

# Third Paper Selection: Comparison of Candidates

November 24, 2025

## 1 Selected Papers for Detailed Study

### 1.1 Paper Links

Paper Title	Link	Shortform
Data Poisoning Attacks to Local Differential Privacy Protocols	<a href="#">USENIX PDF</a>	Cao2020
Locally Differentially Private Protocols for Frequency Estimation	<a href="#">USENIX PDF</a>	Wang2017

### 1.2 Publication Details

Shortform	Year	Venue	Rank	Google Scholar Category
Cao2020	2020	USENIX Security	#1	<a href="#">Computer Security &amp; Cryptography</a>
Wang2017	2017	USENIX Security	#1	<a href="#">Computer Security &amp; Cryptography</a>

## 2 Candidate Papers

### 2.1 Paper Links

Paper Title	Link	Shortform
Locally Differentially Private Heavy Hitter Identification	<a href="#">Semantic Scholar</a>	Wang2021
Discrete Distribution Estimation under Local Privacy	<a href="#">Semantic Scholar</a>	Kairouz2016
Further Study on Frequency Estimation under Local Differential Privacy	<a href="#">USENIX</a>	Fang2025

### 2.2 Publication Details

Shortform	Year	Venue	Rank	Google Scholar Category
Wang2021	2021	IEEE TDSC	#6	<a href="#">Computer Security &amp; Cryptography</a>
Kairouz2016	2016	ICML/PMLR	#3	<a href="#">Artificial Intelligence</a>
Fang2025	2025	USENIX Security	#1	<a href="#">Computer Security &amp; Cryptography</a>

### 3 Unreviewed Candidate Papers

#### 3.1 Paper Links

Paper Title	Link	Shortform
RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response	<a href="#">Scopus</a>	RAPPOR2014
Locally Differentially Private Frequency Estimation with Consistency	<a href="#">NDSS 2020 PDF</a>	Wang2020
Mitigating Data Poisoning Attacks to Local Differential Privacy	<a href="#">arXiv</a>	Li2025Mitig

#### 3.2 Publication Details

Shortform	Year	Venue	Rank	Google Scholar Category
RAPPOR2014	2014	ACM CCS	#5	<a href="#">Computer Security &amp; Cryptography</a>
Wang2020	2020	NDSS	#7	<a href="#">Computer Security &amp; Cryptography</a>
Li2025Mitig	2025	ACM CCS	#5	<a href="#">Computer Security &amp; Cryptography</a>

## 4 Analysis of Wang2021

#### 4.1 Relevance to Cao2020

Introduces the PEM, which is mentioned in Cao2020 in the following sections:

Cao2020 Section	PEM Discussion
Section 2.2	Introduces PEM as state-of-the-art heavy hitter protocol with iterative prefix-based mechanism using OLH
Section 4.2	Data poisoning attacks (RPA, RIA, MGA) manipulate bits in each iteration to push attacker-chosen items into top-k

*Continued on next page*

Table 7 – *Continued from previous page*

<b>Cao2020 Section</b>	<b>PEM Discussion</b>
Section 5.3	MGA achieves 100% attack success with $\sim 5\%$ fake users on multiple datasets
Section 6.2	Fake user detection via frequent itemset mining at each PEM iteration

## 5 Analysis of Fang2025

### 5.1 Contribution

- It's a very recent paper and introduces a latest LDP protocol called RWS
- To be filled
- To be filled

### 5.2 Relevance to Wang2017

Shows that OUE and OLH are not optimally parameterized, introducing improvements with RUE and RLH. The paper discusses OUE and OLH in the following sections:

<b>Fang2025 Section</b>	<b>Sec- tion</b>	<b>Protocol</b>	<b>Discussion</b>
Section 3.2		OUE	Main definition section for Optimized Unary Encoding
Section 3.3		OLH	Main definition section for Optimized Local Hashing
Section 3.5		OUE & OLH	Summary comparing protocols; states OUE and OLH only achieve optimal MSE for large $d$
Section 4		OUE & OLH	Explains that OUE and OLH were optimized using approximate equations that need improvement
Section 4.1.1		OUE $\rightarrow$ RUE	Introduces Re-optimized Unary Encoding (RUE) built from OUE
Section 4.1.2		OLH $\rightarrow$ RLH	Introduces Re-optimized Local Hashing (RLH) built from OLH
Section 4.1.3		OUE vs RUE	Parameter discussion comparing OUE and RUE optimization approaches
Section 4.2		OLH $\rightarrow$ RLH	Addresses OLH's slow server-side computation and how RLH solves it

## 6 Analysis of Kairouz2016

This paper is **not ideal for selection** as it is published in an Artificial Intelligence venue rather than a cryptography one