World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924

AN OPTIMAL CHANNEL PREDICTION OF PSEASMC MODEL

***[1]S. Samson Dinakaran and [2]Dr. M. Devapriya**

[1]Assistant Professor/Department of CSVLB Janakiammal College of Arts & Science, Coimbatore, Tamil Nadu, India.

[2]Assistant Professor/Department of CS Government Arts College, Coimbatore, Tamil Nadu, India.

Article Received on 09/08/2019 **Article Revised on 30/08/2019** **Article Accepted on 20/09/2019**

***Corresponding Author**
S. Samson Dinakaran
Assistant Professor/ Department of CSVLB Janakiammal College of Arts & Science, Coimbatore, Tamil Nadu, India.

ABSTRACT

In the previous researches, Sublinear communication and Quantum protocol in Performance and Security Enhanced Asynchronous Secure Multiparty Computation (SQPSEASMC) model has been designed to reduce both storage and communication costs. In this model, the upper bounds of multiparty quantum channels were represented in terms of multiparty squashed entanglement and derived on the rates at which GHz channels or multiparty secret channels which can be distributed among a number of parties over an arbitrary quantum broadcast network. On the other hand, the open issue was that whether bounds can also be obtained for a network of multiple access channels which were normally noisy non-local gates. For this reason, an aggregating quantum repeater was presented that derives the upper bound to restrict the quantum and secret abilities over the network. Still, the open issue is that whether the optimality of the aggregated quantum repeaters satisfies the relationship between the quantum channels and the number of links between Alice and Bob in deriving entanglement. Hence in this paper, Sublinear communication and Quantum protocol with Channel Prediction in Performance and Security Enhanced ASMC (SQPSECP-ASMC) is proposed. In this model, the optimality of aggregated quantum repeaters is achieved by using a supervised rank aggregation method that predicts the unconnected links in a SMC networks. At first, different topological measures are used to rank a list of unlinked nodes in a network at a given time. After that, the new links at a consecutive time interval is predicted based on the weighted value of each topological

measure. Further, the supervised rank aggregation model for link prediction is built by using these learned weights. Finally, the experimental results show that the proposed SQPSECP-ASMC model achieves better performance than the SQPSEASMC in terms of differential privacy, latency and accuracy.

KEYWORDS: Secure multiparty computation, SQPSEASMC, Link prediction, Aggregated quantum repeaters, Supervised rank aggregation.

I. INTRODUCTION

Typically, Secure Multiparty Computation (SMC) or Multi-Party Computation (MPC) is a kind of cryptography with the aim of developing techniques for parties in order to jointly measure the function over their inputs when preserving those inputs. Though it prevents the party's confidentiality from each other, it cannot be used efficiently in most of the real-time applications. Consider a set of parties who want to correctly decide few general functions of their local inputs when preserving their local information as private as possible, however who do not confidence each other, not the channels by which they communicate. This is the very common security issue in SMC i.e., it can be utilized for resolving many real-time challenges like distributed selection, privacy request, signature distribution or decryption functions, etc. Regrettably, solving SMC without further considerations is very expensive in terms of number of payloads to be sent, number of redundancy and number of synchronous rounds.

To tackle these problems, TrustedPals,[1] model has been developed which is a smart card-based security structure that facilitates more important solutions to the SMC challenges. This model has a distributed system in which functions were locally employed with tamper-proof security elements. In traditional methods, the functions were executed as a Java desktop application and the security components were predicted by Java Card Technology enabled smart cards, tamper-proof Subscriber Identity Modules (SIM) similar to those utilized on smart phones or memory devices with integral tamper-proof processing elements. In this framework, the function F is embedded as a Java function and is shared within the networks in an initial phase. After that, the functions provide their input value to their security element and the model obtains the secure allocation of the input values. At last, all security elements decide the function and return the result to their function. The network security elements initiate private and authentic channels between each other and acts as a secure transfer within the distribution phase.

Consequently, this model tolerates the avoidance of safety issues in SMC to a problem of fault-tolerant synchronization. As well, the decrement from security to fault-tolerance offers a novel set of authentication requests concerning a combination of a fault-tolerant algorithm into secure systems. This provides this framework vulnerable to the rapid changes in the network delay and so this is not perfect for network execution. Cortinas et al.[2] explored how to make Trusted Pals applicable in a network configuration with less synchrony. Also, they proved how to solve the Asynchronous version of SMC (ASMC) using asynchronous synchronization algorithms motivated by the current outcomes in fault-tolerant distributed computing. They used an asynchronous consensus algorithm and encapsulate timing hypotheses within a device known as a failure detector.[3] However, it generates fixed size messages in fixed time intervals. Therefore, the size of the payload field was required to choose for finding an acceptable tradeoff between security and performance such that a message size offers better security in cost of worse performance.

To overcome such issue, Performance Enhanced ASMC (PEASMC) and Security Enhanced ASMC (SEASMC) were proposed to quantitatively measure the performance and security by improving the set of metrics. As well, Performance and Security Enhanced ASMC (PSEASMC) was proposed,[4] to compute the best tradeoff by reducing the tradeoff objective function which has both performance and security metrics together instead of automatically switching from one security configuration to another until the required tradeoff was achieved. According to this model, an acceptable tradeoff between security and performance is achieved based on the chosen payload size efficiently. On the other hand, the consensus in this model was not solved due to high storage and communication efforts. Also, the bit complexity of the payload was high due to utilization of unbounded buffers. As a result, Sublinear communication and Quantum protocol in PSEASMC (SQPSEASMC) was proposed,[5] in which One-Time Truth Table (OTTT) protocol was used for enabling several parties to commonly assess N-party functionality by sharing between Alice and Bob. The secret sharing was depending on the oblivious transmit of a bit-string message from Alice to Bob. The hash functions were used for authenticating whether Bob receives the message or not. Based on this protocol, both capacity and communication complexities were reduced with high security level against malicious adversaries. In this multi-party quantum channels, the upper bounds were derived on the rates at which GHz states or multi-party private states which can be shared among a number of different parties over an arbitrary quantum broadcast network. The upper bounds were represented in terms of multi-party squashed entanglement.

However, the problem was that whether bounds can also be obtained for a network of multiple access channels. Also, the multiple access channels were noisy non-local gates.[6] So, aggregating quantum repeaters were presented to derive the upper bound that restricts the quantum capacity and the private capacity over the network.[7] The quantum network is composed of a wide range of stretchable quantum channels such as erasure channels, dephasing channels, bosonic quantum amplifier channels and optical lossy channels in the asymptotic limit; however, may not be in general. But, it is more vital fact that the optimality of the aggregated quantum repeater protocol is currently related to the basic questions on whether the given quantum channels satisfy the fundamental relations between Alice and Bob for the secret-key distillation or not.

Hence in this article, a supervised rank aggregation method is proposed to predict the links in SMC networks and enhance the optimality of aggregated quantum repeaters. Initially, a list of unlinked nodes in a network at a given time is ranked based on different topological measures i.e., quantum communication capacity, assortativity (it indicates how much nodes tend to link to other nodes with similar degree and it is measured by degree-degree correlation) and centrality measures (it quantifies the significance of a node relative lively behaves for all nodes). Each topological measure must rank a truly occurring link on the top positions. Then, each topological measure is weighted based on its performances in predicting the new links at consecutive time intervals. These learned weights are used to have a supervised rank aggregation model for predicting new links. Therefore, it provides a better prediction of relationship between quantum channels and links between Alice and Bob.

The rest of the paper is organized as follows: Section II presents the previous researches on aggregation method for SMC/MPC. Section III explains the methodology of proposed model. Section IV illustrates the experimental results compared with the existing models and Section V concludes the entire discussion.

II. LITERATURE SURVEY

Pathak et al.[8] proposed the multiparty differential privacy through aggregation of locally trained classifiers. In this method, a privacy-preserving protocol was proposed for making a differentially private aggregate classifier using classifiers trained locally by separate mutually untrusting parties. These parties were allowed to interact with an untrusted curator for constructing additive shares of a perturbed aggregate classifier. However, the computation cost was high and also the classifier performance was not effective.

Goryczka et al.[9] proposed a secure multiparty aggregation with differential privacy. In this method, the security was guaranteed by SMC protocols using Shamir's secret sharing, perturbation-based and different encryption schemes. Differential privacy of the final result was achieved by Distributed Laplace Perturbation (DLPA) mechanism. To satisfy the differential privacy, partial random noise was generated by all parties such that the aggregated noise follows Laplace distribution. However, the computation overhead was high that limits the scalability.

Jung et al.[10] proposed the privacy-preserving data aggregation without secure channel by introducing novel secure product and sum computation protocol. This method was considered how an external aggregator or multiple parties can learn few algebraic statistics over parties privately owned data when preserving the data confidentiality. Also, considered that all channels were subjected to the eavesdropping attacks and all the communications via the aggregation were open to others. However, the information leakage during computation and communication was high.

Tian et al.[11] proposed an aggregation of private sparse learning models using MPC. In this approach, the problem of privately learning a sparse model was considered across multiple sensitive datasets. Also, learning individual models were proposed and privately aggregated by using SMC. However, this model has limitations on analyzing accuracy loss and amount of data leaked by the aggregated model.

Bonawitz et al.[12] proposed a practical secure aggregation for privacy-preserving machine learning. In this approach, MPC was controlled to compute total of model parameter that updates from individual parties components in a secure way. The server has two responsibilities such as it routes payloads between the other parties and computes the final outcome. Nevertheless, the communication cost was not reduced efficiently.

Bindschaedler et al.[13] considered the privacy preserving aggregation in constrained scenarios where inter-participant communication was not realistically possible. Shamir secret sharing was employed within a star network to provide the collusion resistance and fault tolerance. Also, different protocols were developed to add noise to the computed aggregate function, thereby ensuring differential privacy for the participants. However, the communication cost was depending on the security parameters.

Long et al.[14] proposed a framework for distributed and secure machine learning among untrusted individuals. This framework has two phases such as a two-step training protocol based on homomorphic addition and a zero knowledge proof for data authentication. By combining these two techniques, privacy of per-user data was provided and a malicious user was prevented. However, the authentication time per user was high.

III. Proposed Methodology

In this section, the proposed methodology is explained in brief. Consider $\mathcal{G} = \langle \mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_n \rangle$ is a temporal sequence of an initial graph. The entire sequence is split into three segments such as training, labeling and testing or validation. Three graphs such as $\mathcal{G}_{learn}, \mathcal{G}_{label}$ and $\mathcal{G}_{test}$ are generated by making union of the temporal sequences of the graphs for three corresponding time slots. The training data is built as follows:

An example can be generated for each couple of repeaters (x, y) that are not linked in $\mathcal{G}_{label}$; however both belonging to the same linked component. The class labeling is obtained by verifying whether the couple of repeaters are indeed connected in $\mathcal{G}_{label}$. If such a link exists, then it will be a positive example in the supervised learning process and if no link exists, then it will be a negative example. Therefore, examples are generated from these graphs for both training and testing. Also, these examples are characterized by a given number of topological attributes such as average number of times quantum channel is used, average of all degree (income and outcome) of nodes in the channel and distance between two nodes.

Each attribute of an example has the capacity for providing some unique information about the data while considered individually. The training examples are ranked based on the attribute values. Therefore, for each attribute, a ranked list of all examples is obtained. Considering only the top K ranked examples and with a hypothesis that when the examples are ranked according to their attribute values, the positive examples must be ranked on the top and the performance of each attribute is computed. This performance is measured in terms of either precision i.e., maximizing the prediction of positive examples or False

Positive Rate (FPR) i.e., minimizing the prediction of negative examples or a combination of both. Then, a weight is assigned to each attribute based on these individual performances.

For testing, examples obtained from the testing graph characterized by same attributes are used and all examples are ranked based on their attribute values. Thus, n different rankings of the test examples for n different attributes are obtained. After that, these ranked lists are merged by using a supervised rank aggregation mechanism and the weights of the attributes acquired during learning process. The top n ranked examples in the aggregation are taken to be the predicted list of positive examples. By using this predicted list, the performance this proposed model is computed. In this case, k is equal to the number of positive examples in the testing graph.

3.1 Weights Computation

The topological measures weights are computed based on their capability for predicting correct elements in the top k positions of their rankings. The weights associated to the applied topological measures are computed based on the following criteria:

Maximizing positive precision: By maximizing the prediction of positive examples, the attribute weight is computed as:

$$w_i = n * Precision_i \quad (1)$$

In Eq. (1), n denotes the total amount of attributes and Precision represents the precision of attribute i based on the prediction of positive examples i.e., secure links. Precision is referred to as the percentage of predicted instances that are relevant.

Minimizing FPR: By minimizing the prediction of negative examples i.e., non-secure links, a weight is computed as:

$$w_i = n * (1 - FPR_i) \quad (2)$$

In Eq. (2), FPR denotes the FPR of attribute i based on the prediction of negative examples. FPR is referred to as the percentage of non-relevant instances that are predicted as relevant.

3.2 Supervised Rank Aggregation

Consider Li is the ranked list of n repeaters (a link) and Li (1) is the rank element x in the list Li. The top ranked element has the rank 0. Then, a primary individual Borda score of an element x for a link i is given by:

$$B_i(x) = n - \mathcal{L}_i(x) \quad (3)$$

Consider x and y are two repeaters. The local preference function is defined as follows:

$$Pref_i(x,y) = \begin{cases} 1, & if\ \mathcal{B}_i(x) > \mathcal{B}_i(y) \\ 0, & if\ \mathcal{B}_i(x) < \mathcal{B}_i(y) \end{cases} \quad (4)$$

Introducing the weights in Borda aggregation rule is rather simple. Consider $(w_1, w_2, \dots, w_r)$ are the weights for r links providing r ranked lists on n repeaters. Then, the weighted Borda score for a repeater x is given by:

$$\mathcal{B}(x) = \sum_{i=1}^{r} w_i * \mathcal{B}_i(x) \quad (5)$$

For approximate Kemeny aggregation, the weights are introduced into the definition of the non-transitive preference relationships between repeaters. This is modified as follows:

Consider w_T is the sum of all computed weights i.e., $w_T = \sum_{i=1}^{r} w_i$. For each couple of repeaters x, y, a score function is computed as follows:

$$score(x,y) = \sum_{i=1}^{r} w_i * Pref_i(x,y) \quad (6)$$

After that, the weighted preference relation $(\succ_w)$ is defined as follows:

$$\succ_w\ y: score(x,y) > \frac{w_T}{2} \quad (7)$$

This new preference relation is used for sorting a primary aggregation of repeaters to obtain a supervised Kemeny aggregation. The initial aggregation can be any of the input lists or an aggregation obtained by applying any other conventional aggregation method such as Borda. In this model, merge-sort is applied for the time being.

IV. RESULTS AND DISCUSSIONS

In this section, the performance of the proposed SQPSECP-ASMC model is evaluated and compared with the existing SQPSEASMC model by using Java. This comparative analysis is done in terms of different metrics,[5] such as differential privacy, latency and accuracy.

- **Differential Privacy:** It is used to estimate the confidentiality of this model.
- **Accuracy Measure:** It is used to measure the exactness of this model in terms of average accuracy and worst-case accuracy.
- **Latency:** It is used to measure the number of rounds required to interface all legitimate parties.

Table 1 gives the comparison of proposed SQPSECP-ASMC and existing SQPSEASMC models regarding differential privacy, average accuracy, worst-case accuracy and latency.

Table 1: Comparison of Performance Metrics.

	No. of Corrupt Parties	**SQPSEASMC**	**Sqpsecp-ASMC**
Differential Privacy	25	0.65	0.70
	50	0.69	0.74
	75	0.73	0.78
	100	0.77	0.82
	125	0.81	0.86
	150	0.85	0.90
	No. of Corrupt Parties	**SQPSEASMC**	**Sqpsecp-ASMC**
Average Accuracy (%)	25	78.3	81.5
	50	80.5	83.8
	75	82.9	85.4
	100	85.1	88.3
	125	87.6	90.7
	150	89.4	93.9
	No. of Corrupt Parties	**SQPSEASMC**	**Sqpsecp-ASMC**
Worst-case Accuracy (%)	25	58.2	62.1
	50	60.1	64.5
	75	62.3	66.8
	100	64.7	68.4
	125	66.5	70.2
	150	68.9	72.6
	No. of Corrupt Parties	**SQPSEASMC**	**Sqpsecp-ASMC**
Latency (Number of Rounds)	25	10	7
	50	12	9
	75	14	11
	100	16	13
	125	18	15
	150	20	17

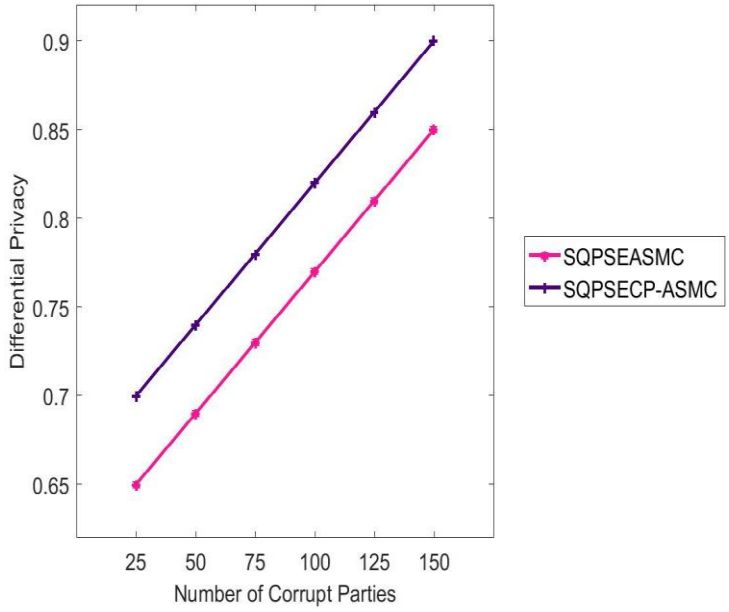

Figure 1: Comparison of Differential Privacy.

Figure 1 exhibits the assessment of SQPSECP-ASMC and SQPSEASMC in terms of differential privacy. For instance, consider the number of fraudulent parties is 150. At that point, the differential privacy for SQPSECP-ASMC is 5.88% boosted than SQPSEASMC. From this investigation, it is shown that the SQPSECP-ASMC model can increase the secrecy for all N parties than the SQPSEASMC model.

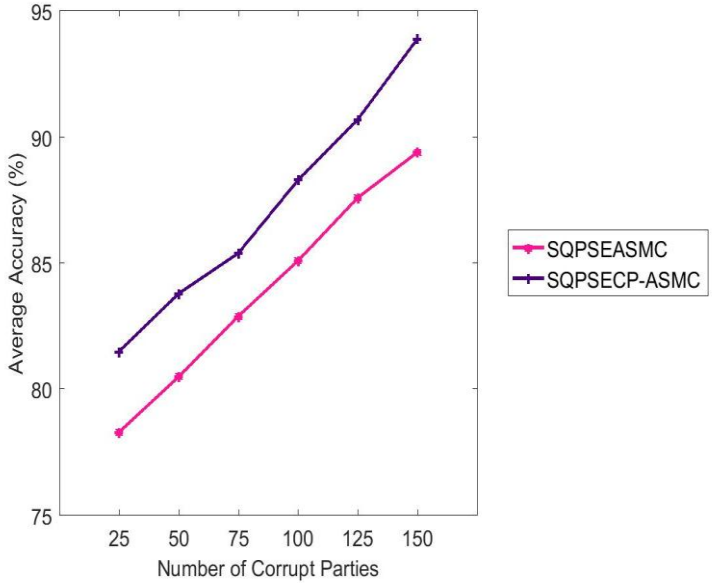

Figure 2: Comparison of Average Accuracy.

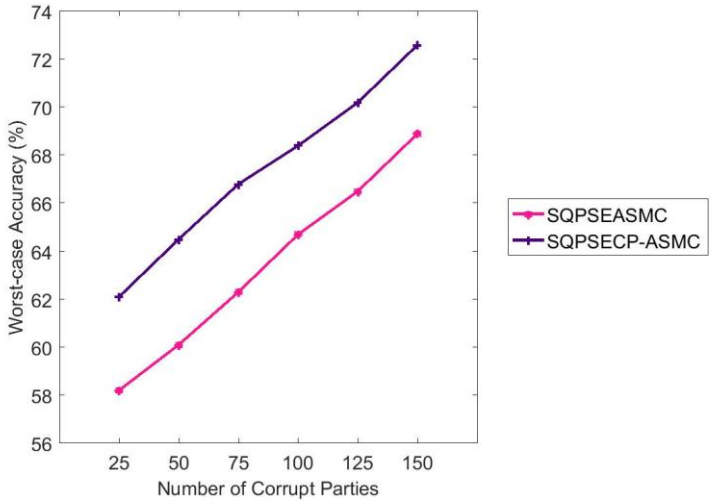

Figure 3: Comparison of Worst-case Accuracy.

Figure 2 and 3 represent the assessment of average and worst-case accuracy for proposed and existing models, correspondingly. On the chance that the amount of dishonest parties is 150, in that case the average accuracy of proposed SQPSECP-ASMC model is 5.03% increments than the SQPSEASMC model. Also, the worst-case accuracy of SQPSECP-ASMC is 5.37% higher than SQPSEASMC model. Along these lines, it is inferred that the proposed SQPSECP-ASMC model accomplishes higher exactness in both average and worst-case scenario for securely computing secret shares of the N-party functionality.

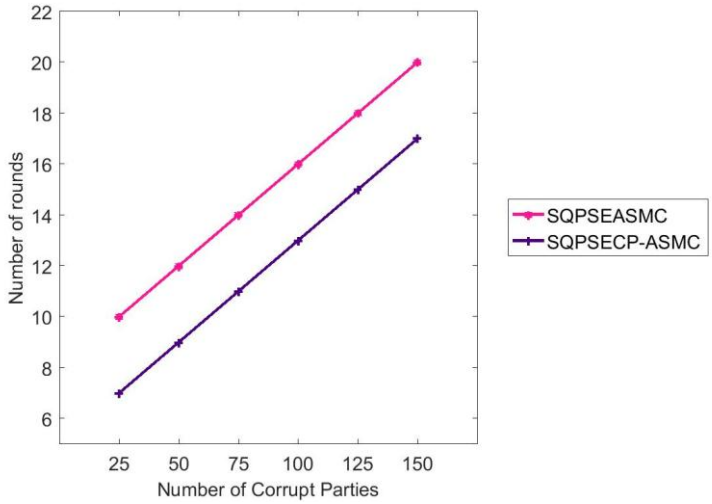

Figure 4: Comparison of Latency.

Figure 4 demonstrates the assessment of SQPSECP-ASMC and SQPSEASMC regarding latency. For instance, consider the amount of fraudulent parties is 150. For this condition, the number of rounds of proposed SQPSECP-ASMC model is 15% reduced than the

SQPSEASMC model. In this way, it is seen that the proposed SQPSECP-ASMC model significantly limits the number of rounds to interface all genuine parties with maximum secrecy.

V. CONCLUSION

In this article, SQPSECP-ASMC model is proposed to achieve the optimality of aggregated quantum repeaters by using a supervised rank aggregation method that predicts the unconnected links in a SMC networks. Initially, a list of unlinked nodes i.e., repeaters is ranked based on the topological measure. Then, the new links at a consecutive time interval is predicted by assigning a weight for each topological measure. Further, the link prediction is built by using these learned weights in a supervised rank aggregation model. In the end, the experimental results proved that the proposed SQPSECP-ASMC model has maximum differential privacy, average and worst-case accuracy and minimum latency.

REFERENCES

1. Fort, M., Freiling, F., Penso, L. D., Benenson, Z., & Kesdogan, D. (September). TrustedPals: Secure multiparty computation implemented with smart cards. In *European Symposium on Research in Computer Security* (pp. 34-48). Springer, Berlin, Heidelberg, 2006.
2. Cortinas, R., Freiling, F. C., Ghajar-Azadanlou, M., Lafuente, A., Larrea, M., Penso, L. D., & Soraluze, I. Secure failure detection and consensus in trustedpals. *IEEE Transactions on Dependable and Secure Computing*, 2012; *9*(4): 610-625.
3. Atif, M. Formal modeling and verification of distributed failure detectors. *Faculty of Mathematics and Computer Science, TU/e*, 2011; *10*.
4. Dinakaran, S. S., & Devapriya, M. Security and performance enhanced asynchronous secure multiparty computation (ASMC). *International Journal of Engineering Research & Technology*, 2019; *8*(06): 724-730.
5. Dinakaran, S. S., & Devapriya, M. Minimizing storage and communication costs in PSEASMC model, 2019.
6. Bäuml, S., & Azuma, K. Fundamental limitation on quantum broadcast networks. *Quantum Science and Technology*, 2017; *2*(2): 024004.
7. Azuma, K., & Kato, G. Aggregating quantum repeaters for the quantum internet. *Physical Review A*, 2017; *96*(3): 032332.

8. Pathak, M., Rane, S., & Raj, B. Multiparty differential privacy via aggregation of locally trained classifiers. In *Advances in Neural Information Processing Systems*, 2010; 1876-1884.
9. Goryczka, S., Xiong, L., & Sunderam, V. (March). Secure multiparty aggregation with differential privacy: A comparative study. In *Proceedings of the Joint EDBT/ICDT 2013 Workshops* (pp. 155-163). ACM., 2013.
10. Jung, T., Mao, X., Li, X. Y., Tang, S. J., Gong, W., & Zhang, L. (2013, April). Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation. In *Proceedings IEEE INFOCOM* (pp. 2634-2642). IEEE., *2013.*
11. Tian, L., Jayaraman, B., Gu, Q., & Evans, D. Aggregating private sparse learning models using multi-party computation. In *NIPS Workshop on Private Multi-Party Machine Learning*, 2016.
12. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., & Seth, K. (October). Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1175-1191). ACM., 2017.
13. Bindschaedler, V., Rane, S., Brito, A. E., Rao, V., & Uzun, E. (March). Achieving differential privacy in secure multiparty data aggregation protocols on star networks. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy* (pp. 115-125). ACM., 2017.
14. Long, Y., Gangwani, T., Mughees, H., & Gunter, C. Distributed and Secure ML with Self-tallying Multi-party Aggregation. *arXiv preprint arXiv:1811.10296*., 2018.