Privacy Preserving Data Aggregating with Multiple Access Channel

Hongyi Yao and Tracey Ho
California Institute of Technology

Abstract—We consider the scenario in which a set of users want to compute an aggregate function of their messages at a message center. The users communicate with the message center over a multiple access channel with fading, where the fading states of the channels from individual receivers are unknown a priori to the message center. For privacy reasons, the users do not want disclose their message information to the message center. No computational limitations on the message center are assumed, and the message center may collude with a set of hidden eavesdroppers to retrieve the message information of the users. This paper proposes a scheme called *MacPDA* that leverages the multiple access properties of wireless signals to achieve privacy. It relies on fairly loose synchronization and does not require secret channels. MacPDA is shown to reveal no message information of the users other than the required function value. The estimation performance of MacPDA is investigated with numerical experiments, and theoretical bounds are given on the asymptotic performance.

I. Introduction

We consider a communication system consisting of multiple users, each with a private message, and a single message center at which a given aggregate function of the messages is to be computed. Except for the computed function value, the users wish to reveal no additional information about their messages. The users communicate with the message center over a multiple access channel with fading. We consider an information theoretic privacy model which assumes no computational limitations on the message center. Moreover, the message center may collude with a set of hidden eavesdroppers to try to retrieve the message information of the users.

Privacy preserving data aggregation (or privacy preserving computation) is a basis for applications such as privacy preserving machine learning e.g. [9], privacy preserving outsourcing e.g. [10], and privacy preserving data mining e.g. [11], [1], [16]. For instance, in the scenario of privacy preserving traffic monitoring [8], the traffic control center needs to know the distribution of vehicle positions, but each individual vehicle does not want to disclose its location.

The setting of information theoretic privacy preserving data aggregating (or secure multiparty computation) was first investigated by Yao [17] for two user case, and was later generalized to multiple users [12], [6], [5]. These works provide generic secure protocols by representing the desired function as an equivalent combinatorial circuit, and using secret pairwise channels between each pair of users. The complexity of the generic protocols depends on the size of the combinatorial circuit representing the function [4]. However, in many practical applications, the complexity of the generic protocol is prohibitive, or it may not be feasible to realize pairwise secret channels among users. To achieve more efficient protocols, other works exploit specific structure of the data set (e.g. [16], [11], [10]), use random perturbations to preserve privacy at the expense of some degradation in estimation accuracy (e.g. [1]), or consider cryptographic settings with computationally bounded adversarial behavior (e.g. [11], [10]).

This paper considers the information theoretic problem formulation, and shows that the multiple access property of wireless signals can be used instead of pairwise secret channels for privacy preserving data aggregating. We propose a scheme called "MacPDA" that uses this approach to realize privacy preserving data aggregation over multiple access channel. Only loose synchronization is needed between the users and the message center. For the data aggregating function considered in this paper, MacPDA is shown theoretically to reveal no message information of the users other than the required function value. The estimation performance of MacPDA is investigated with numerical experiments, and theoretical bounds are given on the asymptotic performance.

A related line of work considers energy-efficient computation of functions over multiple access channels [14] without privacy considerations, where for the Gaussian multiple access channel, lattice codes were proposed to

efficiently compute linear functions. In [7], besides end to end communication, multiple access computation was used to additionally deliver secret information from the source to the relay node. To the best of our knowledge, this is the first paper that considers privacy preserving data aggregating in the setting of physical-layer multiple access channel.

A. *Organization of the paper*

The rest of this paper is organized as follows. Section II formulates the problem. In Section III, we provide the general framework of MacPDA. The security is proved in Section IV. In Section V, we consider a concrete MacPDA scheme and analyze its estimation performance. In Section VI, we conclude the paper.

II. PROBLEM FORMULATIONS

A. *Privacy preserving data aggregation model*

A data aggregation model with n clients $\mathcal{V} = \{V_1, V_2, ..., V_n\}$ and a single message center S is considered. Each client node has a private message $W_i \in \mathcal{Q} = \{1, 2, ..., q\}$. We use $\mathcal{W}$ to denote the collection of user messages, that is

$$\mathcal{W} = (W_1, W_2, ..., W_n).$$

The message center S needs to compute a data aggregation function $f(.)$ that defined as follows:

$$f(\mathcal{W}) = (F_1, F_2, \ldots, F_q),$$

where $\forall j \in \{1, 2, \ldots, q\}$

$$F_j = |\{i : W_i = j, i = 1, 2, \ldots, n\}|.$$

We assume that the message center S does not know the number of users n *a priori*. For brevity, in the following we use $\mathcal{F}$ to denote $(F_1, F_2, \ldots, F_q)$. Besides the output of the aggregation function, the users do not want to disclose their message information at the message center. We note that such aggregation function f is not restrictive. Any symmetric function (e.g., summation, maximum, majority etc.) of $\{W_1, W_2, ..., W_n\}$ can be computed from $\mathcal{F}$.

B. *Channel model*

A physical layer multiple access channel is assumed from the users to the message center. Due to users' mobility or environment changing, the channel condition varies with time. In particular, we assume that the message center has no *a priori* knowledge about the channel impulse responses from the users, and its prior distribution is independent and identical channel fading

for the channel impulse response from each user to the message center. We do not rely on any assumptions on channel coherence time.

We also consider hidden eavesdroppers that may collude with the message center to try to obtain information about the users' messages. Similarly, the eavesdroppers have no *a priori* knowledge about the channel impulse responses from the users, and assume independent and identical channel fading for the channel impulse response from each user to each eavesdropper.

III. THE FRAMEWORK OF MACPDA

A. *The chip-book of MacPDA*

The message center divides its available time and frequency resources into chips. Each user can transmit signals in one or more chips, and the message center can detect whether a chip carries some signal (from one or more users). The message center divides the chips into q disjoint sets $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_q$ of K chips each. Two examples are shown in Figure 1.

B. *User's transmitter*

We consider the transmitter construction for a user V_i.

- Assume $W_i = j$, and $\mathcal{S}_j$ is the set of all subsets of $\mathcal{P}_j$. Thus, $\mathcal{S}_j$ has cardinality 2^K. Let $\mathcal{D}_j$ be a distribution over $\mathcal{S}_j$ which is known by each party.
- User V_i independently and randomly chooses an element in $\mathcal{S}_j$ according to distribution $\mathcal{D}_j$.
- Assume $\mathcal{C}_i$ is the element chosen by user V_i. User V_i transmits a signal on such chip in $\mathcal{C}_i$.

Note that the distribution $\mathcal{D}_j$ is independent of user index i, which is necessary for the security of MacPDA.

C. *Message center's estimator*

The message center estimates the data aggregation function $f(\mathcal{W}) = (F_1, F_2, ..., F_q)$ as follows. Upon receiving the signals from the users, for each chip, the message center detects whether or not it carries some signal (from one or more users). Let $\mathcal{N}_j$ be the indexes of detected chips in part $\mathcal{P}_j$ for each $j \in \{1, 2, ..., q\}$.

For each j in $\{1, 2, ..., q\}$, the message center defines estimator Ψ_j from $\{0, 1\}^K$ to $\{0, 1, \ldots, n\}$, and estimates F_j by

$$\hat{F}_j = \Psi_j(\mathcal{N}_j).$$

In Section IV, we prove the information security of MacPDA schemes that satisfy the framework presented in this section. In Section V, we study a concrete MacPDA scheme. In particular, we define the codeword
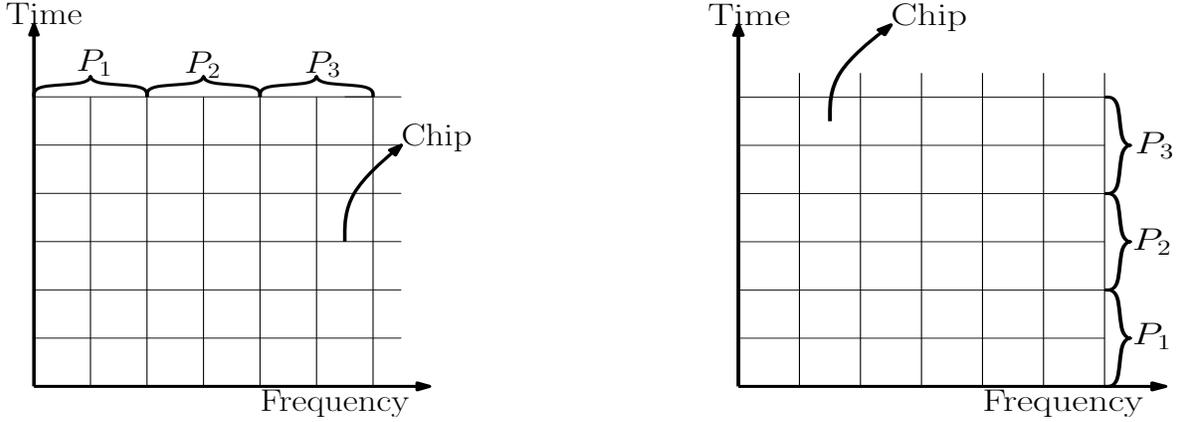
Fig. 1. Two constructions of chip-books.

distributions $\{\mathcal{D}_j, j = 1, 2, ..., q\}$ and the message center's estimators $\{\Psi_j, j = 1, 2, ..., q\}$, and analyze the performance of this MacPDA scheme.

We assume loose synchronization allowing the users and the message center to identify chips belonging to each partition. The message center uses basic energy detection technology to detect whether a chip has been selected by one or more users. Thus, the message center cannot find out the exact number of users that selected that chip. In fact, the message center can apply more advanced signal detection technologies to estimate the number of users that transmitted on the same chip. This is part of our ongoing further work.

IV. SECURITY ANALYSIS

Let $\mathcal{E}$ be the signals that have been received by the message center and the hidden eavesdroppers. The security of MacPDA is proved by the following theorem.

Theorem 1. *Apart from $\mathcal{F}$, the message center and the hidden eavesdroppers cannot retrieve any information about user messages $\mathcal{W}$. That is,*

$$I\left(\mathcal{W}; \mathcal{E}|\mathcal{F}\right) = 0. \tag{1}$$

Proof: Recall that $\mathcal{S}_j$ is the set of all subsets of $\mathcal{P}_j$ and $\mathcal{S}_j$ has cardinality 2^K. We assume an arbitrary partial order on $\overset{q}{\underset{j=1}{\cup}} \mathcal{S}_j$. Let $\mathcal{B}$ be a set defined by $\{b_1, b_2, ..., b_{q2^K}\}$, such that b_i is the number of users that selected the i'th element of $\overset{q}{\underset{j=1}{\cup}} \mathcal{S}_j$. Let $\mathcal{I} = \{I_1, I_2, ..., I_{q2^K}\}$ be the index information from $\mathcal{B}$ to the users. That is, I_i is a subset in $\mathcal{V}$ and consists of the users that selected the i'th subset of $\overset{q}{\underset{j=1}{\cup}} \mathcal{S}_j$.

Since each user independently chooses the chip in the corresponding part with the same distribution, condition-ing on $\mathcal{F}$ there is no other information about $\mathcal{W}$ that can be provided by $\mathcal{B}$. Thus, we have

$$I\left(\mathcal{W}; \mathcal{B}|\mathcal{F}\right) = 0. \tag{2}$$

Since $\mathcal{W}$ can be determined by $(\mathcal{B}, \mathcal{I})$, we have

$$I\left(\mathcal{W}; \mathcal{E}|\mathcal{B}, \mathcal{I}\right) = 0. \tag{3}$$

Note that $\mathcal{E}$ is a function of $(\mathcal{B}, \mathcal{I})$ and channel randomness[1]. Since the channel randomness from each user to each eavesdropper (and the message center) is i.i.d. distributed, we have

$$I\left(\mathcal{I}; \mathcal{E}|\mathcal{B}\right) = 0. \tag{4}$$

Then we have

$$\begin{aligned}
I\left(\mathcal{W}; \mathcal{E}|\mathcal{F}\right) &\leq I\left(\mathcal{W}; \mathcal{B}, \mathcal{E}|\mathcal{F}\right) \\
&= I\left(\mathcal{W}; \mathcal{B}|\mathcal{F}\right) + I\left(\mathcal{W}; \mathcal{E}|\mathcal{B}, \mathcal{F}\right) \\
&= I\left(\mathcal{W}; \mathcal{E}|\mathcal{B}, \mathcal{F}\right) \tag{5} \\
&= I\left(\mathcal{W}; \mathcal{E}|\mathcal{B}\right) \tag{6} \\
&\leq I\left(\mathcal{W}, \mathcal{I}; \mathcal{E}|\mathcal{B}\right) \\
&= I\left(\mathcal{I}; \mathcal{E}|\mathcal{B}\right) + I\left(\mathcal{W}; \mathcal{E}|\mathcal{B}, \mathcal{I}\right) \\
&= 0, \tag{7}
\end{aligned}$$

where (5) is due to (2), (6) is because that $\mathcal{F}$ is a function of $\mathcal{B}$, and (7) is due to (4) and (3). It completes the proof of the theorem. ∎

V. ESTIMATION PERFORMANCE OF MACPDA

In this section, we consider a concrete realization of codeword distributions $\{\mathcal{D}_j, j = 1, 2, ..., q\}$ and the message center's estimators $\{\Psi_j, j = 1, 2, ..., q\}$.

---

[1]Here, we assume the "channel randomness" includes the random-ness from the channel and user's transmit hardware.

- **Definition of $\mathcal{D}_j$.**
- Let z be an positive integer. The distribution $\mathcal{D}_j$ is defined such that each user with message j chooses exactly z chips in $\mathcal{P}_j$ with uniform probability over all subsets of $\mathcal{P}_j$ that have cardinality z. We assume that F_j is bounded by n_m, and $n_m \cdot z < K$.

Due to the existence of channel noise and channel fading, we assume that for each chip that carries the signal from one or more users, the missed detection probability at the message center is p_m; for other unchosen chips, the false detection probability at the message center is p_f. We assume both p_m and p_f are strictly less than $1/2$. Then the estimator Ψ_j is constructed as follows.

- **Definition of Ψ_j.**
- Let N_j be the number of detected chips in $\mathcal{P}_j$, *i.e.*, the cardinality of $\mathcal{N}_j$. The message center first estimates the number of chosen chips, U_j, in $\mathcal{P}_j$. The message center estimates U_j by

$$\hat{U}_j = \min(\max(\frac{N_j - K \cdot p_f}{1 - p_f - p_m}, 0), n_m \cdot z). \quad (8)$$

Note that since $0 \leq U_j \leq F_j \cdot z \leq n_m \cdot z$, the 'min' and 'max' operations would not increase the gap between U_j and $\hat{U}_j$.

- The message center estimates F_j by

$$\hat{F}_j = \log_{(1-z/K)}(1 - \hat{U}_j/K). \quad (9)$$

We first provide the intuition behind this choice of estimator. When there are U_j chosen chips in $\mathcal{P}_j$, due to the false detections and missed detections, the expected number of detected chips at the message center is

$$E(N_j|U_j) = U_j(1 - p_m) + (K - U_j)p_f.$$

Thus we estimate U_j by Equation (8).

Since each active user independently chooses z chips uniformly at random, this corresponds to a "balls and bins" problem. Thus, we can apply Cardenas' formula [3] to show that if there are F_j users having message j, the expected number of U_j is

$$E(U_j|F_j) = K(1 - (1 - z/K)^{F_j}).$$

Thus, F_j is estimated by Equation (9).

In practice, the message center can use a lookup-table to map N_j to the corresponding estimation value $\hat{F}_j$. For each $j = 1, 2, ..., q$, there are K possible values of N_j, and each value of N_j independently decides the estimation value $\hat{F}_j$. Thus, there are K table mappings for estimating each F_j, and in total qK table mappings for such MacPDA scheme. Note that since the message center does not know the user number n *a priori*, it cannot just estimate $\hat{F}_1, \ldots, \hat{F}_{q-1}$ and compute $\hat{F}_q$ as $n - \sum_{j=1}^{q-1} \hat{F}_j$.

A. Asymptotic performance guarantee

We have the following theorem that guarantees the asymptotic performance of this MacPDA scheme.

Theorem 2. *Let $\lambda = 1/(1 - p_m - p_f)$ and $\beta = z(1 - n_m \cdot z/K)$. Then for any $\delta > 0$ we have*

$$\Pr(|\hat{F}_j - F_j| > \delta\sqrt{F_j})$$
$$\leq 4exp(-\frac{\beta^2\delta^2}{2(\lambda+1)^2z}) + 2exp(-\frac{\beta^2\delta^2 F_j}{2(\lambda+1)^2K}). \quad (10)$$

Proof: For the U_j chosen chips, the expected number of detected chips is $U_j(1-p_m)$. Let N'_j be the actual number of the detected chips from these U_j chosen chips. Using the Chernoff Bound [13], we have

$$\Pr(|N'_j - U_j(1 - p_m)| < \frac{\beta\delta\sqrt{F_j}}{2(\lambda+1)})$$
$$\leq 2exp(-\frac{\beta^2\delta^2 F_j}{2(\lambda+1)^2U_j}).$$

Since $U_j \leq z \cdot F_j$, we have

$$\Pr(|N'_j - U_j(1 - p_m)| < \frac{\beta\delta\sqrt{F_j}}{2(\lambda+1)})$$
$$\leq 2exp(-\frac{\beta^2\delta^2}{2(\lambda+1)^2z}). \quad (11)$$

Similarly, for the $K - U_j$ unchosen chips, the expected number of detected chips is $(K - U_j)p_f$. Let N''_j be the actual number of the detected chips from those $K - U_j$ unchosen chips. Using the Chernoff Bound, we have

$$\Pr(|N''_j - (K - U_j) \cdot p_f| < \frac{\beta\delta\sqrt{F_j}}{2(\lambda+1)})$$
$$\leq 2exp(-\frac{\beta^2\delta^2 F_j}{2(\lambda+1)^2(K - U_j)})$$
$$\leq 2exp(-\frac{\beta^2\delta^2 F_j}{2(\lambda+1)^2K}). \quad (12)$$

Since $N_j = N'_j + N''_j$, we have

$$|N_j - U_j(1 - p_m) - (K - U_j)p_f| > \frac{\beta\delta\sqrt{F_j}}{\lambda+1}$$

only if either

$$|N'_j - U_j(1 - p_m)| > \frac{\beta\delta\sqrt{F_j}}{2(\lambda+1)}$$

or

$$|N_j'' - (K - U_j) \cdot p_f| > \frac{\beta \delta \sqrt{F_j}}{2(\lambda + 1)}.$$

Using the union bound [13] on Inequalities (11) and (12), we have

$$\Pr(|N_j - U_j(1 - p_m) - (K - U_j)p_f| > \frac{\beta \delta \sqrt{F_j}}{\lambda + 1})$$
$$\leq 2exp(-\frac{\beta^2 \delta^2}{2(\lambda + 1)^2 z}) + 2exp(-\frac{\beta^2 \delta^2 F_j}{2(\lambda + 1)^2 K}). \quad (13)$$

When we use Equation (8) to estimate U_j, we have

$$|U_j - \hat{U}_j|$$
$$\leq \lambda |N_j - U_j(1 - p_m) - (K - U_j)p_f|.$$

Thus, by Inequality (13), we have

$$\Pr(|U_j - \hat{U}_j| > \frac{\lambda \beta \delta \sqrt{F_j}}{\lambda + 1})$$
$$\leq 2exp(-\frac{\beta^2 \delta^2}{2(\lambda + 1)^2 z}) + 2exp(-\frac{\beta^2 \delta^2 F_j}{2(\lambda + 1)^2 K}). \quad (14)$$

Using Azuma's Inequality [2], [15], we have[2]

$$\Pr(|U_j - E(U_j|F_j)| > \frac{\beta \delta \sqrt{F_j}}{1 + \lambda})$$
$$\leq 2exp(-\frac{\beta^2 \delta^2 F_j}{2(1 + \lambda)^2 z \cdot F_j})$$
$$= 2exp(-\frac{\beta^2 \delta^2}{2z(1 + \lambda)^2}). \quad (15)$$

Thus, using triangle inequality, we have

$$|\hat{U}_j - E(U_j|F_j)| > \beta \delta \sqrt{F_j}$$

only if either

$$|U_j - \hat{U}_j| > \frac{\lambda \beta \delta \sqrt{F_j}}{\lambda + 1}$$

or

$$|U_j - E(U_j|F_j)| > \frac{\beta \delta \sqrt{F_j}}{1 + \lambda}.$$

Using the union bound on Inequalities (14) and (15), we have

$$\Pr(|\hat{U}_j - E(U_j|F_j)| > \beta \delta \sqrt{F_j})$$
$$\leq 4exp(-\frac{\beta^2 \delta^2}{2(\lambda + 1)^2 z}) + 2exp(-\frac{\beta^2 \delta^2 F_j}{2(\lambda + 1)^2 K}). \quad (16)$$

Recall that $\hat{F}_j$ is estimated from $\hat{U}_j$ by Equation (9).

---

[2]The work [15] uses Azuma's Inequality to get a similar inequality for the case $z = 1$. The result here is a generalization of [15].

Define function

$$y(x) = \log_{(1-z/K)}(1 - x/K).$$

We compute the derivative of $y(x)$ as

$$y'(x) = -\frac{1}{1 - x/K} \cdot \frac{1}{K \ln(1 - z/K)}$$

and $y'(x) > 0$ when $x < K$ and $z < K$. Since $\ln(1 - z/K) \leq -z/K$, we have

$$|y'(x)| \leq \frac{1}{1 - x/K} \cdot \frac{1}{z}.$$

Since $F_j = y(E(U_j|F_j))$, we have

$$|F_j - \hat{F}_j| = |y(E(U_j|F_j)) - y(\hat{U}_j)|$$
$$\leq y_m'|E(U_j|F_j) - \hat{U}_j|,$$

where

$$y_m' = \max_{x \in [\min(U_j, E(U_j|F_j)), \max(U_j, E(U_j|F_j))]} |y'(x)|.$$

Since both U_j and $E(U_j|F_j)$ are between 0 and $n_m \cdot z$, we have $y_m' \leq 1/\beta$. Thus we have

$$|F_j - \hat{F}_j| \leq |E(U_j|F_j) - \hat{U}_j|/\beta.$$

Combining this with Inequality (16), we complete the proof of the theorem. ∎

We present a simplified version of Theorem 2 as follows.

Corollary 3. *When $p_m + p_f < 1/2$ and $n_m \cdot z < K/2$, we have*

$$\Pr(|\hat{F}_j - F_j| > \delta \sqrt{F_j})$$
$$\leq 4exp(-\frac{z\delta^2}{72}) + 2exp(-\frac{z^2 \delta^2 F_j}{72K}). \quad (17)$$

B. Numerical analysis

Theorem 2 proves the asymptotic performance guarantee of the proposed MacPDA scheme. In this subsection, we analyze its performance by numerical experiments. Without loss of generality, we consider the estimations of F_1 over independent rounds. For each round, F_1 is randomly chosen from $\{35, 36, ..., 80\}$ with uniform probability, and p_m and P_f are both set to be 0.02. Figure 2, Figure 3 and Figure 4 show the estimation errors for $K = 100$, $K = 200$ and $K = 300$ for 20 independent rounds. The dash line stands for the setting of $z = 1$, and the solid line stands for the setting of $z = 3$. Figure 5 summarizes the estimation bias and mean-square errors over 20000 independent rounds, with the same parameter settings. From the numerical results,
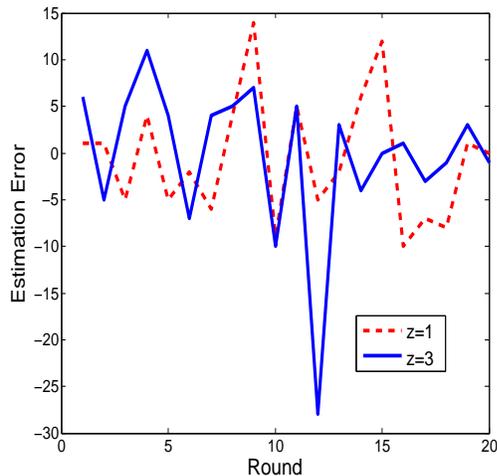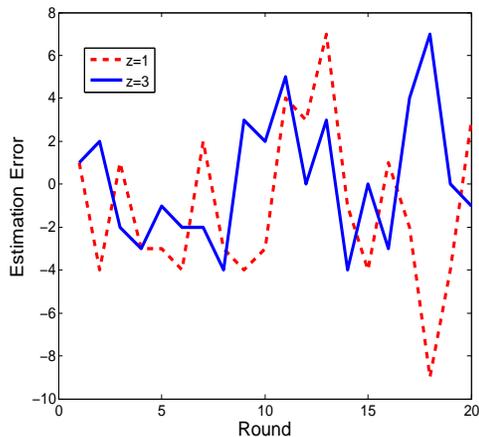
Fig. 2. The estimation error when $K = 100$.

Fig. 4. The estimation error when $K = 300$.
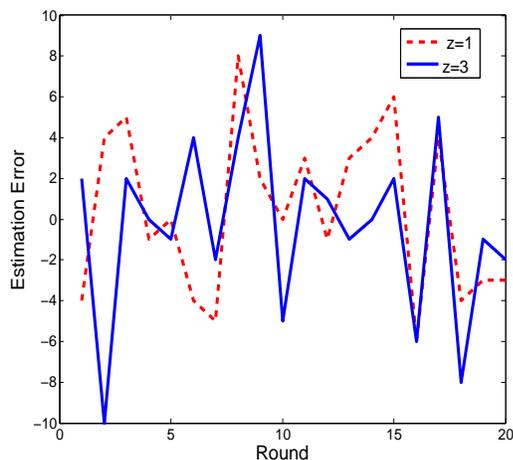
Fig. 3. The estimation error when $K = 200$.

Term	Estimation Bias			Mean Square Error		
K	100	200	300	100	200	300
$z = 1$	-1.6	-0.15	-0.10	31	18	16
$z = 3$	0.33	-0.11	-0.07	57	17	10

Fig. 5. Summation of the numerical experiment for $z = 1$ and $z = 3$.

we can see that the more bandwidth resources (*i.e.*, K), the better estimation performance. For small K, say $K = 100$, z should be small; and when K is large, say $K = 300$, z should be large too.

VI. Conclusion

In this paper we consider privacy preserving data aggregation over multiple access channel. We assume the message center has unlimited computational ability and may collude with a set of hidden eavesdroppers to obtain information about users' messages. In this setting, we propose a scheme named MacPDA, that leverages the multiple access property of wireless signals to achieve privacy preserving data aggregation. The estimation performance and the security of MacPDA are analyzed theoretically and with numerical experiments. In particular, for the data aggregation function considered, MacPDA achieves perfect privacy in terms of leaking zero message information other than function output.

VII. Acknowledgement

References

[1] R. Agrawal and R. Srikant. Privacy-preserving data mining. In *Proc. of ACM SIGMOD Conference*, 2000.

[2] K. Azuma. Weighted sums of certain dependent random variables. *Tôhoku Math*, 19:357–367, 1967.

[3] A. F. Cardenas. Analysis and performance of inverted data base structures. *Commun. ACM*, 1975.

[4] D. Catalano, R. Cramer, I. Damgard, G. D. Crescenzo, D. Pointcheval, and T. Takagi. *Contemporary Cryptology*. Part of Springer Science+Business Media, 2005.

[5] D. Chaum, C. Crepeau, and I. Damgard. Multiparty unconditionally secure protocols. In *Proc. of STOC*, 1988.

[6] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game - a completeness theorem for protocols with honest majority. In *Proc. of STOC*, 1987.

[7] C. K. Ho, K. T. Gowda, and S. Sun. A generalized two-way relay channel with private information for the relay. In *Proc. of IEEE ICC*, 2009.

[8] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J. C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson. Virtual trip lines for distributed privacy-preserving traffic monitoring. In *Proc. of MobiSys*, 2008.

[9] M. Kantarcioglu and J. Vaidya. Privacy preserving naive bayes classier for horizontally partitioned data. In *Proc. of IEEE Workshop on Privacy Preserving Data Min ing*, 2003.

[10] P. Lin and K. S. Candan. Hiding traversal of tree structured data from untrusted data stores. In *Proc. of the 2nd Inernational Workshop on Security In Informtion Systems*, 2004.

[11] Y. Lindell and B. Pinkas. Privacy preserving data mining. In *Proc. of CPYPTO*, 2000.

[12] S. Goldwasser M. Ben-Or and A. Wigderson. Completeness theorems for non cryptographic fault tolerant distributed computation. In *Proc. of STOC*, 1988.

[13] M. Mitzenmacher and E. Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

[14] B. Nazer and M. Gastpar. Computation over multiple-access channels. *IEEE Transactions on Information Theory, Special Issue on Models, Theory, and Codes for Relaying and Cooperation in Communication Networks*, 2007.

[15] M. R. Salavatipour. Azuma's inequality. Technical report, Available at: webdocs.cs.ualberta.ca/ m-reza/courses/Random05/notes/lecture7.ps.

[16] P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. In *Proc. of IEEE Symp. on Security and Privacy*, 1998.

[17] A. C. Yao. How to generate and exchange secrets. In *Proc. of FOCS*, 1986.