International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 04, April 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

TECHNIQUES FOR SECURING MULTIPARTY COMPUTATIONS

Neha Mittal[1], Dr. Amit Sharma [2]

[1]M.Tech Scholar, [2] Professor, Department of Computer Science & Engineering,
Vedant College of Engineering & Technology ,Bundi ,Rajasthan,(India)

ABSTRACT

Secure Multi-party computation is a desirable feature in almost every field. The idea behind it is that any number of parties can communicate for a reason represented in the form of a function without having known about each other's details and still get as output the results of function computation from the given inputs by the parties. Yao in 1980's defined the concept of Garbled circuits for security against adversaries for a secure two-party computation model involving garbling the circuit for security. Over the years, a lot of work has been done in the direction of providing security in a two-party and multi-party environment. This problem is referred to as Secure Multi-party Computation Problem (SMC) in the literature. Research in the SMC area has been focusing on only a limited set of specific SMC problems, while privacy concerned cooperative computations call for SMC studies in a variety of computation domains. Before we can study the problems, we need to identify and define the specific SMC problems for those computation domains. We have developed a frame- work to facilitate this problem-discovery task. Based on our framework, we have identified and defined a number of new SMC problems for a spectrum of computation domains. Those problems include privacy-preserving database query, privacy-preserving scientific computations, privacy-preserving intrusion detection, privacy-preserving statistical analysis, privacy-preserving geometric computations, and privacy-preserving data mining.

This paper provides a brief survey of the recent developments headed in achieving secure computation using garbled circuits.

Keywords: Privacy, secure multi-party computation.

I. INTRODUCTION

Secure Multi-party Computation (MPC) revolves around the fact that any number of parties communicating with each other over a set of their private inputs gets back their outputs without having known the details of each other's inputs. The participants do not need an extra trusted party for solving their inputs and giving the outputs. A simple example to understand the same is the Millionaires' Problem, where two millionaires, say X and Y, need to know who is the richest among them two, without having any idea of what each other's net worth is. Secure MPC in this case will return as output the required answer without involving the two for any other task than providing their inputs. Therefore, for any successful MPC protocol, the two basic necessities are input privacy and correctness, the formal already been discussed above and the latter guaranteeing that the result of computation is correct and not, in any way, corrupt.

The question regarding how secure the Yao's MPC Protocol [1] is can be formally answered through a mathematical definition based on the ideal-real-world-paradigm. Taking the ideal-real-world-paradigm where a trusted third party is used to compute the inputs and send back the output; and the real-world-scenario where the computation only returns the outputs, hiding the inputs from the involved parties; the protocol can be tagged secure if one can learn no more about each party's private inputs in the real world than one could learn in the ideal world. Since no messages are exchanged between the involved parties in the ideal world problem, therefore, the real-world MPC cannot, in any way, disclose any input information and is secure.

The different forms of security, as deduced from the willingness of adversaries of deviating from the protocol can be semi-honest (passive) security and malicious (active) security. Adversary can be anyone who gets involved in the protocol. The first case refers to the adversaries trying to get information from the protocol without deviating from the protocol specification. Being a naïve model, its security in real world applications is weak. The model is still favored because of its efficiency and because at this level of security, inadvertent leakage of information is prevented thereby making the scheme useful if only the information leakage threat was a worry. The second case refers to an adversary deviating from the protocol execution for cheating purposes. The adversary in such a case are willing to cheat and not getting caught which otherwise would mean a damaging reputation. Therefore, security in such a model means a high security guarantee overall. A special case of passive security is covert security proposed by Ahn et al [2] where the communication between the involved parties seems like a normal ordinary looking conversation to the outside world and only when all the parties agree for a protocol, only then the execution of the protocol is visible. In this process, the involved parties also have no knowledge about the other participants of the protocol. To the uninvolved parties, the communication still appears as a normal conversation.

Yao proposed Garbled Circuits for secure 2-Party Computation [3]. Yao's construction encrypts/garbles the circuit for privacy preservation of the input values. This paper provides a brief overview of the working of garbled circuits in achieving secure 2-party and MPC followed by a brief survey of the recent developments in the direction of the same.

II. GARBLED CIRCUIT

Yao's garbled circuit protocol [3] is a secure two party protocol using Oblivious Transfer (OT). OT can be defined as the methods related to the transfer of one of the several values between two parties such that the sending party has no idea of what value was selected for transfer and the receiving party has no idea of what values were discarded for transfer. For two parties P_1 and P_2, Yao's proposal is formally defined in Fig.1 as reported in [4].

Yao's Garbled Circuits Protocol

1: *P1* generates a boolean circuit representation c_c of f that takes input i_{P1} from *P1* and i_{P2} from *P2*.
2: *P1* transforms c_c by garbling each gate's computation table, creating garbled circuit c_g.
3: *P1* sends both c_g and the values for the input wires in c_g corresponding to i_{P1} to *P2*.
4: *P2* uses *1-out-of-2 OT* to receive from *P1* the garbled values for i_{P2} in c_g.
5: *P2* calculates c_g with the garbled versions of i_{P1} and i_{P2} and outputs the result.

Figure 1 Yao's garbled circuit protocol

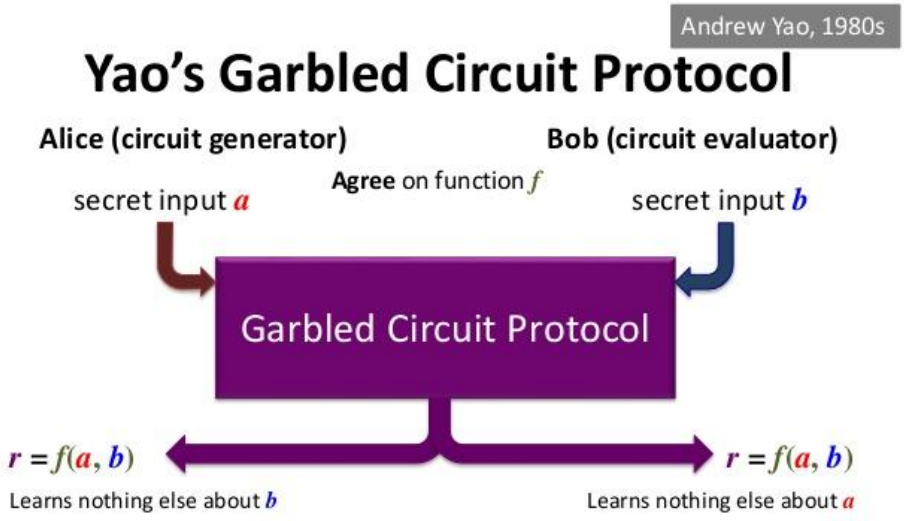

Figure 2 Yao's garbled flow circuit diagram

III. RECENT DEVELOPMENTS

As discussed earlier, Covert Two-party computation by Ahn et al [2] allows parties to run a protocol without them even knowing about the existence of each other and revealing the outputs of the computation only when all the involved parties favor the output. If in case, the outputs are unfavorable to any of the parties, then the execution of the protocol cannot be distinguished from a "ordinary-looking" conversation. Chandran et al [5] proposed a covert multi-party computation in the standard model not involving random oracles. The construction defines a fairness notion that at the end of the protocol, either all parties participating in the protocol will have knowledge about each other or none of them. Honest behavior in the protocol is enforced using "Zero-knowledge to garbled circuits". A covert version of "Timed Commitments" is also constructed for adding fairness in secure computation protocols. In addition, the authors give a formal definition of achieving covert multi-party computation in ideal/real world simulation paradigm.

Goyal et al [6] designed a secure multi-party computational model for security against covert adversaries. In addition to it, an improvement to a similar work of Aumann and Lindel [7] in two-party is also provided. The multi-party model provides security even in cases when majority of the parties involved are dishonest and uses a

black box containing implementable cryptographic primitives. The number of rounds in the two-party and multi-party settings is constant and logarithmic to the interaction between the parties respectively. The proposed two-party technique is secure even against the standard malicious adversaries though designed for the covert adversary model.

David et al [8] proposed a Fairplay Multi Party protocol for security against semi-honest adversaries inspired by Malkhi et al's [9] Fairplay proposal. The proposed technique involves a joint computation run by the involved parties taking as input the details of the parties and outputs the computation results personally to the associated parties. For the input, output and computations, the technique emulates a trusted party responsible for handling the security issues. The function is provided in a high level language description with a configuration file containing the IP addresses of the involved parties. The function is then compiled into a Boolean circuit evaluation of which returns no more information than required. The protocol used for implementation is a modified version of the Beaver- Micali- Rogaway protocol (BMR) [10] involving a constant number of rounds thereby sufficiently improving the performance of the protocol. Tate and Xu [11] also worked on improving the security of the BMR protocol [10] addressing a flaw in their construction that allows a honest-but-curious or passive adversary to take a look at personal data when evaluating the garbled circuit.

Huang et al [12] addressed the shortcomings of the Yao's garbled circuits for secure 2-party computation against semi-honest parties on efficiency grounds. The proposed 2-party technique is significantly faster than any existing technique on arbitrary large circuits and has improved memory requirements. Huang et al [13] then presented a framework involving pipelining and circuit level optimizations for building privacy preservation applications that use garbled circuits for security and which until recently was considered to lack efficiency and scalability in reality. Techniques are proposed in the paper that cut the cost of malicious resistant secure computations to be able to transform a protocol such that it can resist stronger adversaries. Fairness notion of providing results of computations to either all parties or none is also ensured in the work.

Kolesnikov and Kumaresan [14] in 2012 proposed an optimization aimed at improving the communication complexity of evaluation of a secure two party function using information- theoretic garbled circuit approach which is more efficient than the Yao's garbled circuit approach. When dealing with larger circuits, the circuit is sliced into layers and each layer is then evaluated using information-theoretic garbled circuits. The authors also introduced Selection Oblivious Transfer (SOT) as a new key building block. Inspired by the client server model, the authors proposed two variants of the construction; the first one secure against a semi-honest model consisting of semi-honest client and server and the second one providing security against a semi-honest server and covert client. Improvement with an approximation factor 2 for the first variant and of approximately 1.5 for the second variant for the security parameter, k, where $k \in \{128, 256\}$ is achieved. An asymptotic improvement by factor logarithmic to security parameter k is achieved in terms of communication and complexity over the state-of-the-art garbled circuits.

Goldwasser et al [15] proposed using reusable garbled circuits as a solution to the inability of the garbled circuits of providing no security in case of multiple inputs. The work is the first one in the direction of succinct single-key function encryption where succinctness of the scheme represents that the size of the ciphertext should not grow with the input function, but with its depth. Interaction of the scheme with the Learning with Errors

(LWE) problem guarantees security against an adversary as long as the adversary has access to a single key. Applicability of the work is then checked for token-based obfuscation, homomorphic encryption and a delegating computation scheme.

Mohassel et al [16] in 2015 proposed a secure 3-party protocol with efficiency competitive to the conventional information-theoretic 3-party protocols and Yao's 2-party semi-honest protocol [3] though using a constant number of rounds and inexpensive symmetric-key cryptography. Construction of the proposal is based on garbled circuits and it provides security against a single, malicious party.

IV. CONCLUSION

Secure two-party or multi-party computation using garbled circuits is a much popular research area. Garbled circuits for security have been proposed by Yao in 1980's. The proposal lays on the idea of encrypting/garbling the circuit for securing the details of inputs and outputs from semi-honest adversaries. Using the garbled circuits for security against, semi-honest, covert, active or passive adversaries in a two-party or multi-party environment has been the centre of research of many researchers since years. The other highlighted area is the improvements proposed to the existing works for more effective secure computation. This paper covers some of the note-worthy research areas headed in the direction of achieving security through the use of garbled circuits. An overview of the recent trends in the area gives the reader an insight of the techniques proposed as solutions to the problems encountered in secure multi-party computation.

REFERENCES

[1] A. Yao, "How to generate and exchange secrets (extended abstract)", *Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS'86)*, pp. 162-167, IEEE Computer Society Press, 1986.

[2] L. von Ahn, N. Hopper and J. Langford, "Covert two-party computation", Proceedings of the 37th Annual ACM Symposium on Theory of computing (STOC '05), pp. 513–522, New York, NY, USA, 2005. ACM Press.

[3] A. Yao. "Protocols for secure computations (extended abstract)", *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (FOCS '82)*, pp. 160–164, 1982.

[4] Peter Snyder, "Yao's Garbled Circuits: Recent Directions and Implementations".

[5] Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky and Amit Sahai, "Covert Multi-party Computation", 48th Annual IEEE Symposium on Foundations of Computer Science, pp. 238-258, 2007.

[6] Vipul Goyal, Payman Mohassel and Adam Smith, "Efficient Two Party and Multi Party Computation against Covert Adversaries", Advances in Cryptology- EUROCRYPT, pp.289-306, Springer, 2008

[7] Yonatan Aumann and Yehuda Lindell, "Security against covert adversaries: Efficient protocols for realistic adversaries", Proceedings of the Theory of Cryptography Conference, pp. 137-156, 2007.

[8] Assaf Ben-David, Noam Nisan and Benny Pinkas, "FairplayMP – A System for Secure Multi-Party Computation", Proceedings of 15th ACM Conference on Computer and Communications Security, pp. 257-266, 2008.

[9] D. Malkhi, N. Nisan, B. Pinkas and Y. Sella, "Fairplay-A Secure Two-Party Computation System", Proceedings of the 13th USENIX Security Symposium , pp. 287-302, 2004.

[10] D. Beaver, S. Micali and P. Rogaway, "The round complexity of secure protocols", Proceedings of the 22th TOC, pp. 503-513, 1990.

[11] Stephen R. Tate and Ke Xu, "On Garbled Circuits and Constant Round Secure Function Evaluation", Computer Privacy and Security Lab, Department of Computer Science, University of North Texas, Technical Report 2, 2003.

[12] Yan Huang, David Evans, Jonathan Katz and Lior Malka, "Faster Secure Two-Party Computation Using Garbled Circuits", USENIX Security Symposium, Volume 201, No.1, 2011.

[13] Yan Huang, Chih-hao Shen, David Evans, Jonathan Katz and Abhi Shelat, "Efficient Secure Computation with Garbled Circuits", Invited paper in 7th International Conference on Information Systems Security, pp. 28-48, Springer, 2011.

[14] Vladimir Kolesnikov and Ranjit Kumaresan, "Improved Secure Two-Party Computation via Information-Theoretic Garbled Circuits", I. Visconti and R. De Prisco (Eds.), Proceedings of SCN 2012, Volume 7485 of the LNCS, pp. 205–221, 2012.

[15] Shafi Goldwasser, Yael Kalai and Raluca Ada Popa, "Reusable Garbled Circuits and Succinct Functional Encryption", Proceedings of 45th Annual ACM Symposium on Theory of Computing, pp. 555-564, 2013.

[16] Payman Mohassel, Mike Rosulek and Ye Zhang, "Fast and Secure Three-party Computation: The Garbled Circuit Approach", Proceedings of the 22nd ACM SIGSAC Conference on Computers and Communications Security, pp. 591-602, ACM, 2015.