Efficient and Privacy-preserving Min and k-th Min Computations in Mobile Sensing Systems

Yuan Zhang, Qingjun Chen, Sheng Zhong

Abstract—Protecting the privacy of mobile phone user participants is extremely important for mobile phone sensing applications. In this paper, we study how an aggregator can expeditiously compute the minimum value or the k-th minimum value of all users' data without knowing them. We construct two secure protocols using probabilistic coding schemes and a cipher system that allows homomorphic bitwise XOR computations for our problems. Following the standard cryptographic security definition in the semi-honest model, we formally prove our protocols' security. The protocols proposed by us can support time-series data and need not to assume the aggregator is trusted. Moreover, different from existing protocols that are based on secure arithmetic sum computations, our protocols are based on secure bitwise XOR computations, thus are more efficient.

Index Terms—Mobile Sensing, Min/k-th Min computation, Privacy.

1 Introduction

With the advance of Information Technology and modern manufacturing, huge numbers of smartphones equipped with CPUs, ROMs, and a variety of sensors such as GPS, accelerometer, camera, digital compass etc., have replaced outdated "dumb phones" and entered people's lives. Smartphones are ubiquitous nowadays, and have excellent sensing, computing and communication capabilities. These advantages make the smartphone an outstanding carrier for mobile sensing jobs. A large number of projects [1], [2], [3], [4], [5] that utilize smartphones to sense have emerged in recent years.

All applications above demonstrate that technically a sensing job owner can outsource his or her job to a number of mobile phone users, collect the data sensed by these users, and then perform analyses on the aggregation of the data. However, before we put any of these applications into practical use, we still need to ask ourselves a very important question: are mobile phone users willing to give their sensed data to the job owner or the aggregator? One of the major factors that could cause a negative answer is the user's privacy. Data acquired from a user's smartphone may contain this user's private information such as physical location, health condition, etc. Consider, for example, a medical data sensing application that needs to continuously monitor users' data. Clearly, these medical data needs to be protected with caution. Without reliable privacy protection, many users would hesitate to accept an invitation from such a mobile sensing application.

In this paper, we study how to protect users' privacy in a general mobile sensing scenario: an aggregator wants to periodically learn the minimum value (Min) of all users' time-series data. Notice that we do not assume the aggregator is trusted here, so our target is to protect every user's data against other users as well as against the aggregator. Besides the Min, we also study how to securely compute the k-th minimum value (k-th Min) of all users' data, where k is a positive integer that is no greater than the total number of users.

Min and k-th Min are both very fundamental statistics that are often computed in data analysis. First, it is easy to compute the Max value using the same method that computes the Min value. Compared with the Min, k-th Min is even more powerful and can be used for computing many other important aggregation statistics, such as the median, quartiles, deciles, duo-deciles, percentiles and many other specific types of quantiles. These statistics are often computed in the mobile sensing system that monitors the temperature, air quality indexes, radiation level or the traffic speed in an area to evaluate its overall status. For example, in [6], the 85-th percentile speed of traffic on a road is often used as a guideline to set speed limits or assess whether such a limit is too high or low.

As far as we know, there are only a couple of works [7], [8], [9] that study the privacy-preserving Min or k-th Min computation in mobile phone sensing scenarios. In [7], the authors first propose an additively homomorphic encryption based on a slicing technique, and then use it to run binary searches securely to look for the minimum value. In [8], [9], the authors propose to let the aggregator traverse the entire space of data from the smallest to the largest till it finds the first data that is owned by

• *Yuan Zhang, Qingjun Chen and Sheng Zhong are with State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China. Sheng Zhong is the corresponding author.*
Emails: zhangyuan05@gmail.com, knight.chan319@gmail.com, zhongsheng@nju.edu.cn.

This work is supported by NSFC-61321491, NSFC-61425024, NSFC-61300235 and NSFC-61402223.

at least one user. The security of the above process relies on another additively homomorphic encryption proposed by Castelluccia et al. [10]. Despite many differences between them, both works are based on additive-homomorphic encryptions that can securely compute arithmetic sums.

In this paper, we propose new Min and k-th Min computation protocols for time-series data based on another technique, XOR-homomorphic encryption. Our protocols can be used by an untrusted aggregator to securely compute the minimum value or k-th minimum values in the aggregation of all users' private data. We rigorously define and prove the security of our two protocols in a standard cryptographic model (please see Section 3 for the definition and Sections 4.2 and 5.3 for the proofs). Our protocols support time-series data well in the sense that they only need to establish the keys for once only. Due to the fact that we construct our protocols based on secure bitwise XOR computations, rather than based on secure arithmetic sum computations, our protocols are more efficient in general.

The rest of this paper is organized as follows. In Section 2, we discuss the related work. Then, we introduce some necessary preliminaries in Section 3. After that, we present and analyze our privacy-preserving protocols for Min computation and for k-th Min computation, in Sections 4 and 5, respectively. After providing experimental results in Section 6, we conclude the paper in Section 8.

2 Related Work

Most previous works on privacy-preserving data aggregation assume a trusted aggregator, which is different from our scenario.

In recent years, there are a few works [7], [8], [9], [11], [12], [13], [14], [15] that study privacy-preserving data aggregation for mobile sensing without assuming a trusted aggregator. However, most of them [11], [12], [13], [14], [15] only consider how to let the aggregator compute the sum of users' data securely. Only in [7], [8], [9], after proposing their privacy-preserving protocols for sum computation, the authors show how to compute the Min based on their sum computation protocols.

In [7], Shi et al. use a binary search approach in privacy-preserving data aggregation, for computing the maximum, minimum, and percentile of data. A similar idea of binary search is also used in this paper, for constructing our protocols for computing the minimum and k-th minimum value. However, our protocols also use a number of techniques that they do not use, such as secure bitwise XOR computations, "report-determine" (see Section 4.1), probabilistic coding schemes (see Section 4.1 and Section 5.1), etc. Moreover, their protocols require communication channels between users for slicing and storing the data pieces while our protocols do not require those channels.

Li et al. 's works [8], [9] are very close to ours. Both [8] and [9] consider the same problem in a similar scenario as we do in this paper. Based on [8], Li et al. propose a scheme that utilizes the redundancy in security to reduce the communication cost incurred by each user's joining and/or leaving activities in [9]. The main differences between their works and ours is that their protocol traverses the entire data space to find the minimum value, and is based on summation protocols, while our protocols follow the idea of binary search and are based on bitwise XOR operations.

Unlike summation-based protocols, our XOR-based protocols require the use of dedicated probabilistic coding schemes for our problems, as we show in Sections 4.1 and 5.1. The advantage of using our XOR-based protocols is that they are more efficient especially when user's data space is big.

In wireless sensor networks, similar privacy-preserving data aggregation problems have been studied. Most works [16], [17], [18], [19], [20] done in this area rely on the communication and cooperation among sensor nodes. However, in our scenario, such methods may not work well because the nodes participating in the sensing may not know each other in advance. In comparison, our approach in this work does not assume any interaction among sensor nodes. Another relevant work is [21]. It proposes SDA_MIN$_{XOR}$ that uses homomorphic bitwise XOR operations to do Min aggregation similarly as us. However, there are two major differences between [21] and our work. First, the computation cost and communication cost of SDA_MIN$_{XOR}$ are much higher compared to our protocol, especially when users' data space is large (to be more precise, if the range of data is $[0, M-1]$, SDA_MIN$_{XOR}$ requires an M-dimensional vector to represent the value of a node. Also, M loops of searching are needed to find the Min value). Second, the result of SDA_MIN$_{XOR}$ protocol could be wrong when there exists duplicate values while our Min protocol does not have such an issue.

In the database community, order-preserving encryptions (OPE) [22], [23] have been studied in recent years. OPEs allow comparison operations to be directly applied on encrypted data without any decryption operation. Thus, functions such as the MAX, MIN, and COUNT can be directly processed over encrypted data. Although OPEs allow easy ciphertext-based comparison and thus Min/k-th Min computation, OPE preserves numerical ordering of the plaintexts. If we use OPE in our problem, the order information of the users' data would be revealed to the aggregator. But the order information would not be revealed to the aggregator when using our protocols. And the order information may be very sensitive in some mobile sensing applications.

3 Preliminaries

3.1 Models and Definitions

In this paper, we aim to design protocols for the following problem: a group of mobile phone users are helping a server/aggregator to do some sensing task. Assume each user's sensing data can be represented by an integer. The aggregator is interested in finding the Min/k-th Min of all users' numbers. However, users are not willing to reveal their data to the aggregator due to privacy concerns. Before we present the details of our protocols, we introduce the models and definitions used in this paper.

Network Model: We discuss a general network model in mobile phone sensing. In particular, we assume a bi-directional communication channel exists between the aggregator and every mobile phone user. In other words, the aggregator and all mobile phone users form a star network topology. In practice, the communication channels could be 3G/4G, wifi, or other kinds of channels that are supported by the mobile phones and the aggregator.

Security Model: To rigorously define the privacy requirements for our Min/k-th Min computation protocol, we adapt the standard definition of privacy [24] for cryptographic protocols in the *semi-honest* model here.

In the semi-honest model, all parties or participants are assumed to follow the protocol, but may attempt to derive extra knowledge about other parties' private inputs from what they "see" during the protocol's execution. The semi-honest model has been extensively studied in cryptography and widely applied in the privacy-preserving data aggregation area [7], [8], [9], [11], [12], [13], [14], [15], [19].

Given all parties are semi-honest, a protocol is believed to be secure if it guarantees that every party learns no more knowledge from the protocol than the knowledge that this party is entitled to know. (Generally, this knowledge is the output of the protocol.) The above security can be defined following the standard simulation paradigm [24]: If we can construct a polynomial-time simulator for each party that simulates this party's view (e.g. messages received, its own coin flips) given only this party's private input, the coins it uses, and the protocol's final output as the inputs, we can conclude that the protocol reveals no extra knowledge and thus is secure, or privacy-preserving (since without participating in the protocol, every party can simulate what it sees from participating in the protocol by running the simulator itself).

Denote by P_0 the data aggregator and by $P_1, \ldots, P_n$ the n users. Denote by $VIEW_i$, x_i, and $\mathcal{K}_i$ ($i \in \{0, \ldots, n\}$) party P_i's view, its private input and the extra knowledge revealed to it respectively, in our Min/k-th Min protocol $\mathcal{M}$. We formally define our security requirements for $\mathcal{M}$ as follows.

Definition 1. *The Min/k-th Min protocol $\mathcal{M}$ is* ***perfectly privacy-preserving*** *against party P_i in the sense that it reveals no more knowledge than the final output to P_i, if there exists a polynomial-time simulator $\mathcal{S}_i$ such that*

$$\{\mathcal{S}_i(x_i, \mathcal{M}(x_0, \ldots, x_n), \mathcal{K}_i)\}_{\{x_0,\ldots,x_n\}} \overset{c}{\equiv} \{VIEW_i(x_0, \ldots, x_n)\}_{\{x_0,\ldots,x_n\}}$$

and $\mathcal{K}_i = \emptyset$ given all possible inputs $\{x_0, \ldots, x_n\}$, where $\overset{c}{\equiv}$ denotes computational indistinguishability of two distribution ensembles. (Please refer to [24] for the definitions of computational indistinguishability and distribution ensemble.)

In cases that $\mathcal{K}_i \neq \emptyset$, we say M is ***weakly privacy-preserving*** *against P_i, in the sense that it reveals no more knowledge than $\mathcal{K}_i$ and the final output to P_i.*

Note that here we consider the cases that all protocol participants, including the aggregator and the users, are entitled to know the protocol's final output, i.e. the Min or k-th Min. Accordingly, $\mathcal{M}(x_0, \ldots, x_n)$ is included in the inputs of simulator S_i as party P_i's legitimate knowledge for both $i = 0$ (corresponding to the aggregator) and $i \neq 0$ (corresponding to the users). In cases where only the aggregator is entitled to know the protocol's final output, $\mathcal{M}(x_0, \ldots, x_n)$ should be removed from S_i's input for every $i \neq 0$ in the above security definition. Note that "perfectly privacy-preserving" is a very strong privacy requirement, since it requires that the adversary learns no extra knowledge at all except for the protocol's final output.

3.2 The Cipher in Our Protocols

The cipher we use here is a bitwise XOR homomorphic cipher, and its main idea is very similar to that of a stream cipher, or an additively homomorphic encryption scheme proposed in [10]. Denote by $h_{s,\alpha,\beta}(\dot{})$ a function in the pseudo-random function family $\mathcal{H}_{s,\alpha,\beta} = \{h_{s,\alpha,\beta} : \{0,1\}^{\alpha} \to \{0,1\}^{\beta}\}_{s \in \{0,1\}^{\gamma}}$, where $\alpha, \beta, \gamma \in \mathbb{N}$. Denote by $t \in \{0, \ldots, 2^f - 1\}$ the nonce information of data. The details of the cipher are given below.

Key Generation:

stage 1: The authority first picks $s_1, \ldots, s_n \in \{0,1\}^{\gamma}$ uniformly and independently. For each user i ($i = 1, \ldots, n$), the authority computes $S_a^i = s_i$ and $S_b^i = s_{(i \bmod n)+1}$ and sends them to user i.

stage 2: For each data set with the nonce information t, user i computes its secret key using

$$k_i = h_{S_a^i,f,l}(t) \oplus h_{S_b^i,f,l}(t)$$

Encryption: For a bit-string $x_i \in \{0,1\}^l$, user i encrypts it by computing

$$\overline{x_i} = x_i \oplus k_i$$

Decryption of user i's plaintext: For a ciphertext $\overline{x_i}$ of user i, user i decrypts by computing

$$\overline{x_i} = x_i \oplus k_i$$

Decryption of the bitwise XOR of all users' plaintexts: Anyone can decrypt the bitwise XOR of all users' plaintexts without any secret key by computing

$$x_1 \oplus \ldots \oplus x_n = \overline{x_1} \oplus \ldots \oplus \overline{x_n}$$

It is straightforward to see the bitwise XOR of all users' keys equals to 0. Thus, the bitwise XOR of all users' ciphertexts equals the bitwise XOR of all users' plaintexts. In other words, the cipher is homomorphic on the bitwise XOR computation.

In this paper, the aggregator does not have any user's private key, so that it never decrypts any user's plaintext. However, it can decrypt the bitwise XOR of all users' plaintexts and use this information to compute the Min or k-th Min. Therefore, when we talk about the aggregator's decryption operation, we mean the decryption of the bitwise XOR of all users' plaintexts.

4 Privacy-Preserving Min Computation

In this section, first we introduce our protocol for computing the minimum. After that, we present our efficiency and security analysis.

We assume there is a trusted authority who can help the aggregator and users to establish a key system for once. Assume the space of the users' data is $[0, M - 1] (M \geq 2)$. Let $l = \lceil \log_2 M \rceil$ and $m = \lceil \log_2 l \rceil$.

4.1 Privacy-preserving Min computation

In this section, we construct a protocol that allows the aggregator to compute the minimum of all users' numbers and to keep each user's data private at the same time.

Our protocol is based on a probabilistic coding scheme and the cipher system introduced in Section 3.2. Specifically, our protocol lets all users help the aggregator to determine the minimum number bit by bit, from the most significant bit (MSB) to the least significant bit (LSB). The probabilistic coding scheme is particularly designed to transform the determining process into bitwise XOR computations. The cipher system is used to encrypt users' data or codes, and perfectly protects the data privacy in these computations. In more detail, the minimum number determination is as follows. (Notice that the explanation of ideas below is written for ease of understanding. Some parts may *look insecure* but the actual complete protocol is secure, as we formally prove in Theorem 3.)

To determine the MSB of the minimum number, every user reports to the aggregator whether its data's MSB is 0 or not. (Please temporarily ignore the privacy leak here, which will be fixed later.) If there is any affirmative report, the aggregator knows that the MSB of the minimum number is 0, and is 1 otherwise. Then the aggregator broadcasts the bit that is just determined to every user, so that every user knows the MSB of the minimum number. When a user finds its number's MSB is different from the minimum number's MSB, it knows its number is greater than the minimum number, and its number's remaining bits are ineffective in determining the remaining bits of the minimum number. Therefore, the user always reports negative during the determination of the remaining bits of the minimum number. All users and the aggregator repeat the above "report-determine-broadcast-compare" procedure similarly for the remaining bits. In the end, the aggregator knows every bit of the minimum number, thus the minimum number itself.

Although the above process can determine the minimum number efficiently, it reveals every user's data. To fix this problem, we first adopt a probabilistic coding scheme to encode users' reports as random bit strings. This scheme transforms the above logic deductions in the "report-determine" steps to bitwise XOR computations of bit strings.

Denote by r a user's report ($r \in \{$"affirmative", "negative"$\}$), and by $C(r)$ the corresponding code of r in the coding scheme used in our Min computation protocol. The coding scheme is defined as follows.

$$C(r) \begin{cases} = 0^q & \text{if } r = \text{"negative"}, \\ \overset{\$}{=} \{0,1\}^q & \text{if } r = \text{"affirmative"}, \end{cases} \quad (1)$$

where $q \in \mathbb{N}$ is the accuracy controlling parameter and $\overset{\$}{=}$ denotes to sample uniformly at random.

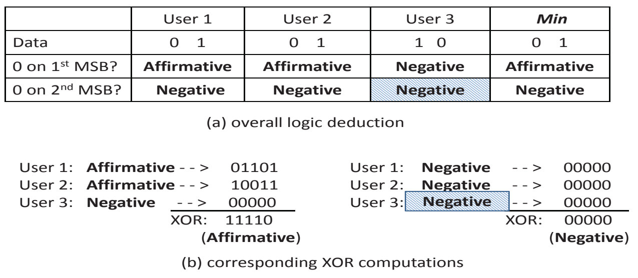
It is easy to see if all reports are negative, then the bitwise XOR of the corresponding strings is always a q-bit string of 0s, which encodes "negative". If there is any affirmative report, with a very good probability of $1 - 1/2^q$ (please see the proof of Proposition 2 for more details), the bitwise XOR of all reports' corresponding strings is not a q-bit string of 0s, especially when q is large, thus encodes "affirmative". Figure 1 gives a detailed example of determining the minimum using above logic deduction and corresponding bitwise XOR computations.

To protect users' bit strings, we use the cipher introduced in Section 3.2 to encrypt them. Users send the aggregator the ciphertexts instead of plain bit strings. When the aggregator receives all users' ciphertexts, the aggregator computes the bitwise XOR of all ciphertexts. According to Section 3.2, we know the result equals the bitwise XOR of all users' plaintexts.

Below we present more details of the protocol.

In each time period, all users help the aggregator to compute the minimum number.

All users help the aggregator to determine the MSB, the second-MSB,..., and the l-th-MSB, one by one, as



	User 1	User 2	User 3	*Min*
Data	0 1	0 1	1 0	0 1
0 on 1st MSB?	**Affirmative**	**Affirmative**	**Negative**	**Affirmative**
0 on 2nd MSB?	**Negative**	**Negative**	**Negative** ▨	**Negative**

(a) overall logic deduction

```
User 1: Affirmative - - >  01101        User 1: Negative  - - >  00000
User 2: Affirmative - - >  10011        User 2: Negative  - - >  00000
User 3: Negative    - - >  00000        User 3: Negative  - - >  00000
              XOR:  11110                             XOR:  00000
              (Affirmative)                          (Negative)
```

(b) corresponding XOR computations

Figure 1. An example of determining the Min of three users' data (without any privacy protection), where the bit string for a negative answer is encoded as a 5-bit string 00000 ($q = 5$), the bit string for an affirmative is randomly chosen from $\{0,1\}^5 \setminus \{00000\}$. The shadow area indicates a user starts to report negative after it finds it has a bit that is different from the Min's bit at the same bit location.

follows.

In the beginning, every user has a status of being "effective". During the computation, users' status may be changed to being "ineffective". Once a user's status is changed to being "ineffective", it will not be changed any more.

To determine j-th-MSB ($j = 1, \ldots, l$) of the minimum number, first every user generates a bit string x according to its status and the j-th-MSB of its number. If its status is "ineffective" or its j-th-MSB is 1, it sets x to a bit string of q 0s; otherwise, it sets x to a random q-bit string. Then it uses the cipher introduced in Section 3.2 to encrypt the q-bit string. When the aggregator receives all users' ciphertexts, the aggregator computes the bitwise XOR of all ciphertexts. According to Section 3.2, we know the result equals the bitwise XOR of all users' plaintexts. If the result equals q 0s, the aggregator sets the j-th-MSB of the minimum number to 1; otherwise, it sets it to 0.

After that, the aggregator broadcasts the j-th-MSB to every user. If the j-th-MSB of an "effective" user's number is different from it, this user sets its status to "ineffective".

Remark: One may notice a *"security flaw"*: when the aggregator finds one bit of the minimum number equals 0, it knows the bit string sent by every user in that round is q 0s with a very high probability. In this case, the cipher used in our protocol cannot protect the bit string generated by each user and the encryption keys are revealed. However, knowing one user's bit string is q 0s does NOT reveal the bit of this user's number that is currently tested. This is because both an effective user with a bit 1 and an ineffective user with a bit 0 would generate the same bit string of q 0s and the aggregator does not know a user's status. In addition, since our protocol generates new pseudo random keys in every round of the encryption operation, revealing the keys used in one round does not affect other rounds.

A formal description of the entire protocol can be found in Algorithm 1.

Algorithm 1 Privacy-preserving Min Computation Protocol

```
Require:
    A group of $n$ users;
    An aggregator;
    User $i$ ($i = 1, \ldots, n$) has two secret seeds $S_a^i$ and $S_b^i$;
    In each time period, user $i$ ($i = 1, \ldots, n$) has a number $d^i \in [0, 2^l - 1]$;
    In each time period, a public known nonce number $t \in [0, 2^f - 1]$;
    An accuracy controlling parameter $q \in \mathbb{N}$.
Ensure:
    The aggregator outputs the minimum number in $\{d^i\}_{i=1,\ldots,n}$;
1:  every user sets its status as "effective".
2:  for $j = 1, \ldots, l$ do
3:      user $i$ ($i = 1, \ldots, n$) computes $k^i = h_{S_a^i, f+m, q}(t|j) \oplus h_{S_b^i, f+m, q}(t|j)$;
4:      user $i$ ($i = 1, \ldots, n$) encodes its answer by a $q$-bit string $d^i$ according to Formula 1 and its status. $d^i$ equals to $\{0\}^q$ if user $i$'s status is "ineffective" or the $j$-th-MSB equals to 1; $d^i$ is randomly chosen in $\{0,1\}^q$ otherwise.
5:      user $i$ ($i = 1, \ldots, n$) computes $\overline{d^i} = d^i \oplus k^i$, and sends $\overline{d^i}$ to the aggregator.
6:      the aggregator computes the XOR of all $\overline{d^i}$. If the result is $\{0\}^q$, the aggregator sets $d_j^\star$, the $j$-th-MSB of the minimum number, to 1; otherwise, it sets $d_j^\star$ to 0;
7:      the aggregator broadcasts the $d_j^\star$ to all users.
8:      If an "effective" user finds the $j$-th-MSB of its number is different from $d_j^\star$, it sets its status to "ineffective".
9:  end for
10: return the minimum number $d^\star$ as $\Sigma_{j=1}^{l} d_j^\star \times 2^{l-j}$;
```

4.2 Protocol Analysis

First, we analyze the accuracy of our Min computation protocol. We have the following results.

Proposition 2. *The accuracy of the "report and determine" step is greater or equal to $1 - 1/2^q$, and the accuracy of our Min computation protocol is greater than or equal to $1 - l/2^q$.*

Proof: Note that if the "report and determine" step is 100% accurate, the bitwise XOR of all users' generated bit strings should be 0^q when all users have a negative report, and should not be 0^q when any user has an affirmative report. Recall that every user generates a bit string 0^q when it has a negative report, and a random bit string otherwise. It is easy to see that when all users have a negative report, the step is accurate. Consider that one user has an affirmative report, there is only one case that makes the step false: this user's bit string equals the bitwise XOR of all other users' strings. Since this user randomly samples its string from 2^q different choices, the probability for the bitwise XOR result being not accurate is $1 - 1/2^q$. Thus, we have:

$$\begin{aligned} & P(\text{the report and determination is accurate}) \\ = \; & P(\text{all users have negative reports}) \times 1 + \\ & P(\text{any user has an affirmative report}) * (1 - 1/2^q) \\ \geq \; & 1 - 1/2^q \end{aligned}$$

As our Min computation protocol needs to perform "report and determine" for l times, it is not difficult to prove the probability that l times are all correct is no less than $1 - l/2^q$ given q is greater than l. Due to the page limit, we skip this part of the proof here. □

Our Min computation protocol has very good computational efficiency: Once the keys have been established, on average each user mainly needs $2l$ bitwise XOR operations, $2l$ hashing operations, $3l$ comparison operations, and picking no more than ql random bits during each time period; the aggregator mainly needs $(n-1)l$ bitwise XOR operations and l comparison operations during each time period. In terms of communication efficiency, our protocol requires transmissions of $(nq+1)l$ bits on average during each time period.

In terms of security, we have the following theorem.

Theorem 3. *Our Min computation protocol is perfectly privacy-preserving against the aggregator and all users.*

Proof: In our protocol, every user only receives l bits from the aggregator, and these l bits are the same as the l bits in the bit representation of our Min protocol's output. Therefore, our protocol reveals no extra knowledge to the users.

We prove that our protocol reveals no extra knowledge to the aggregator by constructing a probabilistic polynomial-time simulator $\mathcal{S}$ that takes the output of our Min computation protocol, and simulates the aggregator's view during the execution of the protocol as follows.

In our protocol, the aggregator's view consists of the ciphertexts it receives from n users. Denote its view by $V = (V_1, V_2, \ldots, V_l)$ where $V_j = (\overline{d_j^1}, \ldots, \overline{d_j^n})$ $(j = 1, \ldots, l)$ is the ciphertexts of all users' bit strings generated to determine the j-th bit of the Min.

On input of $d^\star$ $(d^\star = \Sigma_{j=1}^{l} d_j^\star \times 2^{l-j})$, the output of our Min computation protocol, $\mathcal{S}$ simulates each V_j for determining $d_j^\star$ using $V_j' = (v_j^1, \ldots, v_j^n)$ as follows.

If $d_j^\star = 0$, $\mathcal{S}$ generates $v_j^1, \ldots, v_j^{n-1}$ independently as random q-bit strings uniformly distributed on $\{0,1\}^q$ and sets v_n to $v_j^1 \oplus v_j^2 \oplus \ldots, \oplus v_j^{n-1}$. If $d_j^\star = 1$, $\mathcal{S}$ generates $v_j^1, \ldots, v_j^n$ independently as random q-bit strings uniformly distributed on $\{0,1\}^q$. Below we prove the computational indistinguishability between V and $V' = (V_1', \ldots, V_l')$.

Due to the pseudo-randomness of the pseudo-random functions used in the cipher's key generation, it is easy to verify that

$$\overline{d_j^i} \overset{c}{\equiv} U_j^i \tag{2}$$

for every i, j and $\overline{d_j^1}, \overline{d_j^2}, \ldots, \overline{d_j^{n-1}}$ are independent variables, where U_j^i $(i = 1, \ldots, n; j = 1, \ldots, l)$ are random variables that are uniformly distributed over $\{0,1\}^l$.

Since the cipher is homomorphic on the bitwise XOR computation, we know

$$(\overline{d_j^1}, \ldots, \overline{d_j^{n-1}}, \overline{d_j^n}) \overset{c}{\equiv} (U_j^1, \ldots, U_j^{n-1}, D_j \oplus U_j[1:n-1]) \tag{3}$$

,where $D_j = d_j^1 \oplus \ldots \oplus d_j^n$ and $U_j[1:n-1] = U_j^1 \oplus, \ldots, \oplus U_j^{n-1}$.

When $d_j^\star = 0$, we have $D_j = 0^l$ according to the coding scheme, and $V_j' = (U_j^1, \ldots, U_j^{n-1}, D_j \oplus U_j[1:n-1])$. When $d_j^\star = 1$, we know $D_j \overset{c}{\equiv} U_j^n$, thus $(U_j^1, \ldots, U_j^{n-1}, D_j \oplus U_j[1:n-1]) \overset{c}{\equiv} (U_j^1, \ldots, U_j^{n-1}, U_j^n)$. In both cases,

$$V_j \overset{c}{\equiv} V_j'. \tag{4}$$

Moreover, due to the pseudo-randomness of the keys, we know $V_1, \ldots, V_l$ are independent. Thus, we know

$$V \overset{c}{\equiv} V'. \tag{5}$$

□

Remark: as we have explained in Section 3.1, here we consider all of the protocol's participants including the aggregator and the users, are entitled to know the output of the protocol. In cases where users are not entitled to know the output, we can conclude our Min protocol is weakly privacy-preserving against all users in the sense that it reveals the value of the Min to all users. (Note that this would allow each user to know whether its input is the minimum.) The proof would be almost the same as above. Only this time, we let $\mathcal{K}_i$ (i.e. knowledge that the protocol reveals to user i) equal the Min and use it as the input of the simulator constructed to simulate user i's view.

5 Privacy-Preserving k-th Min Computation

In this section, we work on the secure computation of the k-th Min in the aggregation of all users' data. First, we present a secure "pseudo-counting" protocol and analyze its accuracy. Then we show how to build our privacy-preserving k-th Min protocol based on it.

5.1 A secure pseudo-counting protocol and its accuracy

Below, we propose a secure pseudo-counting protocol, which will be used in constructing our k-th Min protocol. (By "pseudo-counting", we mean the protocol intends to count, but the result can have an error with a certain probability.) Suppose there are n users. Consider a question, for which each user has two possible answers: "affirmative" or "negative". Our protocol enables the aggregator to compute the total number of affirmative answers without knowing any specific user's reply.

First, the protocol uses a probabilistic coding scheme that is different from the one used in the secure Min computation protocol to encode users' replies. In particular, each user's reply is encoded by a q-bit string. If its reply is affirmative, the user randomly chooses a bit location x $(1 \leq x \leq q)$ and sets the x-th bit of the string to 1 and all other bits to 0; If its reply is negative, the user sets the bit string to 0^q. Denote by $C'(r)$ the code of a user's reply r in the coding scheme used here. We have

$$C'(r) = \begin{cases} 0^q & \text{if } r = \text{"negative"}, \\ \overbrace{0\dots0}^{x-1}1\overbrace{0\dots0}^{q-x} & \text{if } r = \text{"affirmative"}, \end{cases} \tag{6}$$

where $q \in \mathbb{N}$ is the accuracy controlling parameter and x is a random variable that is uniformly distributed over $\{1, \dots, q\}$.

Then, using the cipher system in Section 3.2, users encrypt their bit strings and send the ciphertexts to the aggregator. Given all users' ciphertexts, the aggregator can compute the bitwise XOR of all users' bit strings. The aggregator counts the number of 1s in the result, and outputs it as the total number of affirmative answers.

Notice that the above process does not always output the correct number of users with affirmative answers. Consider an optimistic case in which all users with affirmative answers have chosen different bit locations. Then it is easy to see that the number of 1s in the bitwise XOR of all users' bit strings is the same as that of the affirmative users. In practice, different users may have collisions, i.e. choosing the same bit location. This would cause the output of our counting protocol to be smaller than the actual number. Therefore, the probability of our counting protocol being accurate equals the probability that the optimistic case happens in a counting process or the "non-collision probability".

Proposition 4. *The probability of our pseudo-counting protocol being accurate in a counting process of n users is greater than or equal to $\frac{q(q-1)\dots(q-n+1)}{q^n}$.*

Proof: Denote by P_{opt} the probability of our protocol being accurate. P_{opt}'s lower bound can be computed by considering an extreme case where n users' answers are all "affirmative". (The more users with affirmative answers there are, the smaller the non-collision probability is.)

It is easy to see the non-collision probability equals $q(q-1)\dots(q-n+1)/q^n$ when all n users have affirmative answers. Let us imagine the n users with affirmative answers choose bit location one after another. Each user has q possible choices, and thus there are q^n different outcomes for n users' choices. However, to avoid collisions with the previous users, the second user has only $q-1$ choices, the third user has only $q-2$ choices, ... , the last user has only $q-n+1$ choices, which means there are only $q(q-1)\dots(q-n+1)$ possible non-collision outcomes.Thus

$$P_{opt} \geq \frac{q(q-1)\dots(q-n+1)}{q^n} \tag{7}$$

□

Proposition 5. *The probability of our pseudo-counting protocol being accurate in a counting process of n users is around $\frac{q(q-1)\dots(q-\lceil n/2\rceil+1)}{q^{\lceil n/2\rceil}}$ in the average case.*

Proof: In an average case, users' answers are uniformly random. Thus, the average total number of users with affirmative answers is around $\lceil n/2\rceil$. Denote by P_{opt}^{avg} the probability of our protocol being accurate in the average case. Similar to the analysis in Proposition 4's proof, we know:

$$P_{opt}^{avg} \approx \frac{q(q-1)\dots(q-\lceil n/2\rceil+1)}{q^{\lceil n/2\rceil}} \tag{8}$$

□

To improve the accuracy, we have two possible approaches: 1) We can use a larger value for q, so that there is a lower probability for two users' chosen bits to collide. 2) We can repeat the counting process for a number of times (denote by p the number of times the counting process is repeated). Then, we can choose the largest output among all repetitions as the final output.

Specifically, the probability for an optimistic case to happen in p times of counting process can be computed as:

$$\begin{aligned} P'_{opt}(p) &= 1-(1-P_{opt})^p \\ &\geq 1-\left(1-\tfrac{q(q-1)\dots(q-n+1)}{q^n}\right)^p \end{aligned} \tag{9}$$

$$\begin{aligned} P_{opt}^{avg\prime}(p) &= 1-(1-P_{opt}^{avg})^p \\ &\approx 1-\left(1-\tfrac{q(q-1)\dots(q-\lceil n/2\rceil+1)}{q^{\lceil n/2\rceil}}\right)^p \end{aligned} \tag{10}$$

Table 1 lists the theoretical estimations of probability for a non-collision case to happen, computed using Formula 10 with different q and different p in a 100-user scenario in average case.

We formally present our protocol in Algorithm 2.

Table 1
Theoretical estimation probability for a non-collision case to happen in a 100-user scenario in average case.

q	1000	2000	3000	4000	5000
$p=1$	28.77%	53.92%	66.33%	73.53%	78.21%
$p=2$	49.27%	78.77%	88.66%	92.99%	95.25%
$p=3$	63.86%	90.22%	96.18%	98.14%	98.96%
$p=4$	74.26%	95.49%	98.71%	99.51%	99.77%
$p=5$	81.67%	97.92%	99.57%	99.87%	99.95%
$p=6$	86.94%	99.04%	99.85%	99.97%	99.99%

Algorithm 2 The Secure Pseudo-counting Protocol

```
Require:
    A group of $n$ users;
    An aggregator;
    User $i$ ($i = 1, \dots, n$) has two secret seeds $S_a^i$ and $S_b^i$;
    In each time period, user $i$ ($i = 1, \dots, n$)'s reply is either affirmative or negative;
    In each time period, a public known nonce number $t \in [0, 2^f - 1]$;
    Two precision controlling numbers $p, q \in \mathbb{N}$.
Ensure:
    The aggregator outputs $tot \in \mathbb{N}$, the approximate total number of affirmative users;
1: the aggregator sets $tot$ to 0;
2: for $j = 1, \dots, p$ do
3:     user $i$ ($i = 1, \dots, n$) computes $k^i = h_{S_a^i, f+\lceil \log_2 p \rceil, q}(t|j) \oplus h_{S_b^i, f+\lceil \log_2 p \rceil, q}(t|j)$;
4:     user $i$ ($i = 1, \dots, n$) encodes its answer by a $q$-bit string $d^i$ according to Formula 6. If user $i$'s status is negative, $d^i$ equals $\{0\}^q$; otherwise, the user randomly choose a bit in $d^i$, sets the chosen bit to 1 and other bits to 0.
5:     user $i$ ($i = 1, \dots, n$) computes $\overline{d^i} = d^i \oplus k^i$, and sends $\overline{d^i}$ to the aggregator.
6:     the aggregator computes the bitwise XOR of all $\overline{d^i}$ and finds out $d$, the total number of 1s in $\overline{d^i}$.
7:     the aggregator sets $tot$ to Max$\{tot, d\}$.
8: end for
9: return $tot$ as approximate total number of affirmative users;
```

5.2 Privacy-preserving k-th Min computation protocol

With a pseudo counting protocol, we construct our privacy-preserving k-th Min computation protocol as follows.

Our protocol determines every bit of the k-th minimum value from the MSB to the LSB. The process follows a similar "report-determine-broadcast-compare" pattern as our Min computation protocol.

In particular, the aggregator and all users first run the secure pseudo-counting protocol to find out how many users have a number whose MSB is 0. Denote by tot the total number of affirmative users. If tot is greater than or equal to k, the aggregator knows the k-th minimum value is also the k-th minimum value in all affirmative users' numbers and its MSB is 0. Otherwise, the aggregator knows the k-th minimum value is also the $(k - tot)$-th minimum value in all negative users' numbers and its MSB is 1. To determine the second-MSB, the aggregator only needs to repeat the above counting process among the users who have the same MSB as the k-th minimum value's MSB. To implement this selective counting, the aggregator broadcasts the k-th minimum value's MSB to all users, and the users whose MSB is different would always report negative in the remaining counting process. Similarly, the aggregator can determine the third, the fourth, ..., the LSB of the k-th minimum value.

We summarize our protocol in Algorithm 3.

Algorithm 3 Privacy-preserving k-th Min Computation Protocol

```
Require:
    A group of $n$ users;
    An aggregator;
    User $i$ ($i = 1, \dots, n$) has two secret seeds $S_a^i$ and $S_b^i$;
    In each time period, user $i$ ($i = 1, \dots, n$) has a number $d^i \in [0, 2^l - 1]$;
    In each time period, a public known nonce number $t \in [0, 2^l - 1]$;
    A preset number $K \in \mathbb{N}$.
Ensure:
    The aggregator outputs $d'$, the $k$-th minimum number in $\{d^i\}_{i=1,\dots,n}$;
1: the aggregator sets $f$ to 0.
2: every user sets its status as "effective".
3: for $j = 1, \dots, l$ do
4:     user $i$ ($i = 1, \dots, n$) sets its reply according to its status and its $j$-th MSB: If its status is "effective" and the bit equals 0, it sets its reply to affirmative; otherwise, it sets its reply to negative.
5:     user $i$ ($i = 1, \dots, n$) helps the aggregator to compute $tot$, the total number of affirmative users, by participating in the secure pseudo-counting protocol;
6:     If $f + tot < k$, the aggregator updates $f$'s value to $f + tot$, sets the $d'$'s $j$-th MSB to 1, and broadcasts 1 to every user; otherwise, the aggregator sets the $d'$'s $j$-th MSB to 0 and broadcasts 0.
7:     If an "effective" user finds the bit received different from its number's $j$-th MSB, it sets its status to "ineffective".
8: end for
9: return the $k$-th minimum number $d'$ as $\Sigma_{j=1}^{l} d'_j \times 2^{l-j}$;
```

5.3 Security Analysis

Here we analyze the security of our k-th Min computation protocol. Define $pcd(k, d^1, \ldots, d^n)$ a function that takes k and n users' numbers as inputs, outputs $\{pc_j\}_{j\in\{1,\ldots,l\}}$ where pc_j equals the count of users whose number has the same j-bit binary prefix as the k-th Min. For example, suppose $l = 3$ and the k-th Min is 100, then pc_1, pc_2, pc_3 equals the count of users whose number is of form $1 * *$, $1\ 0\ *$ and $1\ 0\ 0$ respectively. Since $\{pc_j\}_{j=\{1,\ldots,l\}}$ is actually a distribution of all users' number compared with the k-th Min's prefix, we call $pcd(k, d^1, \ldots, d^n)$'s output the k-th Min's *"prefix-count-distribution"*.

Theorem 6. *Our k-th Min computation protocol is perfectly privacy-preserving against all users and weakly privacy-preserving in the sense that all users learn no more knowledge from it than k-th Min of all users' data, and the aggregator learns no more knowledge than the output of our k-th Min protocol as well as the its prefix-count-distribution.*

Proof: Similar as our Min computation protocol, it is straightforward to see our protocol reveals every bit of the protocol's output to each user only, thus our protocol reveals no extra knowledge to the users.

It is not difficult to see the $\{pc_j\}$ equals the count of effective users in round j of step 3. Using this information, the aggregator could easily simulate all users' ciphertexts in the j-th round by first generating a random q-bit string s that has pc_j bits of 1 and $q - pc_j$ bits of 0, and then generating n random q-bit strings the bitwise XOR of which is s.

Same as our proof of Theorem 3, the computational indistinguishability here follows from the pseudo-randomness of the pseudo-random functions that we use to generate keys and the cipher's homomorphic property on bitwise exclusively-OR computations. □

Remark: Please note that although our k-th Min protocol reveals the k-th Min's prefix-count-distribution, it does not cause significant violation to individual user's privacy since it is a piece of statistic information about all users' numbers. In addition, in cases that users are not entitled to know the k-th Min, we can conclude our k-th Min protocol is weakly privacy-preserving against the users in the sense that it reveals the k-th Min to all users.

5.4 Optimal Choice of (q, p)

Recall that two parameters q (the bit string's length) and p (the number of times of repeating) control our pseudo-counting protocol's accuracy, and thus the k-th Min protocol's accuracy. To guarantee the protocol's accuracy is no less than a particular threshold, we can simply choose a large q and a large p. But since large p or large q would decrease the protocol's efficiency, we are interested in finding the optimal (q, p) pair. In this section, we analyze how to find the optimal (q, p) pair for the pseudo-counting protocol.

In the pseudo-counting protocol, the aggregator needs to receive all users' bit strings and performs bitwise XOR computations on them. Compared with the workload of a user, the aggregator's workload is generally much heavier especially when the total number of users is large. Therefore, here we study how to optimize the workload of the aggregator to improve the protocol's efficiency. In particular, we study how to find the optimal (q, p) pair that minimizes the total bits sent to the aggregator, and guarantees the accuracy is no less than the threshold.

Let $b^\star$ be the threshold and let a and b be the non-collision probability lower bounds for running the pseudo-counting protocol once and p times respectively in a n-user counting process. According to formula (7) and (9), we have:

$$a = \frac{q(q-1)\ldots(q-n+1)}{q^n} \tag{11}$$

$$b = 1 - (1-a)^p. \tag{12}$$

Let $Z(q, p)$ be the total bits sent to the aggregator when every user's answer is a q-bit string and the pseudo-counting protocol is repeated for p times. In every time, the aggregator receives n q-bit strings from all users. Therefore,

$$Z(q, p) = nqp, \tag{13}$$

and our goal is to compute $(q^\star, p^\star)$, the solution of the following problem:

$$\begin{aligned} &\textbf{argmin: } Z(q,p) \\ &\textbf{subject to: } b \geq b^\star \end{aligned} \tag{14}$$

According to equation (12), Z can be represented as a function of q as:

$$\begin{aligned} Z(q,p) &= n \ln \tfrac{1}{1-b} \times \tfrac{q}{\ln \frac{1}{1-a}} \\ &= n \ln \tfrac{1}{1-b} \times \tfrac{q}{n \ln q - \ln[q^n - q(q-1)\ldots(q-n+1)]} \end{aligned} \tag{15}$$

The optimal $q^\star$ that minimizes Z could only be an integer near the solution of equation: $\frac{dZ}{dq} = 0$, which is equivalent to

$$\frac{d\left(\frac{q}{n \ln q - \ln[q^n - q(q-1)\ldots(q-n+1)]}\right)}{dq} = 0. \tag{16}$$

Consequently, we have proved the following proposition.

Proposition 7. *Suppose that $\bar{q}$ is the solution to equation (16). Then either $q^\star = \lfloor \bar{q} \rfloor$ or $q^\star = \lceil \bar{q} \rceil$.*

Although equation (16) specifies the optimal value of q, the equation is so complicated that getting an analytic solution would be hard. In practice, we could use some numerical methods to find the optimal (q, p) pair. For example, we can enumerate the possible candidates of p and q, and then use the pair that has the smallest product of p and q in all enumerated pairs as the final $(q^\star, p^\star)$. (Enumeration of possible values is feasible because p and q must be integers located in a certain range.)

Specifically, given any (q, p) pair, we can compute b, the corresponding lower bound of the non-collision probability, using formula (11) and (12). It is easy to see b is an increasing function of p, and also an increasing function of q. Therefore, for any q, there is a minimal p that makes b no less than the threshold $b^\star$. Denote by p_{min} this minimal p and it can be computed as:

$$p_{min} = \max\{\lceil \ln(1-b^\star)/\ln(1-a)\rceil, 1\} \qquad (17)$$

Apparently, for any q, p_{min} computed as above is the optimal value of p that minimizes the product of p and q and satisfies the probability threshold requirement. By enumerating every possible q and its corresponding p_{min}, we traverse every possible candidate of the optimal (q, p) pair.

Note that the enumeration does not need to traverse all possible values of q. Since a is an increasing function of q, we know p_{min} is a non-increasing function of q. Also, we can prove there is q_{max} that is finite, and its corresponding p_{min} is 1. Due to the non-increasing property of p_{min}, the corresponding p_{min} of any q that is greater than q_{max} is 1. (Recall $q \geq 1$.) Therefore, q_{max} and its corresponding p_{min} dominate any q and this q's corresponding p_{min}, when q is greater than q_{max}. The enumeration can be terminated when q reaches q_{max}.

Below, we provide a possible value of q_{max} to prove its existence:

$$q_{max} = \lceil \frac{n-1}{1-(b^\star)^{\frac{1}{n}}} \rceil. \qquad (18)$$

It is easy to verify the corresponding b for $(q_{max}, 1)$ is no less than $b^\star$.

6 Performance Evaluation

In this section, we conduct theoretical analysis and perform experiments to evaluate the accuracy and efficiency of our protocols. In the aspect of accuracy, we consider two metrics—the probabilities of our protocols being accurate, and the relative errors.

In all our experiments, our protocols are implemented using Microsoft Visual Studio 2012 and the Crypto++ library [25]. The experiments are performed on a laptop running the 64-bit Windows 7 Professional operating system with Intel Core i7 3520M CPU and 8 GB memory. Results shown in Figure 2 and Figure 5 are the average of 10000 runs. Other experimental results shown are the average of 1000 runs.

The hash function we use in our Min protocol is HMAC<SHA-1> which can produce a 160-bit hash value as 160-bit is enough in our Min protocol. And HMAC<SHA-512> is used in our secure counting protocol and k-th Min protocol. In particular, HMAC<SHA-512> generates a 512-bit output. In case we need a shorter output of length q, we truncate the output to short bit strings of length q, and then use the bitwise XOR of all these strings as the final output. In case q is greater than 512, we first break the input message into several 512 bit strings and one string of length q' ($q' < 512$), then generate several 512-bit output strings and one q'-bit output string, and finally use the concatenation of these output strings as the final output.

We use the privacy-preserving Min computation protocol from [8] as the baseline and compare our protocols with it. Note that the protocol in [8] is designed for computing the Min. However, it can also be used to find the k-th Min, since the aggregator knows the entire distribution of all users' data from it.

6.1 Communication Cost of Our Protocols

Table 2 shows the total bits sent and received by the aggregator and a user in three protocols. Also, the round complexity of three procotols is shown in it.

Table 2
Communication Cost of Our Protocols (the range of data is $[0, M-1]$, n is the total number of users)

	bits sent/received by the aggregator	bits sent/received by a user	round complexity
Baseline	$0/nM\lceil\log_2 n\rceil$	$M\lceil\log_2 n\rceil/0$	1
Min Protocol	$n\lceil\log_2 M\rceil/nq\lceil\log_2 M\rceil$	$q\lceil\log_2 M\rceil/\lceil\log_2 M\rceil$	$\lceil\log_2 M\rceil$
k-th Min Protocol	$pn\lceil\log_2 M\rceil/pnq\lceil\log_2 M\rceil$	$pq\lceil\log_2 M\rceil/p\lceil\log_2 M\rceil$	$p\lceil\log_2 M\rceil$

According to Proposition 2, $l/2^q$ is the upper bound of our Min protocol's error rate ($l = \lceil\log_2 M\rceil$). It is easy to see that when l is not too small, for example greater than 20, by simply setting $q = l$ our Min protocol would achieve a very good error rate bound (less than 0.0001%). Our Min protocol requires much less data to send/receive compared with the baseline protocol, as long as n is not too much greater than M (i.e. $n = O(M)$).

Notice that the accuracy bound of the pseudo-counting protocol on which our k-th Min protocol is based is determined by p, q and n. Compared with the baseline protocol, our k-th Min protocol requires less data to send and receive, typically when the system has a large M and a relatively small n. For example, when $M = 2^{20}-1$ and $n = 100$, experiments show our k-th Min protocol achieves an accuracy that is above 99.5% by setting $p = 10$ and $q = 1400$. (Please see Figure 4 in the next Section for more details.) It is easy to verify our k-th Min protocol requires much fewer bits to be sent and received by both the aggregator and the users in this setting.

Although the amount of data to be sent and received in either protocol of ours is quite less than that in baseline, it is worth noting that the baseline

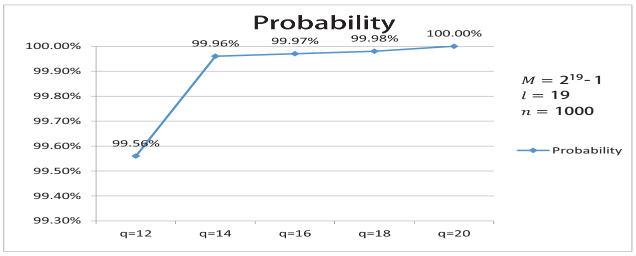


Figure 2. Probability of Min Protocol Being Accurate

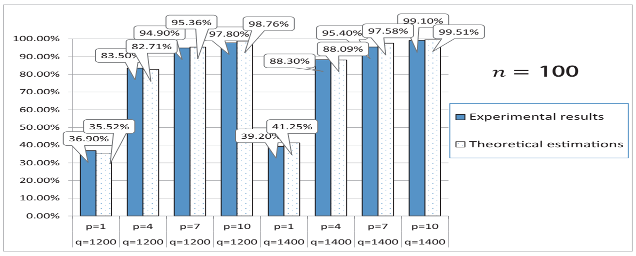


Figure 3. Probability of Pseudo Counting Protocol Being Accurate (Also Called Non-Collision Probability)

protocol has a promising advantage in communication: the baseline protocol only needs one round unidirectional communication (ORUC). Besides the total amount of data that a user needs to send or receive, the round complexity also impacts the amount of time that a user needs to keep being online. Therefore, the baseline protocol suits cases that the network connection is not stable, while our protocol performs well in cases that stable network connections are present.

6.2 Experimental results on probability of being accurate

The accuracy of our privacy-preserving Min computation protocol is closely related to parameters q and l.

In this set of experiments, we set the number of users to 1000, and consider six different lengths of data: $l = 2$, 5, 10, 15, 17, and 19. For all data lengths tested, our protocol is accurate with a probability that is more than 99.9% when $q \geq 14$. Figure 2 shows the probabilities of being accurate for the largest l ($l = 19$). We can see that the probability of being accurate is very high when $q = 20$, which tallies with our theoretical analysis in the previous section.

In addition, we test the probability of our pseudo counting protocol being accurate for a variety of values of p and q. In this set of experiments, we set the number of users to 100 and a user's answer uniformly at random from affirmative and negative. Meanwhile, we present the theoretical estimations of probability for our pseudo counting protocol being accurate in the average case, computed based on Formulas 8 and 10 here. The results are shown in Figure 3.

Also, we fix the number of users as 100 and measure the probability of the k-th Min protocol being accurate. For simplicity, we set l to 20. The results are shown in Figure 4. We can see that, with reasonably large p and q, the probability is pretty high. For example, with $p = 10$ and $q = 1200$, the probability is 99.00%. (We will see in Section 6.4 that the corresponding efficiency is also good.)

6.3 Experimental results on relative error

We are also interested in their relative errors. For our privacy-preserving Min protocol, we measure its relative error for different values of q. Figure 5 shows a curve of the relative error in a set of experiments with 1000 users and $l = 19$. Clearly, the error shrinks quickly when q grows. In this set of experiments, the relative error drops to 0.0003% when $q = 18$.

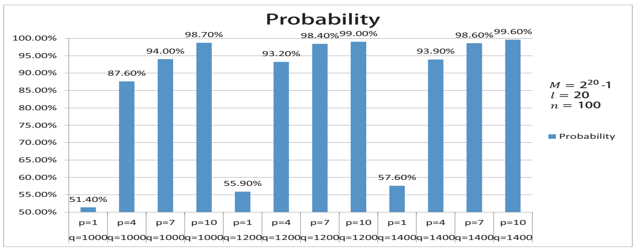


Figure 4. Probability of k-th Min Protocol Being Accurate

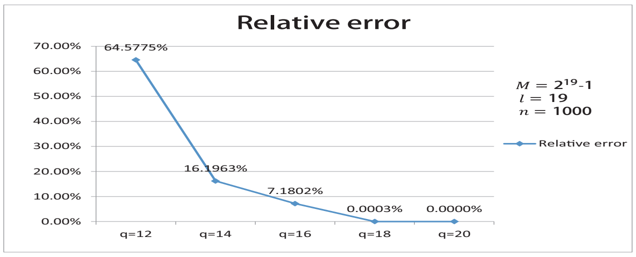


Figure 5. Relative Error of Min Protocol

We also measure the relative error of the k-th Min protocol. In this set of experiments, we set the data length l to 20, and the number of users to 100. The results are shown in Figure 6. We can see that, without reasonably large p and q, the error is very small. For example, with $p = 10$ and $q = 1200$, the relative error is 0.03%. (Again, we will see in Section 6.4 that the corresponding efficiency is also good.)

6.4 Experimental results on efficiency

To see the efficiency of our protocols, we test their computation time. Here the computation time includes the encryption time for each user, and the decryption time for the aggregator. Note that here (and the following) decryption is the decryption of

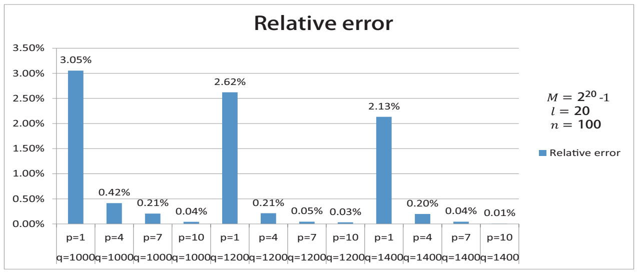


Figure 6. Relative Error of k-th Min Protocol

the bitwise XOR of all users' plaintexts. Also, all operations that encryptions/decryptions need are included in our efficiency experiments, such as the hash operations, comparison operations and bitwise XOR operations.

Table 3
Efficiency of Min Protocol

		$l=20$	$l=25$	$l=30$	$l=32$	$l=34$	$l=36$	$l=38$	$l=40$
Enc.	baseline	$2.5ms$	$33.2ms$	$1.2s$	$4.1s$	$10.4s$	$59.9s$	$282.3s$	$1476.3s$
	ours	$64.4\mu s$	$81.2\mu s$	$96.6\mu s$	$103.0\mu s$	$109.8\mu s$	$117.8\mu s$	$123.3\mu s$	$132.2\mu s$
Dec.	baseline	$33.4ms$	$750.0ms$	$32.2s$	$119.7s$	$328.4s$	$2315.9s$	$> 2500s$	$> 2500s$
	ours	$9.9\mu s$	$12.2\mu s$	$14.0\mu s$	$14.7\mu s$	$15.6\mu s$	$18.8\mu s$	$18.9\mu s$	$19.7\mu s$

The results on the Min protocol are shown in Table 3. In this set of experiments, we fix the number of users to 1000 and let the value of l vary to see how the computation time of the Min protocol changes. We can see that our Min protocol's computation time increases slowly when l grows. When l grows to 40, the encryption time is only 132.2 microseconds and the decryption time is only 19.7 microseconds. In contrast, the baseline protocol's computation time grows very fast. When l reaches 40, the baseline protocol's computation time becomes very long (1476.3 seconds for encryption, and over 2500 seconds for decryption).

Table 4
Efficiency of k-th Min Protocol

		$l=15$	$l=20$	$l=22$	$l=24$	$l=26$	$l=28$
Enc.	baseline	$21.2ms$	$960.5ms$	$1.9s$	$9.8s$	$38.3s$	$187.2s$
	ours	$3.3ms$	$4.4ms$	$4.9ms$	$5.2ms$	$5.7ms$	$6.0ms$
Dec.	baseline	$285.5ms$	$17.2s$	$37.4s$	$216.3s$	$916.7s$	$> 1000s$
	ours	$6.3ms$	$8.3ms$	$9.2ms$	$9.9ms$	$10.8ms$	$11.4ms$

The results on the k-th Min protocol are shown in Table 4. In this set of experiments, we fix the number of users to 100 and $p = 10$, $q = 1400$. When $l = 28$, the baseline protocol's computation time is already very long. It needs 187.2 seconds for encryption and more than 1000 seconds for decryption. However, our k-th Min protocol is still very fast. The encryption/decryption time is only $6.0/11.4$ milliseconds.

7 Discussion

In this section, we discuss some potential enhancements of our protocols.

7.1 Dealing with collusion attack

In some cases, the aggregator may be able to collude with a few users in the system. Since the secret that generates a user's key is shared with two other users, this user's data privacy can be easily comprised when the two other users who share the secret happen to be the colluding ones. To deal with such collusion attacks, we present an enhanced keying system which is more secure compared with the basic one.

Specifically, the authority first picks $s_{i,j} \in \{0,1\}^\gamma$ $(i,j = 1,\ldots,n)$ uniformly and independently, where n is the number of users. For each user i $(i = 1,\ldots,n)$, the authority sends $s_{i,1}, s_{i,2}, \ldots, s_{i,n}$ and $s_{1,i}, s_{2,i}, \ldots, s_{n,i}$ to it. And then for each data with the nonce information t, user i computes its secret key using

$$k_i = k_i^r \oplus k_i^c$$

where

$$k_i^r = h_{s_{i,1},f,l}(t) \oplus h_{s_{i,2},f,l}(t) \oplus \ldots \oplus h_{s_{i,n},f,l}(t)$$

$$k_i^c = h_{s_{1,i},f,l}(t) \oplus h_{s_{2,i},f,l}(t) \oplus \ldots \oplus h_{s_{2,i},f,l}(t)$$

The encryption and decryption operations are the same as the cipher presented in Section 3.2. Note that here the decryption operation is the decryption of the bitwise XOR of all users' plaintexts. For a bit-string $x \in \{0,1\}^l$, user i encrypts it by computing

$$\overline{x} = x \oplus k_i$$

As for decryption, the bitwise XOR of all users' ciphertexts equals that of all users' plaintexts, since the bitwise XOR of all users' secret keys equals 0.

In this key generation method, user i's secret key is calculated by $s_{i,1}, s_{i,2}, \ldots, s_{i,n}$ and $s_{1,i}, s_{2,i}, \ldots, s_{n,i}$. It's easy to see that only if the aggregator is in collusion with all remaining $n-1$ users can he recover the user i's key and compute its plaintexts. Therefore the collusion attack can be thwarted by this keying system. Meanwhile, we note that the encryption cost is increased accordingly due to the cost of improved security.

7.2 Dealing with offline users

In practice, some users may not be able to provide the sensed value for various reasons (e.g. battery is dead, connection is lost, etc.) during the protocol's process. (We regard such a user to be offline, either intendedly or unintendedly.) In this case, to acquire the correct Min or k-th Min value of the remaining users' data, the protocol has to be restarted by the remaining online users. A straightforward solution would be letting the remaining online users establish a new set of keys, and restart our protocols using the new keys. However, this could be time-consuming, especially when users go offline frequently. Below we provide a method which avoids re-establishing keys every time a user goes offline. It only requires the trusted authority's help once.

The main idea is to set the offline user's sense data as the maximum value $2^l - 1$, so that its data do not impact the result since the Min or k-th Min value is to be computed. If a user goes offline, the aggregator can request the help of the trusted authority. The trusted authority can "simulate" the offline user's behavior (with $2^l - 1$ as its data) in the protocol using its keys and the correct nonce information. Notice that if a user's data is $2^l - 1$, its answers in all l rounds are always "negative" regardless of the meta-result returned by the aggregator. Thus the trusted authority can compute all responses before the protocol is restarted, and send them to the aggregator at one time. Using the responses, the aggregator can complete the protocol with other remaining online users correctly.

7.3 Keeping the minimum value secret from the users

Both protocols presented in this paper allow users to know the output of protocols. There might be some cases in which users are restricted from knowing the minimum/k-th minimum value.

Recall that both our Min protocol and k-th Min protocol consists of l rounds of "report and determine" steps. Starting from the second round, each user needs to determine its private input in the j-th round ($j = 2, \dots, l$) based on the MSB, the 2nd-MSB, ..., and the $(j-1)$-th-MSB that are received from the aggregator in previous rounds. To keep our protocols functioning and meanwhile hide these bits of the final outputs, we could utilize the well-known oblivious transfer protocols [26], [27]. A 1-out-of-N oblivious transfer protocol (e.g. [28]) allows the sender with N private messages $M_1, M_2, \dots, M_N$ to transmit M_σ to the receiver as requested by the receiver, and guarantees that the sender does not know the value of σ and the receiver learns no more than M_σ. We can let each user and the aggregator run one 1-out-of-2^{j-1} oblivious transfer protocol in the j-th round to make sure the aggregator receives the correct data (and the correct data only) and the user does not know the bit values. In more details, below we explain how to apply the above technique by taking the interactions between the aggregator and the user i in the j-th round as an example.

Denote by D_j the j-th-MSB of the protocol's output ($j = 1, \dots, l$), and by $r^i_j(x_1, \dots, x_{j-1})$ the function that returns user i's private input in the j-th round when the MSB, ..., and the $(j-1)$-th-MSB of the protocol's output equal $x_1, \dots, x_{j-1}$ respectively ($x_1, \dots, x_{j-1} \in \{0, 1\}$). Denote by $OT^N_1(M_1, \dots, M_N; \sigma)$ the 1-out-of-N oblivious transfer protocol with $M_1, \dots, M_N$ and σ as the sender's private input and the receiver's private input respectively. Specifically, in the beginning of round j, user i computes $M_x = r^i_j(x_1, \dots, x_{j-1})$ where $\Sigma^{j-1}_{k=1} x_k \times 2^{j-1-k} + 1 = x$ for $x = 1, \dots, 2^{j-1}$ as its answer in the Algorithm 1 or Algorithm 3, and compute $\overline{M_x}$ by encrypting M_x same as user i does in the Algorithm 1 or by processing M_x as user i does in Algorithm 2 respectively. After this, user i uses $\{\overline{M_x}\}_{x=1,\dots,2^{j-1}}$ as its private inputs of the oblivious transfer protocol. At the same time, the aggregator computes $\sigma = \Sigma^{j-1}_{k=1} D_k \times 2^{j-1-k} + 1$ as its private input. Next, the aggregator and user i jointly run $OT^{2^{j-1}}_1(\{\overline{M_x}\}_{x=1,\dots,2^{j-1}}; \sigma)$ to let the aggregator acquire the correct report generated based on $r^i_j(D_1, \dots, D_{j-1})$ without revealing $D_1, \dots, D_{j-1}$ to user i. A flow chart is shown in Figure 7.

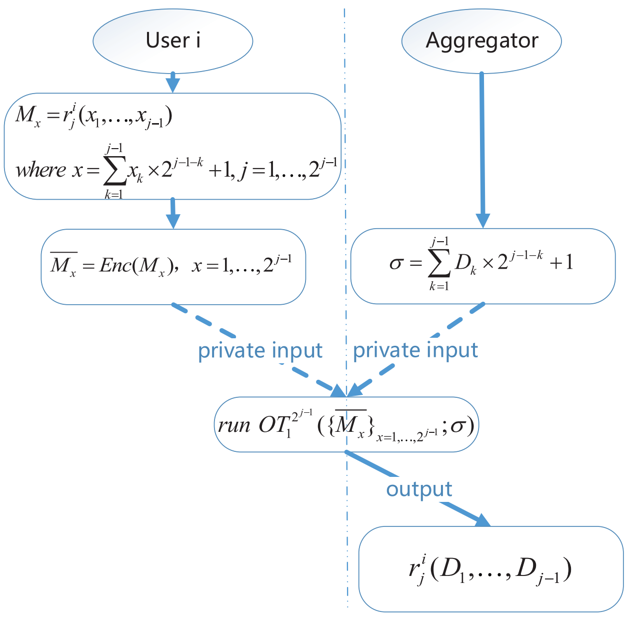

User i
Aggregator
$M_x = r^i_j(x_1,\dots,x_{j-1})$
where $x = \sum_{k=1}^{j-1} x_k \times 2^{j-1-k} + 1, j = 1,\dots,2^{j-1}$
$\overline{M_x} = Enc(M_x),\ x = 1,\dots,2^{j-1}$
$\sigma = \sum_{k=1}^{j-1} D_k \times 2^{j-1-k} + 1$
private input
private input
run $OT_1^{2^{j-1}}(\{\overline{M_x}\}_{x=1,\dots,2^{j-1}}; \sigma)$
output
$r^i_j(D_1,\dots,D_{j-1})$

Figure 7. The aggregator and the user i apply OT protocols in the j-th round.

8 Conclusion

In this paper, we study how a data aggregator in a mobile phone sensing scenario can efficiently compute the minimum value or the k-th minimum value in all mobile phone users' private data. Using standard definitions and paradigms in cryptography, we formally prove our protocols are secure and thus are able to protect all users' private data. Compared with existing protocols that are based on arithmetic sum computation, our protocols are based on bitwise XOR computation and thus are more efficient.

References

[1] R. Herring, A. Hofleitner, D. Work, O. Tossavainen, and A. Bayen, *Mobile Millennium-Participatory Traffic Estimation Using Mobile Phones*, 2009.

[2] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, “Vtrack: accurate, energy-aware road traffic delay estimation using mobile phones,” in *SenSys*, D. E. Culler, J. Liu, and M. Welsh, Eds. ACM, 2009, pp. 85–98.

[3] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma, “Prism: platform for remote sensing using smartphones,” in *MobiSys*, S. Banerjee, S. Keshav, and A. Wolman, Eds. ACM, 2010, pp. 63–76.

[4] R. Rana, C. Chou, S. Kanhere, N. Bulusu, and W. Hu, “Ear-phone: an end-to-end participatory urban noise mapping system,” in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*. ACM, 2010, pp. 105–116.

[5] X. Bao and R. R. Choudhury, “Movi: mobile phone based video highlights via collaborative sensing,” in *MobiSys*, S. Banerjee, S. Keshav, and A. Wolman, Eds. ACM, 2010, pp. 357–370.

[6] R. Johnson and P. Kuby, *Elementary statistics*. Cengage Learning, 2007.

[7] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, “Prisense: Privacy-preserving data aggregation in people-centric urban sensing systems,” in *INFOCOM*. IEEE, 2010, pp. 758–766.

[8] Q. Li and G. Cao, “Efficient and privacy-preserving data aggregation in mobile sensing,” in *ICNP*. IEEE, 2012, pp. 1–10.

[9] Q. Li, G. Cao, and T. F. L. Porta, “Efficient and privacy-aware data aggregation in mobile sensing,” *IEEE Trans. Dependable Sec. Comput.*, vol. 11, no. 2, pp. 115–129, 2014.

[10] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, “Efficient and provably secure aggregation of encrypted data in wireless sensor networks,” *ACM Trans. Sen. Netw.*, pp. 1–36, 2009.

[11] V. Rastogi and S. Nath, “Differentially private aggregation of distributed time-series with transformation and encryption,” in *SIGMOD Conference*, A. K. Elmagarmid and D. Agrawal, Eds. ACM, 2010, pp. 735–746.

[12] G. Ács and C. Castelluccia, “I have a dream! (differentially private smart metering),” in *Information Hiding*, ser. Lecture Notes in Computer Science, T. Filler, T. Pevný, S. Craver, and A. D. Ker, Eds., vol. 6958. Springer, 2011, pp. 118–132.

[13] E. G. Rieffel, J. T. Biehl, W. van Melle, and A. J. Lee, “Secured histories: computing group statistics on encrypted data while preserving individual privacy,” *CoRR*, vol. abs/1012.2152, 2010.

[14] E. Shi, T.-H. H. Chan, E. G. Rieffel, R. Chow, and D. Song, “Privacy-preserving aggregation of time-series data,” in *NDSS*. The Internet Society, 2011.

[15] T.-H. H. Chan, E. Shi, and D. Song, “Privacy-preserving stream aggregation with fault tolerance,” in *Financial Cryptography*, ser. Lecture Notes in Computer Science, A. D. Keromytis, Ed., vol. 7397. Springer, 2012, pp. 200–214.

[16] M. M. Groat, W. He, and S. Forrest, “Kipda: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks,” in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 2024–2032.

[17] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1621–1631, 2012.

[18] Y. Yang, X. Wang, S. Zhu, and G. Cao, “Sdap: a secure hop-by-hop data aggregation protocol for sensor networks,” in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2006, pp. 356–367.

[19] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. F. Abdelzaher, “Pda: Privacy-preserving data aggregation in wireless sensor networks,” in *INFOCOM*. IEEE, 2007, pp. 2045–2053.

[20] C. Wang, G. Wang, W. Zhang, and T. Feng, “Reconciling privacy preservation and intrusion detection in sensory data aggregation,” in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 336–340.

[21] B. K. Samanthula, W. Jiang, and S. Madria, “A probabilistic encryption based MIN/MAX computation in wireless sensor networks,” in *2013 IEEE 14th International Conference on Mobile Data Management, Milan, Italy, June 3-6, 2013 - Volume 1*, 2013, pp. 77–86. [Online]. Available: http://dx.doi.org/10.1109/MDM.2013.18

[22] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order-preserving encryption for numeric data,” in *SIGMOD Conference*, G. Weikum, A. C. König, and S. Deßloch, Eds. ACM, 2004, pp. 563–574.

[23] A. Boldyreva, N. Chenette, Y. Lee, and A. O’Neill, “Order-preserving symmetric encryption,” in *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, 2009, pp. 224–241.

[24] O. Goldreich, *Foundations of cryptography: Basic applications*. Cambridge Univ Press, 2004, vol. 2.

[25] W. Dai. (2010) Crypto++ library. [Online]. Available: http://www.cryptopp.com

[26] M. O. Rabin, “How to exchange secrets with oblivious transfer,” 1981.

[27] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” in *Advances in CryptologyCRYPTO89 Proceedings*. Springer, 1990, pp. 547–557.

[28] M. Naor and B. Pinkas, “Oblivious transfer and polynomial evaluation,” in *Proceedings of the thirty-first annual ACM symposium on Theory of computing*. ACM, 1999, pp. 245–254.

[29] S. Banerjee, S. Keshav, and A. Wolman, Eds., *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys 2010), San Francisco, California, USA, June 15-18, 2010*. ACM, 2010.

Yuan Zhang received his BS (2005) in Automation from Tianjin University, MS (2009) in Software Engineering from Tsinghua University, and PhD (2013) in Computer Science from State University of New York at Buffalo. He is interested in security, privacy, and economic incentives.

Qingjun Chen received his BS (2013) in computer science from Nanjing University. He is currently working toward the MS degree with the department of computer science and technology, Nanjing University. He is interested in security, privacy, and economic incentives.

Sheng Zhong received his BS (1996), MS (1999) from Nanjing University, and PhD (2004) from Yale University, all in computer science. He is interested in security, privacy, and economic incentives.