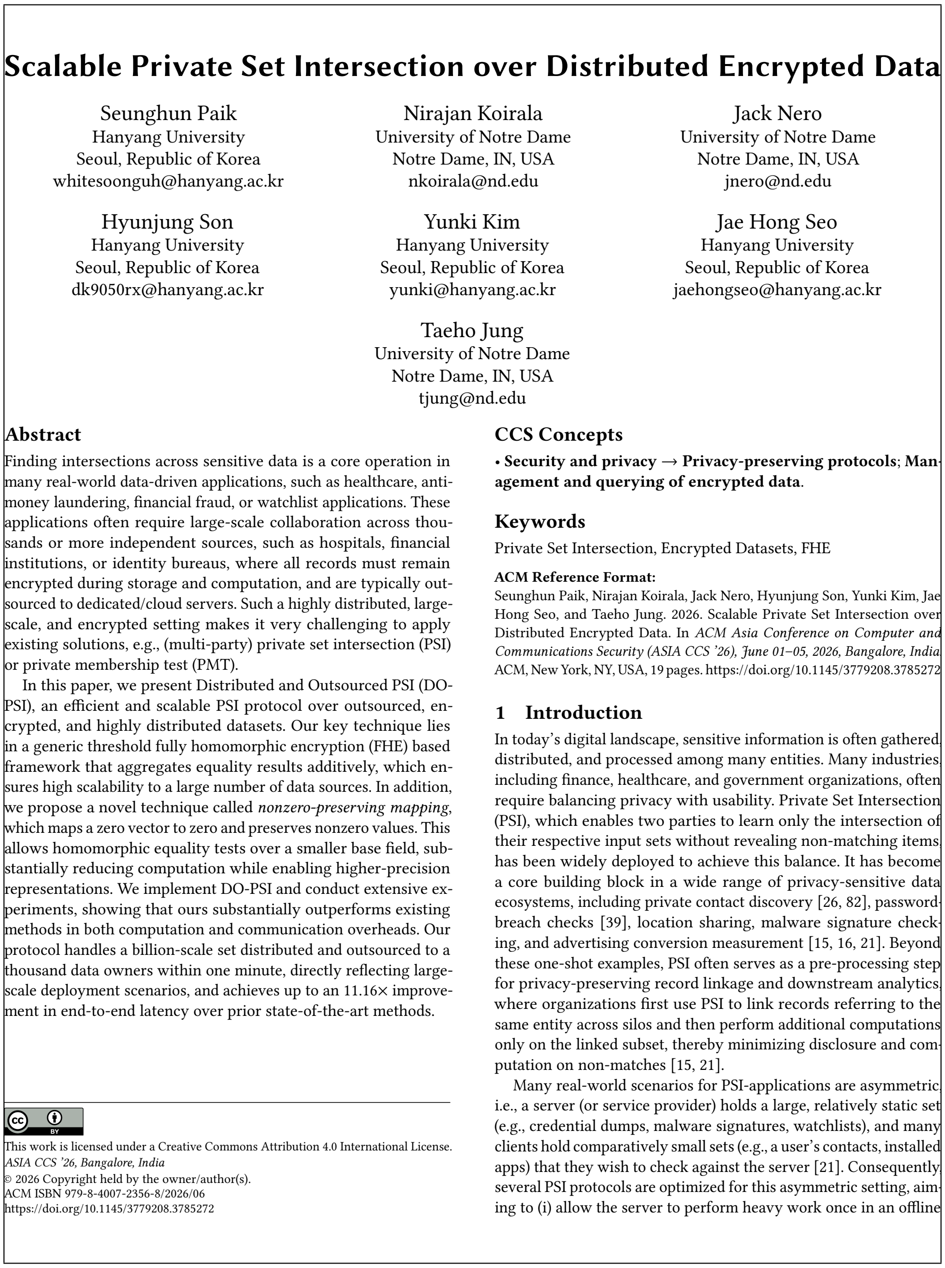
ACM Reference Format:
Seunghun Paik, Nirajan Koirala, Jack Nero, Hyunjung Son, Yunki Kim, Jae Hong Seo, and Taeho Jung. 2026. Scalable Private Set Intersection over Distributed Encrypted Data. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '26), June 01–05, 2026, Bangalore, India.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3779208.3785272

1 Introduction

In today's digital landscape, sensitive information is often gathered, distributed, and processed among many entities. Many industries, including finance, healthcare, and government organizations, often require balancing privacy with usability. Private Set Intersection (PSI), which enables two parties to learn only the intersection of their respective input sets without revealing non-matching items, has been widely deployed to achieve this balance. It has become a core building block in a wide range of privacy-sensitive data ecosystems, including private contact discovery [26, 82], password-breach checks [39], location sharing, malware signature checking, and advertising conversion measurement [15, 16, 21]. Beyond these one-shot examples, PSI often serves as a pre-processing step for privacy-preserving record linkage and downstream analytics, where organizations first use PSI to link records referring to the same entity across silos and then perform additional computations only on the linked subset, thereby minimizing disclosure and computation on non-matches [15, 21].

Many real-world scenarios for PSI-applications are asymmetric, i.e., a server (or service provider) holds a large, relatively static set (e.g., credential dumps, malware signatures, watchlists), and many clients hold comparatively small sets (e.g., a user's contacts, installed apps) that they wish to check against the server [21]. Consequently, several PSI protocols are optimized for this asymmetric setting, aiming to (i) allow the server to perform heavy work once in an offline

Figure 4: Inserted PDF



Scalable Private Set Intersection over Distributed Encrypted Data

Seunghun Paik
Hanyang University
Seoul, Republic of Korea
whitesoonguh@hanyang.ac.kr

Nirajan Koirala
University of Notre Dame
Notre Dame, IN, USA
nkoirala@nd.edu

Jack Nero
University of Notre Dame
Notre Dame, IN, USA
jnero@nd.edu

Hyunjung Son
Hanyang University
Seoul, Republic of Korea
dk9050rx@hanyang.ac.kr

Yunki Kim
Hanyang University
Seoul, Republic of Korea
yunki@hanyang.ac.kr

Jae Hong Seo
Hanyang University
Seoul, Republic of Korea
jaehongseo@hanyang.ac.kr

Taeho Jung
University of Notre Dame
Notre Dame, IN, USA
tjung@nd.edu

Abstract

Finding intersections across sensitive data is a core operation in many real-world data-driven applications, such as healthcare, anti-money laundering, financial fraud, or watchlist applications. These applications often require large-scale collaboration across thousands or more independent sources, such as hospitals, financial institutions, or identity bureaus, where all records must remain encrypted during storage and computation, and are typically outsourced to dedicated/cloud servers. Such a highly distributed, large-scale, and encrypted setting makes it very challenging to apply existing solutions, e.g., (multi-party) private set intersection (PSI) or private membership test (PMT).

In this paper, we present Distributed and Outsourced PSI (DO-PSI), an efficient and scalable PSI protocol over outsourced, encrypted, and highly distributed datasets. Our key technique lies in a generic threshold fully homomorphic encryption (FHE) based framework that aggregates equality results additively, which ensures high scalability to a large number of data sources. In addition, we propose a novel technique called *nonzero-preserving mapping*, which maps a zero vector to zero and preserves nonzero values. This allows homomorphic equality tests over a smaller base field, substantially reducing computation while enabling higher-precision representations. We implement DO-PSI and conduct extensive experiments, showing that ours substantially outperforms existing methods in both computation and communication overheads. Our protocol handles a billion-scale set distributed and outsourced to a thousand data owners within one minute, directly reflecting large-scale deployment scenarios, and achieves up to an 11.16× improvement in end-to-end latency over prior state-of-the-art methods.

ASIA CCS '26, Bangalore, India

ACM ISBN 979-8-4007-2356-8/2026/06
https://doi.org/10.1145/3779208.3785272

CCS Concepts

• **Security and privacy → Privacy-preserving protocols**; **Management and querying of encrypted data**.

Keywords

Private Set Intersection, Encrypted Datasets, FHE

ACM Reference Format:
Seunghun Paik, Nirajan Koirala, Jack Nero, Hyunjung Son, Yunki Kim, Jae Hong Seo, and Taeho Jung. 2026. Scalable Private Set Intersection over Distributed Encrypted Data. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '26), June 01–05, 2026, Bangalore, India*. ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3779208.3785272

1 Introduction

In today's digital landscape, sensitive information is often gathered, distributed, and processed among many entities. Many industries, including finance, healthcare, and government organizations, often require balancing privacy with usability. Private Set Intersection (PSI), which enables two parties to learn only the intersection of their respective input sets without revealing non-matching items, has been widely deployed to achieve this balance. It has become a core building block in a wide range of privacy-sensitive data ecosystems, including private contact discovery [26, 82], password-breach checks [39], location sharing, malware signature checking, and advertising conversion measurement [15, 16, 21]. Beyond these one-shot examples, PSI often serves as a pre-processing step for privacy-preserving record linkage and downstream analytics, where organizations first use PSI to link records referring to the same entity across silos and then perform additional computations only on the linked subset, thereby minimizing disclosure and computation on non-matches [15, 21].

Many real-world scenarios for PSI-applications are asymmetric, i.e., a server (or service provider) holds a large, relatively static set (e.g., credential dumps, malware signatures, watchlists), and many clients hold comparatively small sets (e.g., a user's contacts, installed apps) that they wish to check against the server [21]. Consequently, several PSI protocols are optimized for this asymmetric setting, aiming to (i) allow the server to perform heavy work once in an offline

Figure 5: Trimmed PDF