Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/5/20230590

The development of secure multi-party computation

Wanqing Hao

Western Canada High School, Calgary, Canada

anitah10@educbe.ca

Abstract. In an increasingly technological world, some significant issues that have developed in the past few years are privacy and data protection. This is generalized in the broad field of cryptography. People often use concepts from cryptography to find ways to access a distributed set of data without exposing or altering it, protecting them from outside parties obtaining access to their data for malicious purposes. This is often achieved through a specific method called Secure Multi-Party Computation. Throughout the past few decades, improvements in Secure MPC have skyrocketed, becoming an essential part of society. Whether in finance, statistics, or just typical data collection and protection, Secure MPC plays an important role. This paper will discuss the history behind Secure MPC as well as some of its modern-day applications. Furthermore, this paper will analyze the advantages and disadvantages of Secure MPC, evaluating its potential for growth in the coming century.

Keywords: Secure Multi-Party Computation, computing parties, input, output.

1. Introduction

Secure Multi-Party Computation is one of the most popular computational methods in using data without leaking or exposing private information. Parties can get their desired computed function output without gaining any knowledge of the data's specific inputs. In general, MPC works to ensure two properties: input privacy and robustness. To maintain input privacy, no party can interfere with the input data to affect the output function and results and to maintain robustness, dishonest parties also cannot interfere with the accuracy of results for the output result [1-3].

The process of MPC undergoes a three-step process. First, the input parties enter data into computation. Then, the computing parties undergo confidential computation. Finally, the result parties receive the output results [1-3]. The general idea of Secure MPC is shown in Figure 1 below:

DOI: 10.54254/2755-2721/5/20230590

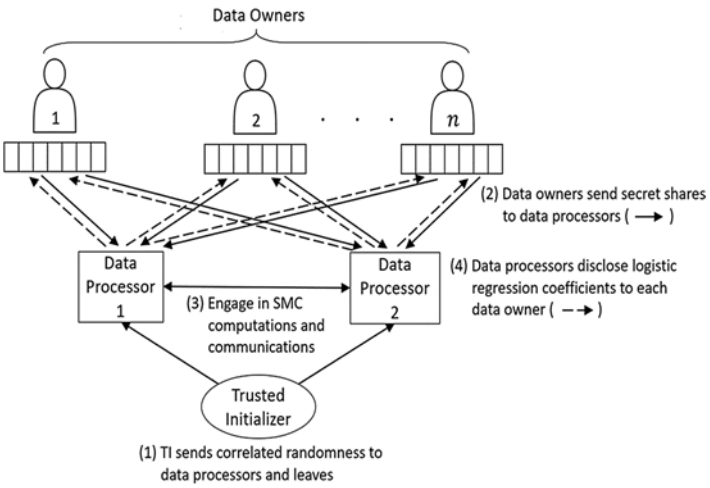

Fig. 1. Basic overview of the function procedures of SMPC [4].

With record-high accuracy and wide-ranging applications and abilities, many elements of Secure Multi-Party Computation are worth further consideration and development. This paper will explore the significance of Secure Multi-Party Computation in various modern-day applications and discuss its advantages and disadvantages and how it can be improved for the future.

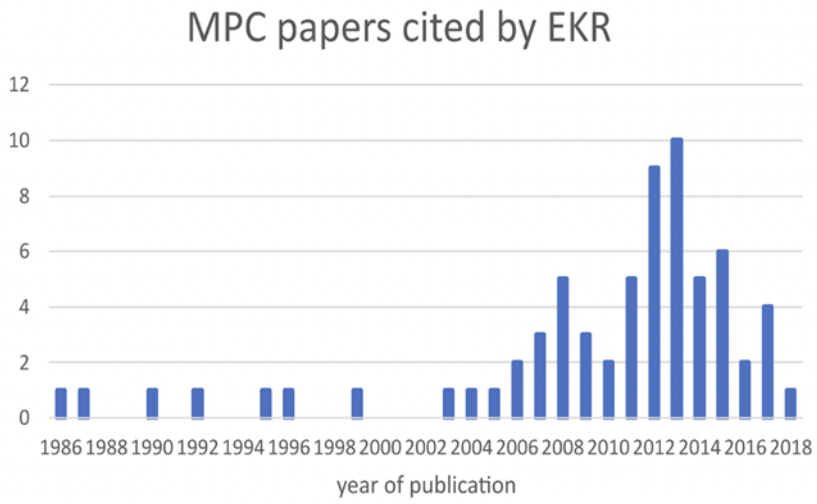

Fig. 2. Increased research has been done on Secure MPC to apply it to real-world scenarios.

As seen in the data graph above, almost 10 times the number of SMPC papers from the 1980s are being published today [2]. This shows how SMPC is constantly growing and holds an important place in society.

2. The Development of SMPC

First theoretical developments in Secure Multi-Party Computation occurred in 1982 by computational theorist and computer scientist Andrew Yao through the Millionaire Problem. In the Millionaire Problem, Yao questioned how two millionaires could determine who is the wealthiest without revealing their individual riches, and Secure Multi-Party Computation was born [5].

DOI: 10.54254/2755-2721/5/20230590

2.1. The Millionaire Problem

Suppose two people, Sally and Tristan want to determine who has more money among them without telling each other the specific amount they have. Sally has X dollars and Tristan has Y dollars and they want to determine if X > Y or Y > X. The goal of Secure Multi-Party Computation is to determine if X > Y or Y > X without knowing the specific values of X and Y. Let both X and Y be in the set of values {1, 15} [6].

First, Tristan sends Sally a random number n and Tristan also chooses a secret number N where |N| is a natural number. Then n + Y - 1is the encryption of N where Y is in the set {1, 15}. Sally then decrypts numbers n, n + 1, n + 2…n + 14 to get the corresponding $A_1 \ldots A_{15.} A_Y$, which is Tristan's secret N. However, Sally does not know which one it is, so Sally reduces all the values $A_1 \ldots A_{15}$ mod a random prime p, resulting in $Z_1 \ldots Z_{15}$ where Z_Y = N mod p and all the other Z values look random. Looking at all the Z_i values, she adds 1 (mod p) to all the Z_i values where i > X creating a new set of numbers $W_1 \ldots W_{15.}$ From the new set of numbers Sally sends Tristan, if W_Y = N mod p, that means that X ≥ Y. Otherwise, Y > X.

This was the beginning of Secure Multi-Party Computation. Following Yao's initial introduction to Secure Multi-Party Computation, David Chaum introduced the Dining Cryptographers Problem.

2.2. The Dining Cryptographers Problem

Suppose three cryptographers are dining together in their favorite restaurant. They are informed that arrangements have been made for them to pay the bill anonymously or the National Security Agency (NSA) has already paid for them. The way to find out if the NSA has not paid while keeping the identity of the payer is presented below [7-8]:

Each cryptographer flips a coin (0 - tails, 1 - heads). Ally's number is a, Bobby's number is b, and Carl's number is c. Let

$$A = a \wedge c \text{ and } B = b \wedge a \text{ and } C = c \wedge b \text{ (} \wedge \text{ stands for xor)}$$

If NSA has paid for the meal, then if we xor all of these computed values together, we get

$$A \wedge B \wedge C = a \wedge c \wedge b \wedge a \wedge c \wedge b$$

In this case, each pair of equivalent values cancel out, so

$$A \wedge B \wedge C = 0$$

If NSA has not paid for the meal, then whoever paid for the meal can flip the value of their own computed result. If Bobby paid for the meal, then

$$B = \neg(b \wedge a) \text{ (} \neg \text{ stands for not) and } A \wedge B \wedge C = (a \wedge c) \wedge \neg(b \wedge a) \wedge (c \wedge b) = (b \wedge a) \wedge \neg(b \wedge a) = 1$$

2.3. The Multi-Party Case

Olded Goldreich, Silvio Micali, and Avi Wigderson applied Yao's ideas to a multi-party case in 1987, expanding the applications of MPC in real-life [2]. Suppose we wanted to determine the average age of the 20 students in our class:

The first person would choose a random number N and whisper it to the second student. The second student would add his own age to N and whisper $N + A_2$ to the third student. The third student would add his own age to $N + A_2$ and whisper $N + A_2 + A_3$ to the fourth student and so on. The final twentieth student would whisper $N + A_2 + A_3 + \ldots + A_{20}$ to the first person and the first person would add his age A_1 to the sum as well getting $N + A_1 + A_2 + \ldots + A_{20}$. The first person would then just subtract N from the total sum and divide by 20 to get the average age without knowing any of the other students' ages [9].

2.4. Recent Developments

More recently, in the 2008 Danish Sugar Beet auction, farmers were able to bid for contracts at the auction without revealing the exact amount they were willing to pay for. They could participate in the

DOI: 10.54254/2755-2721/5/20230590

bid without revealing their own economic circumstances. This was the first large-scale real-life application of MPC [10].

3. Applications in Finance, Statistics and Privacy

In the past five years, the usage of MPC has increased worldwide. They have been applied to various aspects of society such as evaluating gender pay disparities, detecting tax fraud in Estonia, and preventing satellite collisions in space [10]. Apart from theoretical frameworks for its working system, Secure Multi-Party Computation also has many real-world applications, spanning 3 main areas: finance, statistics and data collection, and secure data exchange [1].

3.1. Finance

In the financial sector, some of the main problems burdening its industry are fraud and money laundering [11]. This paper will discuss three main projects to explore the use of MPC to solve this problem, including the tax fraud detection pilot project, collaborative statistics in finance, and off-exchange matching. In general, finance follows the following steps for data anonymization and analysis for business. First, they collect financial indicators, which include: total return (annual and semi-annual), number of employees (annual and semi-annual), percentage of export (annual and semi-annual), added value (annual and semi-annual), labor costs (annual), training costs (annual), and profit (annual). Second, the data set is then anonymized and sent to the Information Technology Laboratory, where the data is finally sorted and analyzed [12].

3.1.1. Tax Fraud Detection Projects. Starting off with the tax fraud detection projects, tax enforcement organizations require a database of information in order to conduct their research and investigations. They usually use mass surveillance systems to achieve this goal and engage in data collection on a grander scale. The processing of this collected data can help them discover potential suspects of tax evasion and fraud. However, this process of data processing requires Secure Multi-Party Computation.

For example, in 2016, the Estonian Tax and Customs Board wanted to process data from companies that detail their transactions with their partners. Specifically, if the transactions cost over 1000 euros, information will be used in the fight against Value Added Tax fraud. However, this lack of privacy resulted in backlash from the companies, so computer scientists invented an MPC system to solve this problem. As a result, companies entered the program as anonymous input parties, protected by cryptography. Similar to the systems mentioned in the generalization examples above, parties had access to their desired output information, but no details on the input values [13].

3.1.2. Collaborative Statistics in Finance. In collaborative statistics in finance, there exists an application system called Collaborative Statistics that allows for encrypted data to be shared between finance companies with only the results returned to the users, namely, the bank and its customers. The MPC system can aid in this process in three main ways. Firstly, they can help customers select banks and products by providing relevant information on their credit score and funds. Secondly, they can also help banks access customer information by collecting consumer performance data and records. Finally, it can also use this private input information to compare banks against their competitors and customers against other users, analyzing this data without any breach of privacy [1].

3.1.3. Off-Exchange Matching. Another application of MPC in finance is off-exchange matching. In many instances, buyers and sellers need to be matched through specialized matching services called Alternative Trading Systems. In this system, a lot of private information is held regarding how much a buyer is willing to buy and how much the seller is willing to sell. Using this private information, the system determines the compatibility between buyer and seller and makes recommendations based on these computed values. However, often, this system relies on trust to solve problems. This is where MPC comes in. With the development of MPC, people no longer need to rely on trust to undergo such

DOI: 10.54254/2755-2721/5/20230590

processes. Instead, they can rely on their information being fully encrypted and protected in most possible scenarios [1].

3.2. Data Analysis

For large scale data collection and analysis, there are two main applications: KPI analysis for an industrial sector and social studies on tax and education records. Both require widespread authorization and collection of data through private-preserving means such as MPC.

3.2.1. KPI Analysis. Regarding KPI analysis in an industrial sector, the Estonian government wanted to collect data on the specific financial situations and performance of various industrial companies and processes to gain a better understanding of the state of the industry. They also wanted to gain more knowledge on the state of their industry against competitors. In 2011, this goal was fulfilled through a secure MPC system that allowed input parties to upload their financial metrics to respective computing parties to obtain their desired results [12].

3.2.2. Records Analysis. In Social Studies on Tax and Education Records, researchers wanted to test their question: does working during studies cause students to extend or quit their studies? In Estonia, the Tax and Customs Board and the Ministry of Education and Research both acted as input parties in this project, finding their desired product from the MPC system. The study was officially conducted in 2015. However, the researchers were unable to get their desired result and further study needs to be conducted in order to create a fool proof system [14-15].

3.3. Privacy

Finally, as hinted in the previous applications, the main purpose and application of secure MPC is quite obviously, preservation of privacy. One specific application of this aspect of MPC is privacy-preserving statistics. This was mainly developed in the Danish R&D project “Big Data by Security” [16], focusing on how MPC can aid in the use of sensitive data in statistics and large collections of private information. Similar to the above applications, data inputted into the system is encrypted, later adapted into user-specific information that still maintains privacy above all else. Users are aware of the system analysis that happens in the computation of data and agree to its terms and conditions beforehand [1]. Figure 3 shows the process of privacy preservation in Secure MPC.

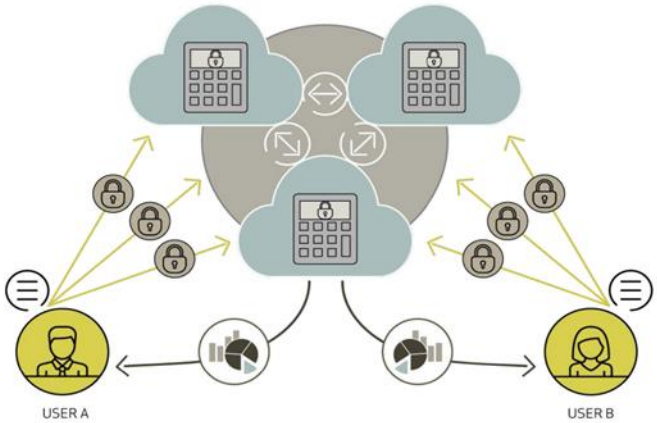

Fig. 3. Typical process of privacy preservation in Secure MPC [1].

DOI: 10.54254/2755-2721/5/20230590

4. Advantages and Disadvantages

Given the many applications of Secure MPC in the modern world, it is important to discuss its advantages and disadvantages.

4.1. Advantages

First considering its advantages, there are many reasons as to why Secure MPC is becoming increasingly popular in systematic cryptographic methods. These benefits include: commercial readiness, consistent data protection, high accuracy and precision, speed, and compliance to all privacy regulations [17].

Commercial readiness is the product's ability to handle and adapt to the existing consumer market apart from its technological maturity [18]. Compared to other forms of cryptography, MPC is one of the foremost programs for in-market use. It is easily programmable and easily used as one of the most widespread systems for this privacy preservation. This is mainly due to its flexibility. It can be altered to serve all purposes in various industries [19]. Suppose a company had an existing set of funds in Data Box A. If they want to move the set of funds into Data Box B while maintaining encryption and working through the same address and system, usually, this involves a certain risk of losing the funds or data because of the following steps. First, they create the new Data Box B. Then, they have to move all funds to a new Box. Finally, they also have to notify everyone of the change in Box.

Through Secure MPC, they can easily achieve this without risking the possibility of losing the funds. This is advantageous because funds do not need to be moved and no new Data Box must be created. Furthermore, no new address or system is created, simplifying the process for users too, making it among one of the most applicable cryptography systems to date [19].

Furthermore, Secure MPC is reliable and provides consistent data protection. In MPC, the private key, or the variable that encrypts data, is never held in one single place, lowering the risk of breaches from cybercriminals. Often, there are multiple keys to further ensure privacy. No employee can steal the digital assets as not everything is concentrated in one place [19]. The system is also fast and efficient, using minimal time to achieve its purposes.

Most importantly, Secure MPC can fulfill most requirements for privacy, offering the highest level of encryption.

4.2. Disadvantages

However, Secure MPC still has many faults and many realistic failures. There are still instances of passive and active corruption within the system. For example, competing parties may plant spy technology or viruses in each other's MPC systems, possibly leaking company information and data [20]. The main problem with MPC is that people need to place their trust in technology. Even if technology is a much safer and reliable source to trust, there are still so many things out of one's control.

5. Conclusion

Even with minor faults within its system, Secure Multi-Party Computation is by far the most innovative and progressive form of cryptography. Being applied to almost every single field requiring technology in the world, its impacts are constantly growing. The unique characteristic of Secure MPC is its potential. Ranging from two-party cases to million-party ones, SMPC has an unlimited range of use in a multitude of industries. In this paper, I have discussed some of the most overarching applications of SMPC in modern society, as well as its advantages and disadvantages in various computer programs. Evidently, SMPC is a highly impressive tool in data collection and privacy that needs to be developed. In the upcoming decades, it is important to further study in this area of cryptography, as it has the potential to completely change the world for the better.

References

[1] Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From Keys to Databases—Real-World Applications of Secure Multi-Party Computation. *The Computer Journal*, *61*(12). https://doi.org/10.1093/comjnl/bxy090.

DOI: 10.54254/2755-2721/5/20230590

[2] Kogan, D. (2021, May 27). *A few lessons from the history of multiparty computation*. Theory Dish. https://theorydish.blog/2021/05/26/few-lessons-from-the-history-of-multiparty-computation/.
[3] Lindell, Y. (2021). Secure multiparty computation. *Communications of the ACM, 64*(1), 86–96. https://doi.org/10.1145/3387108.
[4] De Cock, M., Dowsley, R., Nascimento, A. C. A., Railsback, D., Shen, J., & Todoki, A. (2021). High performance logistic regression for privacy-preserving genome analysis. *BMC Medical Genomics*, *14*(1). https://doi.org/10.1186/s12920-020-00869-9.
[5] *Yao's millionaire problem*. (n.d.). Xianmu.github.io. Retrieved October 6, 2022, from https://xianmu.github.io/posts/2018-11-11-yaos-millionaire-problem.html.
[6] Fisher, M. J. (2009). *Foundations of Cryptography - Lecture Notes 21*.
[7] *The Dining Cryptographers Problem*. (n.d.). Users.ece.cmu.edu. https://users.ece.cmu.edu/~adrian/731-sp04/readings/dcnets.html.
[8] *The Dining Cryptographer's Problem*. (n.d.). Smerity.com. Retrieved October 6, 2022, from https://smerity.com/articles/2012/dining_crypto.html.
[9] *In-Depth Guide Into Secure Multi-Party Computation in 2022*. (2021, October 25). Research.aimultiple.com. https://research.aimultiple.com/secure-multi-party-computation/.
[10] *What is Multi-Party Computation (MPC)? | Security Encyclopedia*. (n.d.). Www.hypr.com. https://www.hypr.com/security-encyclopedia/multiparty-computation-mpc.
[11] Sangers, A., van Heesch, M., Attema, T., Veugen, T., Wiggerman, M., Veldsink, J., Bloemen, O., & Worm, D. (2019). Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection. *Financial Cryptography and Data Security*, 605–623. https://doi.org/10.1007/978-3-030-32101-7_35.
[12] Bogdanov, D., Talviste, R., & Willemson, J. (2012). Deploying Secure Multi-Party Computation for Financial Data Analysis. *Financial Cryptography and Data Security*, 57–64. https://doi.org/10.1007/978-3-642-32946-3_5.
[13] Bogdanov, D., Jõemets, M., Siim, S., & Vaht, M. (2015). How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation. *Financial Cryptography*.
[14] Bogdanov, D., Kamm, L., Kubo, B., Rebane, R., Sokk, V., & Talviste, R. (2016). Students and Taxes: a Privacy-Preserving Study Using Secure Computation. *Proceedings on Privacy Enhancing Technologies*, *2016*(3), 117–135. https://doi.org/10.1515/popets-2016-0019.
[15] Talviste, R. (2016). *Applying Secure Multi-party Computation in Practice*.
[16] *Big Data by Security | Big Data by Security*. (n.d.). Bigdatabysecurity.dk. Retrieved October 6, 2022, from https://bigdatabysecurity.dk/.
[17] Iredale, G. (2021, September 21). *Know Everything about MPC (Multi-Party Computation)*. 101 Blockchains. https://101blockchains.com/mpc-multi-party-computation/.
[18] *What is CRL?* (2021, October 21). Granted Consultancy. https://grantedltd.co.uk/funding-blog/what-is-crl/.
[19] Tay, V. (2019, October 3). *7 reasons MPC is the next gen of private key security*. Fireblocks. https://www.fireblocks.com/blog/7-reasons-why-mpc-is-the-next-generation-of-private-key-security/.
[20] Zikas, V., Hauser, S., & Maurer, U. (2009). Realistic Failures in Secure Multi-party Computation. *Theory of Cryptography*, 274–293. https://doi.org/10.1007/978-3-642-00457-5_17.