2009 International Symposium on Computing, Communication, and Control (ISCCC 2009)
Proc .of CSIT vol.1 (2011) © (2011) IACSIT Press, Singapore

Security Analysis of Secure Multi-Party Computation using Virtual Parties for Computation on Encrypted Data along with Performance

Rohit Pathak [1] and Satyadhar Joshi [2 +]

[1] Acropolis Institute of Technology & Research, Indore, M.P., India
[2] Shri Vaishnav Institute of Technology & Science, Indore, M.P., India

Abstract. There are many computations and surveys which involve confidential data from many parties or organizations. As the concerned data is property of the organization or the party, preservation and security of this data is of prime importance for such type of computations. Although the computation requires data from all the parties, but none of the associated parties would want to reveal their data to the other parties. The Virtual Party Protocol is a highly scalable protocol to perform computation on encrypted data using forced encryption and virtual cryptography. The data is encrypted in a manner that it does not affect the result of the computation. It uses modifier tokens which are distributed among virtual parties, and finally used in the computation. The computation function uses the acquired data and modifier tokens to compute right result from the encrypted data. Thus without revealing the data, right result can be computed and privacy of the parties is maintained. In this paper we have shown the security analysis of VPP protocol. We have given a probabilistic security analysis of hacking the protocol. We have obtained the results using MATLAB and shown how zero hacking security can be achieved.

Keywords: Secure Multi-Party Computation, Security, Forced Encryption, Virtual Cryptography.

1. Introduction

Yao has described millionaires' problem and gave the solution by using Deterministic Computations and introduced a view of Secure Computation [1]. We see about collaborative benchmark problem and a proposed solution in which the private shares are changed but in a manner that the sum remained the same [2]. Mikhail et al. has provided privacy-preserving solutions to collaborative forecasting and benchmarking that can be used to increase the reliability of local forecasts and data correlations, and to conduct the evaluation of local performance compared to global trends [3]. Wenliang et al. has proposed development of practical solutions to SMC problems, a new paradigm, in which we use an acceptable security model that allows partial information disclosure [4]. Linda et al. presents a unified approach to multi level database security based on two ideas: a trusted filter and an inference engine [5]. Wenliang et al. proposes the privacy preserving cooperative linear system of equations problem and privacy-preserving cooperative linear least-square problem [6]. Ran et al. has shown how uncorrupted parties may deviate from the case where even protocol by keeping record of all past configurations [7]. We have already seen the Anonypro Protocol, which had a good concept to make the incoming data of anonymous identity [8-10]. Anonypro Protocol assumed the connection between the party and anonymizer to be secured. In this paper we have shown the security analysis of VPP (Virtual Party Protocol). With proper configuration zero hacking security can be achieved with this protocol. We have shown the security analysis of the protocol. We have given a probabilistic security analysis of hacking the protocol. We have obtained the results using MATLAB and shown how zero hacking security can be achieved. We have illustrated this using many graphs.

+ Corresponding author. Tel.: + +91-94254-96651.
E-mail address: xrohit@hotmail.com, satyadhar_joshi@yahoo.com.

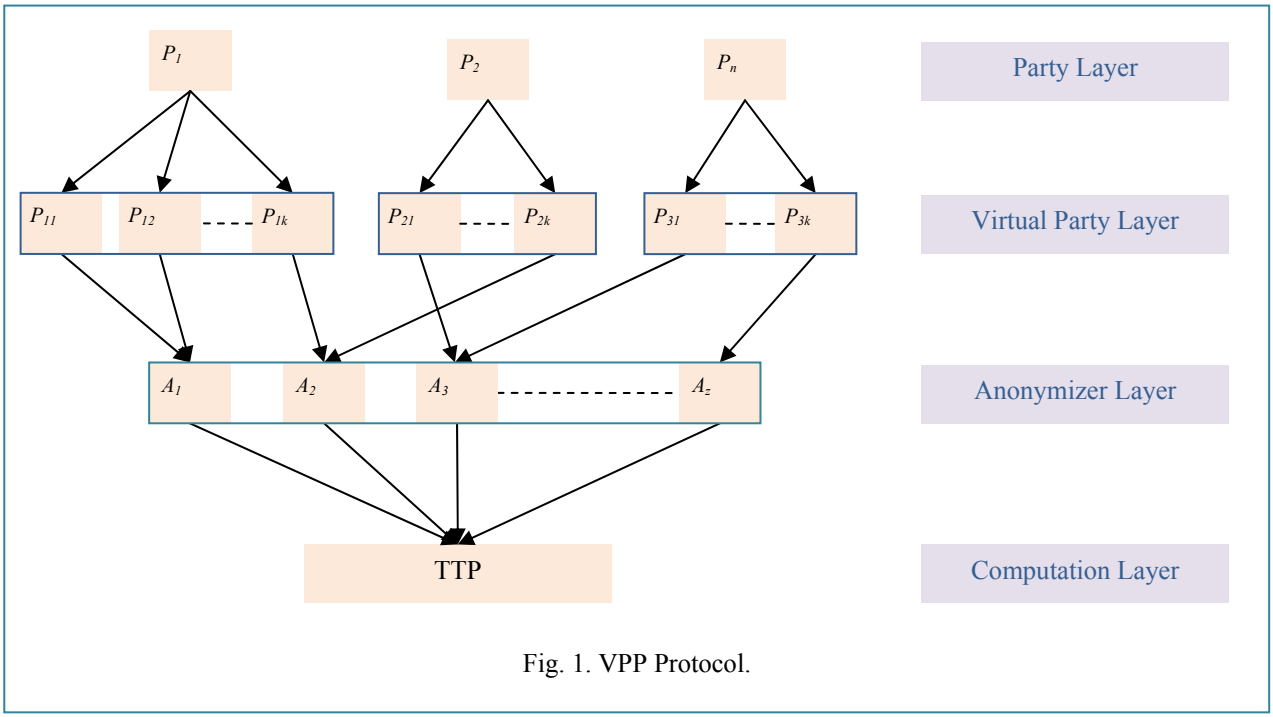

Fig. 1. VPP Protocol.

In our previous work we devised the Virtual Cryptography technique which used Enforced Encryption. We proposed the Virtual Party Protocol (VPP) which can be used safely to ensure the privacy of individual and preserving the data of the organization as a whole by not revealing the right data and will allow us to reach zero hacking security. In this method we will create some fake data and some virtual parties. Since the calculation is not dependent upon the number of parties, we can create any desired number of virtual parties. Now we will encrypt the data and create modifier tokens correspondingly. This modified data is mixed with fake data. These modifier tokens are related to the modification done in the data and will be used in the final computation to obtain the correct result. Now this modified data and the modifier tokens are distributed among the virtual parties. These parties will send their data to anonymizers. The anonymizers will send this data to Third Party for computation. Third Party will use the data and the modifier tokens to compute the result. The modifier tokens will aid to bring the result obtained by the encrypted data values. The modifier tokens in any manner will not reveal the identity of the party or such. The modifier is a short collection of information which is used in the final computation to ensure the right result. The method of encryption, modifier tokens, encrypted data and the method of computation all are interdependent.

2. Security Analysis of Virtual Party Protocol

If the TTP is malicious then it can reveal the identity of the source of data. The two layers of anonymizers will preserve the privacy of source of data. A set of anonymizers will make the source of data anonymous and will preserve the privacy of individual. The more the number of anonymizers in the anonymizer layer the less will be the possibility of hacking the privacy of the data. Each virtual party reaches TTP on their own. Each party will reach TTP as an individual party and TTP will not know the actual party which created the virtual party. The probability of hacking data of virtual party P_{ir} is

$$P\left(VP_{ir}\right)=\frac{1}{\sum_{i=1}^{n} k_i} \tag{1}$$

When party P_i has k_i number of virtual parties, the probability of hacking data of any virtual party of party P_r is

$$P\left(VP_{r}\right)=\frac{k_r}{\sum_{i=1}^{n} k_i} \tag{2}$$

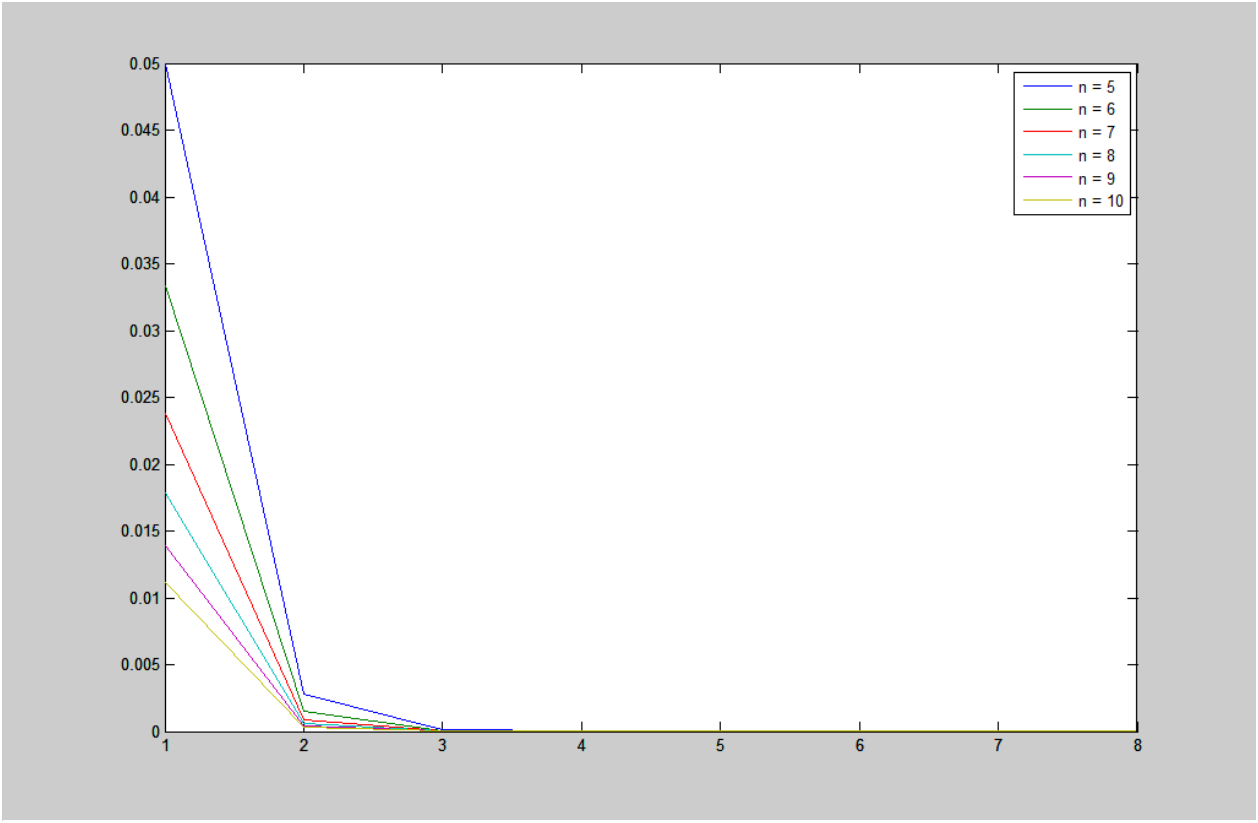

Fig. 2. Graph between number of Virtual Parties (x axis) vs Probability of hacking (y axis).

Even if the data of virtual party is hacked it will not breach the security as this data is encrypted. Probability of hacking the data of any party r is calculated as

$$P(P_r) = \frac{k_r}{\sum_{i=1}^{n} k_i} \times \frac{k_r - 1}{\sum_{i=1}^{n} k_i - 1} \times \cdots \times \frac{1}{\sum_{i=1}^{n} k_i - k_r} \tag{3}$$

The graph between number of virtual parties k vs. the probability of hacking $P(P_r)$ for $n=5,6,7,8,9,10$ is shown in Fig. 2. which clearly depicts that probability of hacking is nearly zero when the number virtual parties is three or more. Also the graph between number of parties and probability of hacking for $k=5,6,7,8,9,10$ is shown in Fig. 3. As the number of virtual parties is eight the probability of hacking is in the order of 10^{-5} or we can say nearly zero. Suppose that the number of virtual parties is k_a then

$$P(P_a) = \frac{k_a}{\sum_{i=1}^{n} k_i} \times \frac{k_a - 1}{\sum_{i=1}^{n} k_i - 1} \times \cdots \times \frac{1}{\sum_{i=1}^{n} k_i - k_a} \tag{4}$$

For k_b number of virtual parties we have

$$P(P_b) = \frac{k_b}{\sum_{i=1}^{n} k_i} \times \frac{k_b - 1}{\sum_{i=1}^{n} k_i - 1} \times \cdots \times \frac{1}{\sum_{i=1}^{n} k_i - k_b} \tag{5}$$

if ka > kb then P(Pa) < P(Pb) by Eq. (4) and Eq. (5). We can see that as the number of virtual parties increases the probability of hacking the data will decrease by harmonic mean.

Special Case 1 When the number of virtual parties is increased from k_a to k_a+1, the effect in probability of hacking is evaluated as

$$P(P_a) = \frac{k_a}{\sum_{i=1}^{n} k_i} \times \frac{k_a - 1}{\sum_{i=1}^{n} k_i - 1} \times \cdots \times \frac{1}{\sum_{i=1}^{n} k_i - k_a} \tag{6}$$

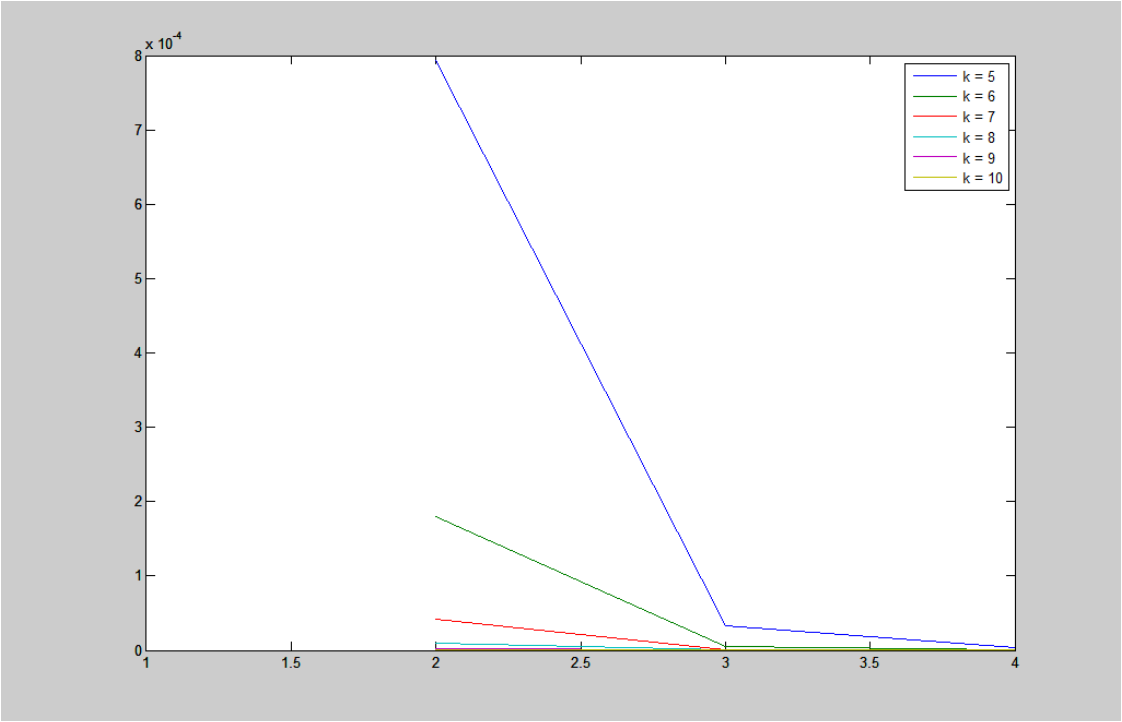

Fig. 3. Graph between number of Parties (x axis) vs Probability of hacking(y axis).

$$P\left(P_{a+1}\right)=\frac{k_a+1}{\sum_{i=1}^{n}k_i+1}\times\frac{k_a}{\sum_{i=1}^{n}k_i}\times\cdots\times\frac{1}{\sum_{i=1}^{n}k_i-k_a} \tag{7}$$

from Eq. (6) and Eq. (7) we can evaluate the ratio as

$$\frac{P\left(P_{a+1}\right)}{P\left(P_a\right)}=\frac{k_a+1}{\sum_{i=1}^{n}k_i+1} \tag{8}$$

There is a linear increase in the security of data when the number of virtual parties is increased, providing no significant change in security ratio. Graph between number of Virtual Parties k vs. $P(P_{a+1})/P(P_a)$ for $n=4$ has been shown in Fig. 4. and graph of number of Parties n vs. $P(P_{a+1})/P(P_a)$ for $k=8$ has been shown in Fig. 5.

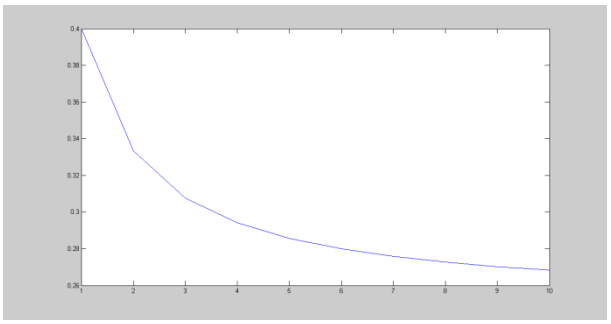

Fig. 4. Graph of number of Virtual Parties k (x axis) vs. $P(P_{a+1})/P(P_a)$ (y axis).

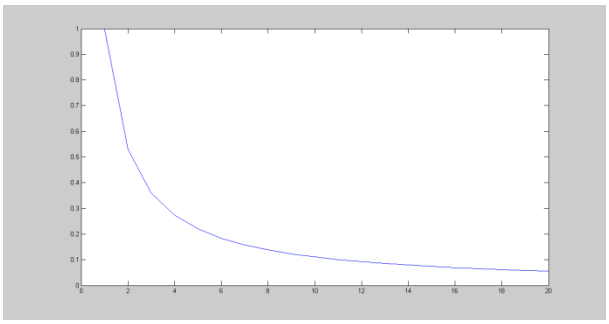

Fig. 5. Graph of number of Parties n (x axis) vs. $P(P_{a+1})/P(P_a)$ (y axis).

Special Case 2 When the number of virtual parties are increased from k_a to k_b where $k_b > k_a$ then the security ratio is evaluated as

$$\frac{P\left(P_b\right)}{P\left(P_a\right)}=\frac{\left(k_a+1\right)\times\left(k_a+2\right)\times\cdots\times k_b}{\left(\sum_{i=1}^{n}k_i+1\right)\times\left(\sum_{i=1}^{n}k_i+2\right)\times\cdots\times\left(\sum_{i=1}^{n}k_i+k_b-k_a\right)} \tag{9}$$

which shows that that changes in probability is represented as harmonic mean and it is clear that if the number of virtual parties is increased in multiple then there is a significance change in security ratio. It depicts that we should increase the number of virtual parties in multiples to increase the security. Even if data of all virtual parties of a particular party is hacked it will not breach the security. The data is encrypted and can only be used for computation and exact values can never be obtained from it.

3. Conclusion

Earlier we proposed VPP which uses Forced Encryption and Virtual Cryptography. In this paper we have presented a security analysis and shown how we can achieve zero hacking security by creating fake data and distributing it among the generated virtual parties and send this data along with modifier tokens to carry out computations on encrypted data using an improvised computation method. Anonymizer is used to hide the identity of the parties. VPP is used to perform computation on encrypted data. The protocol is highly scalable and optimized for computations of surveys, banking, business etc. It can allow us to reach zero hacking security for a wide variety of applications Using VPP protocol and algorithm a wide variety of computations can be optimally performed with enhanced security and privacy.

4. References

[1] Yao, Andrew C., "Protocols for secure computations," Proc. of 23rd Annual Symposium Foundations of Computer Science, pp. 160-164.

[2] Mikhail Atallah, Marina Bykova, Jiangtao Li, Keith Frikken, Mercan Topkara, “Private collaborative forecasting and benchmarking,” *Proc. of the 2004 ACM workshop on Privacy in the Electronic Society*, 2004.

[3] Mikhail Atallah, Marina Bykova, Jiangtao Li, Keith Frikken, Mercan Topkara, "Private collaborative forecasting and benchmarking," *Proc. of the 2004 ACM workshop on Privacy in the electronic society*, pp. 103 – 114, 2004.

[4] Wenliang Du, Zhijun Zhan, "A practical approach to solve secure multi-party computation problems," *Proc. of the New Security Paradigms Workshop*, 2002.

[5] Linda M. Null, Johnny Wong, "A unified approach for multilevel database security based on inference engines," *Transaction of ACM New York, NY, USA*, Vol. 21, Issue 1, Feb 1989.

[6] Wenliang Du; Atallah, M.J., "Privacy-preserving cooperative scientific computations," *Proc. 14th IEEE Computer Security Foundations Workshop*, Jun 11-13 2001, pp. 273 – 282.

[7] Ran Canetti, Uri Feige, Oded Goldreich, Moni Naor, "Adaptively secure multi-party computation," *Proc. The 28th annual ACM symposium on Theory of computing*.

[8] Mishra D.K., Chandwani M., “Extended protocol for secure multi-party computation using ambiguous identity,” WSEAS Transactions on Computer Research, Greece, Vol. 2, No. 2, Feb. 2007, pp. 227-233.

[9] Mishra D.K., Chandwani M., “Arithmetic cryptography protocol for secure multi-party computation,” In Proceeding of IEEE SoutheastCon 2007: The International Conference on Engineering – Linking future with past, Richmond, Virginia, USA, 22-25 Mar 2007, pp. 22-24

[10] Mishra D.K., Chandwani M., “Anonymity enabled secure multi-party computation for Indian BPO,” In Proceeding of the IEEE Tencon 2007: International conference on Intelligent Information Communication Technologies for Better Human Life, Taipei, Taiwan on 29 Oct. - 02 Nov. 2007, pp. 52-56.