ICIC Express Letters
Part B: Applications
Volume **9**, Number **12**, December **2018**
 ISSN 2185-2766
pp. **1217–1222**

A $(2, \lambda)$ ANONYMOUS DECISION LOGIC FOR SECURE MULTI-AGENT COMPUTING

Ajeet Singh[1], Vikas Tiwari[1] and Priyanka Garg[2]
[1]C. R. Rao AIMSCS
[2]School of Computer and Information Sciences
University of Hyderabad
Prof. CR Rao Road, Hyderabad 500046, Telangana, India
ajeetcs@uohyd.ac.in; { vikas.tiwari2403; priyankagarg112 }@gmail.com

Received August 2018; accepted October 2018

Abstract. *In some real-time scenarios of multi-agent computing, consider an instance where two committees need to perform some specific computation (here decision oriented logic), which requires collaboration among them but due to lack of mutual trust or to retain the privacy and integrity, they are not willing to expose their attributes with each other or publicly. In real scenarios, querying on various cloud services such as Google safe queries, PhishTank demands users to share their private data or browsing history for some processing. Various privacy preservation computing protocols have been evolved over past years. Still, computationally efficient and accurate method to deal with this problem is need of the hour. In this paper, we present a decision-theoretic vectorized computation model which is fast and simple to adopt practically. Our framework maintains the privacy of individual committee members λ_i, on whom the computation needs to be performed. We termed this way of computation as safe voting. We perform the complexity and accuracy assessment for the given framework. The experimental results discussion and analysis are also given in the paper.*
Keywords: Multi-agent computing, Private information retrieval, Linear vectors, Privacy, Decision theoretic logic

1. **Introduction and Prior Work.** In modern era, it is indispensable for various organizations with global context [1-3], as the threats are becoming more sophisticated day by day. In order to avert the privacy breach, anonymization methods [4-7] have been proposed over past years. Here, we summarize the problem of *anonymous Decision Logic* in *Information Retrieval (IR)*, where the privacy of the customer, who wants to retrieve the information or wants to outsource the information, needs to be preserved. To properly understand the problem scenario, assume user A and user B want to perform the collaborative computation without revealing their private parameters' information or if any untrusted third party is involved then at any particular time, third party or untrusted cloud should not know any type of private parameters' information associated to user A and user B. Various *Information Theoretic Private Information Retrieval (IT-PIR)* [8,9] schemes along with the *Computational Private Information Retrieval (CPIR)* schemes [10-14] have been designed/modeled in past years. Chor and Gilboa [15], Kushilevitz and Ostrovsky [16], Chang [17], Aguilar-Melchor et al. [18] have given privacy preservation techniques and proved them in terms of efficiency and security and analyzed on the factor of available computing resources. Chor et al. [19] proposed an scheme called private retrieval by keywords. Later, this scheme is extended by Olumofin and Goldberg [20] to perform the SQL (Structured Query Language) based queries. These private and anonymous schemes had been applied successfully in various domains such as *e-commerce*, *lookup tables*, and *anonymous data interchange* [13,21,22].

DOI: 10.24507/icicelb.09.12.1217

1.1. **Motivation and key contributions.** The pivotal goal of this line of research has been, to acquire privacy and integrity in the scenarios of anonymous decision logic while multi-agent computing. Despite spectacular advancements made so far, we tried in this paper, to achieve the goal through involvement of lightweight computations. Our key contributions in this paper are as follows.

- A decision theoretic vectorized computation model involving privacy preservation is proposed here.
- The complexity, accuracy assessment, correctness proof along with the experimental analysis for proposed framework is also given.

1.2. **Organization of the paper.** Remaining paper is organized as follows. Section 2 presents some significant preliminaries, definitions and notations. Our proposed system is given in Section 3. Section 4 presents the implementation results and comparative analysis. Finally, Section 5 concludes the paper.

2. **Preliminaries, Definitions and Notations.** This section represents some significant preliminaries, definitions and notations in this domain.

2.1. **Private Information Retrieval (PIR).** In a prototypical private information retrieval [8,9] scheme, a query comes from client side privately at database server such that the database server responds on requests without any intention to know them. Let us denote a user $\mathcal{U}$ and database $\mathcal{DB}$ that is holding the data. PIR is defined as below [10].

Definition 2.1. *Consider a database $\mathcal{DB}$, holding n number of bits, i.e., $x \in \{0,1\}^n$. Index $i \in \{1,2,\ldots,n\}$ is being held by user $\mathcal{U}$. PIR scheme permits to fetch the value of the i^{th} bit in x without leaking information about i to database.*

2.2. **Homomorphic computation.** The homomorphic encryption method [23] is able to perform operations on encrypted data without decrypting them which solves the problem of confidentiality and privacy inside cloud. The Homomorphic Encryption scheme (HE) is based on additive and multiplicative processing functions. Homomorphic encryption schemes are classified into two types.

2.2.1. *Partially homomorphic encryption.* A cryptosystem is thought as partially homomorphic, if it manifests either additive or multiplicative homomorphism property, but not both. Some examples are RSA (based on multiplicative homomorphism), Paillier (based on additive homomorphism), ElGamal (based on multiplicative homomorphism).

2.2.2. *Fully homomorphic encryption.* A cryptosystem is thought as fully homomorphic, if it manifests both additive and multiplicative homomorphism properties. FHE is considered as far more powerful and a great way to secure the outsourced data in an efficient manner. The encryptions on the plaintext p_1 and p_2 can be $Enc(p_1)$ and $Enc(p_2)$. Now, since FHE achieves both additive and multiplicative properties, both $Enc(p_1 + p_2)$ and $Enc(p_1 * p_2)$ can be computed in a secure and efficient manner.

2.3. **Computational verifiability.** Homomorphic Encryption (HE) can be assumed as a better solution to secure outsourcing of scientific computations, but it is useful when the returned result can be trusted.

Lemma 2.1. *It is infeasible to factorize the N in polynomial time if integer factorization in large scale is infeasible.*

Proof: Assume x is an adversary who is able to factorize a number N into primes p and q of probable same bit length in polynomial time. Suppose this operation probability as p'. Each factor *fact_i* of a number N will at least possess two prime factors. So the probability p''_r that the attacker can factorize it is almost lesser than p'. Thus the resultant

probability that attacker can factorize N is $\prod_{i=1}^{m} p_r'' \leq (p')^m$. Now if p' is negligible, the resultant probability is also negligible.

Definition 2.2. *A matrix $M \in R^{n,n}$ can be called as orthogonal if it satisfies one of the equivalent conditions – (i) $M.M^T = M^T.M = I_n$, (ii) M is invertible and $M^{-1} = M^T$.*

3. **Proposed System.** The limitations in existing schemes are analyzed through state-of-the-art review which drove the development of the proposed solution. In this section, first the methodology overview is presented. Further, the detailed procedure along with the security analysis and correctness proof is given.

3.1. **Methodology overview.** We presented a decision theoretic vectorized anonymity preserving computation model where the model entities and adopted methodology description are as follows: Consider two committees C_1 and C_2, each with total number of members as λ. Here the logic involved in the decision support system is as follows: Suppose the members of both the committees have to give a review vote for a product (here, assume that the review vote is in discrete valued boolean form, i.e., either 1 [positive] or 0 [negative]) in particular instances. So, committee C_1 possesses a linear vector called voting set V_1, similarly committee C_2 possesses a linear vector called voting set V_2 each with length λ. In our scenario, voting set V_1 and voting set V_2 act as private entities/parameters corresponding to C_1 and C_2 respectively.

The exposure of member's private parameters information is required in order to perform certain decision oriented computation ($\mathcal{D}$), but an individual member is not allowed to access other member's private parameters (in our scenario, $\mathcal{D}$ is the result of decision oriented query – *What is the count of positive review votes given by committees' members, occuring simultaneously in linear vectors V_1 and V_2?*). One common solution is to outsource the computation to cloud but in the untrusted environment of cloud, the desired computation may be not secure and feasible. In the framework, KGC is denoted as key generation center. Keeping an eye on this drawback, we adopted the secure decision logic computation methodology in untrusted cloud environment, as shown as Figure 1. The detailed functionality of each component in our framework is given in Section 3.2.

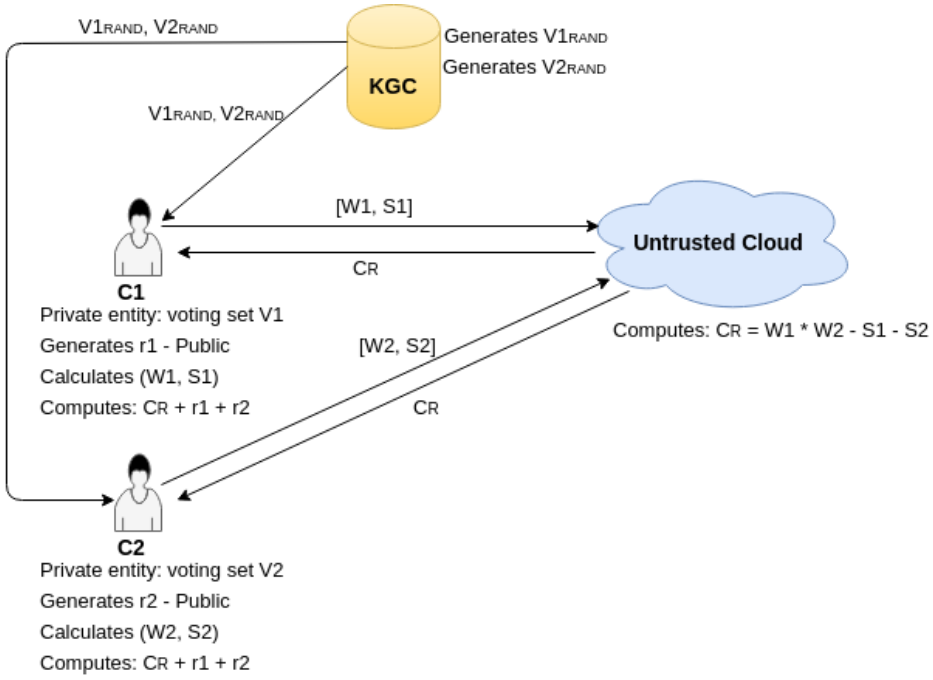


FIGURE 1. Proposed framework

3.2. **Detailed procedure.** The detailed procedure for proposed solution is given as Algorithm 1.

Algorithm 1

1: Begin procedure
2: C_1 possesses: voting set V_1; C_2 possesses: voting set V_2, where (V_1, $V_2 \mapsto$ private entities).
3: KGC: generates two random linear vectors $V_{1_{RAND}}$ and $V_{2_{RAND}}$, each with length λ.
4: KGC: securely transfers the pair of ($V_{1_{RAND}}$, $V_{2_{RAND}}$) to both C_1 and C_2.
5: C_1 and C_2 generate random numbers r_1 and r_2 respectively and declare them as public.
6: C_1 computes: $W_1 = V_1 + V_{1_{RAND}}$; $S_1 = V_1.V_{2_{RAND}} + r_1$
7: C_1 sends the computed entities (W_1, S_1) to cloud.
8: C_2 computes: $W_2 = V_2 + V_{2_{RAND}}$; $S_2 = V_2.V_{1_{RAND}} + r_2 + V_{1_{RAND}}.V_{2_{RAND}}$
9: C_2 sends the computed entities (W_2, S_2) to cloud.
10: Untrusted cloud performs following computation:

$$C_R \leftarrow W_1.W_2 - S_1 - S_2$$

11: Cloud sends back the computed result C_R to C_1 and C_2.
12: C_1 and C_2 independently compute: $\mathcal{D} \leftarrow C_R + r_1 + r_2$
13: End procedure

3.3. **Security analysis and correctness proof.** This section presents security analysis along with the correctness proof of the proposed decision logic oriented multi-agent computing model.

3.3.1. *Proposed protocol logic is correct.*

Proof: C_1 and C_2 are individually able to get desired decision query result $V_1.V_2$ in secure multi-agent computing. In step 10 of the above algorithmic procedure, untrusted cloud computes

$\Rightarrow W_1.W_2 - S_1 - S_2$
$\Rightarrow (V_1 + V_{1_{RAND}}).(V_2 + V_{2_{RAND}}) - (V_1.V_{2_{RAND}} + r_1) - (V_2.V_{1_{RAND}} + r_2 + V_{1_{RAND}}.V_{2_{RAND}})$
$\Rightarrow$ $(V_1.V_2 + V_2.V_{1_{RAND}} + V_1.V_{2_{RAND}} + V_{1_{RAND}}.V_{2_{RAND}} - V_1.V_{2_{RAND}} - r_1 - V_2.V_{1_{RAND}} - r_2 - V_{1_{RAND}}.V_{2_{RAND}})$
$\Rightarrow (V_1.V_2 - r_1 - r_2) \mapsto C_R$

In step 12, each of C_1 and C_2 computes

$\Rightarrow C_R + r_1 + r_2$
$\Rightarrow (V_1.V_2 - r_1 - r_2) + r_1 + r_2$
$\Rightarrow V_1.V_2$

3.3.2. *Privacy preservation holds during entire communication logic.* As voting sets, V_1 and V_2 are private entities of C_1 and C_2 respectively, in the collaborative decision logic computation, C_1 and C_2 are not allowed to share this information with each other or any untrusted third party. In the protocol, since $(V_{1_{RAND}}, V_{2_{RAND}})$ are only known to both C_1 and C_2, when untrusted cloud obtains W_1, W_2, S_1, S_2 from C_1 and C_2, cloud never gets the clue about secret entities V_1 and V_2.

Justification: In step 7 of Algorithm 1, C_1 sends computed entities W_1, S_1 to the untrusted cloud. Since cloud possesses no information about $V_{1_{RAND}}$ the guess and determine attack to obtain V_1 is not possible. Similarily, in step 9, C_2 transmits computed entities W_2, S_2 to the untrusted cloud. Since cloud has no information about $V_{2_{RAND}}$, the guess and determine attack for obtaining V_2 is also not possible.

Resultantly, even though r_1 and r_2 are defined as public entities, cloud has no possibility to guess and determine about V_1 and V_2.

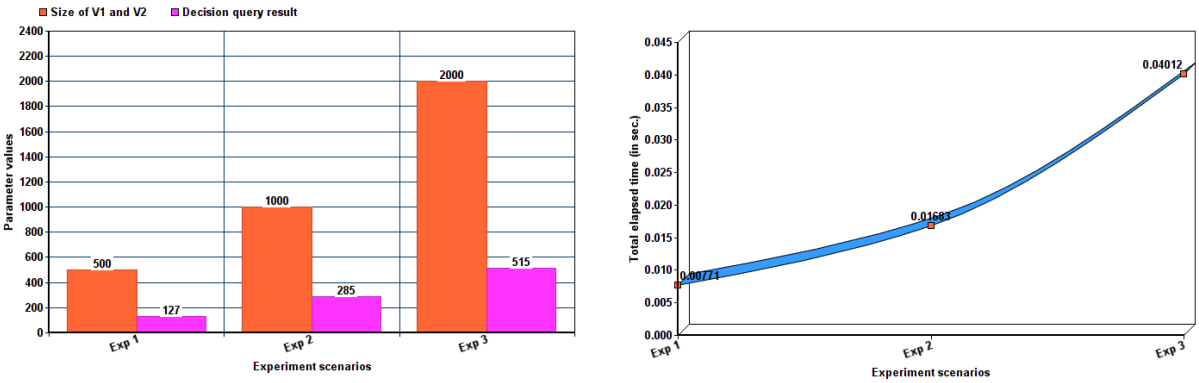
4. **Implementation and Results Discussion.** This section presents the results obtained in different experimental scenarios.

4.1. **Experimental set-up.** Our system specifications (Software and Hardware) are as follows – OS: Ubuntu 16.04 LTS, 64 bit is used; our hardware consists of 4 GB RAM size along with Intel core i5 4030U CPU processor @1.90GHz × 4 clock speed. We used Python v'3.5 language environment in the experiments.

4.2. **Procedure and results.** Experiments have been performed considering different scenarios utilizing the proposed procedure. In first experiment, size of linear vectors (voting sets V_1 and V_2) is taken as 500; in second experiment, it is 1000; and in third experiment, it is 2000. The obtained results are given in Table 1. In the table, computational time acquired by C_1 and C_2 is computed and represented as t_1; computational time acquired by cloud is represented as t_2. Total elapsed time for decision logic computation and communication by multi-agents is given as $(t_1 + t_2)$. Last column in Table 1 represents the final desired result after execution of the entire process. Graphical visualization is shown as Figure 2(a) Performance graph 1 and Figure 2(b) Performance graph 2. In Figure 2(a), X-axis represents different experiment scenarios taken into consideration and Y-axis represents parameter values corresponding to experiments. In Exp 1, the size of V_1 and V_2 is taken as 500 and the decision query result output obtained after execution of the protocol is as 127. Similarily, for Exp 2 and Exp 3, these two corresponding parameter values are shown in graph. In Figure 2(b), X-axis represents different experiment scenarios and Y-axis represents total elapsed time $(t_1 + t_2)$ in seconds.

Table 1. Experimental results

Experiment	Size of V_1 & V_2	t_1 (in sec.)	t_2 (in sec.)	Total elapsed time $(t_1 + t_2)$	Decision query result
I	500	0.0077	0.00001	0.00771	127
II	1000	0.0168	0.00003	0.01683	285
III	2000	0.0401	0.00002	0.04012	515



(a) Performance graph 1

(b) Performance graph 2

Figure 2. Performance plots

5. **Conclusions.** Multi-agent systems interacting intelligently can solve the problems which are sufficiently hard for single party computation. Privacy preservation while computation of a decision logic in multi-agent scenarios is a prime goal in any practical untrusted environment. The ultimate goal of this line of research has been, of course, to obtain a computationally efficient and secure multi-agent decision logic computation

protocol which can function well in untrusted environment. In this paper, the targeted goal has been achieved through the proposed research. As future research directions, we try to generalize the proposed protocol logic into (N, λ) anonymous decision logic, where N can be any number of committees in general. We also test the practicality in privacy preservation oriented real time applications.

REFERENCES

[1] *https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/*, 2016.

[2] C. Gilbert, M. E. Hellman and T. A. Berson, *Scalable Security: Cyber Threat Information Sharing*, 2014.

[3] G. Kuenning and E. L. Miller, *Anonymization Techniques for URLs and Filenames*, Technical Report, University of California, 2003.

[4] *https://www.torproject.org/*.

[5] S. E. Coull, C. V. Wright, A. D. Keromytis, F. Monrose and M. K. Reiter, Taming the devil: Techniques for evaluating anonymized network data, *Proc. of the 15th Annual Network and Distributed System Security Symposium*, San Diego, CA, pp.125-135, 2008.

[6] J. King, K. Lakkaraju and A. Slagell, A taxonomy and adversarial model for attacks against network log anonymization, *Proc. of the 2009 ACM Symposium on Applied Computing*, pp.1286-1293, 2009.

[7] T. Li and N. Li, On the tradeoff between privacy and utility in data publishing, *Proc. of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp.517-526, 2009.

[8] *https://crypto.stanford.edu/pir-library/*.

[9] R. Ostrovsky and W. E. Skeith III, A survey of single-database private information retrieval: Techniques and applications, *Proc. of the 10th International Conference on Practice and Theory in Public-Key Cryptography*, pp.393-411, 2007.

[10] B. Chor, E. Kushilevitz, O. Goldreich and M. Sudan, Private information retrieval, *Proc. of the 36th Annual Symposium on Foundations of Computer Science*, vol.45, no.6, pp.965-981, 1998.

[11] A. Beimel, Y. Ishai and T. Malkin, Reducing the servers computation in private information retrieval: PIR with preprocessing, *Proc. of the 20th Annual International Cryptology Conference on Advances in Cryptology*, pp.55-73, 2000.

[12] I. Goldberg, Improving the robustness of private information retrieval, *Proc. of the 2007 IEEE Symposium on Security and Privacy*, pp.131-148, 2007.

[13] R. Henry, F. Olumofin and I. Goldberg, Practical PIR for electronic commerce, *Proc. of the 18th ACM Conference on Computer and Communications Security*, pp.677-690, 2011.

[14] F. Olumofin and I. Goldberg, Revisiting the computational practicality of private information retrieval, *Financial Cryptography and Data Security*, pp.158-172, 2012.

[15] B. Chor and N. Gilboa, Computationally private information retrieval, *Proc. of the 29th Annual ACM Symposium on Theory of Computing*, pp.304-313, 1997.

[16] E. Kushilevitz and R. Ostrovsky, Replication is not needed: Single database, computationally-private information retrieval, *Proc. of the 38th Annual Symposium on Foundations of Computer Science*, p.364, 1997.

[17] Y.-C. Chang, Single database private information retrieval with logarithmic communication, *Information Security and Privacy*, pp.50-61, 2004.

[18] C. Aguilar-Melchor, J. Barrier, L. Fousse and M.-O. Killijian, Xpire: Private information retrieval for everyone, *Proceedings on Privacy Enhancing Technologies*, pp.155-174, 2016.

[19] B. Chor, N. Gilboa and M. Naor, Private information retrieval by keywords, *Ndss Symposium*, pp.535-540, 1997.

[20] F. Olumofin and I. Goldberg, Privacy-preserving queries over relational databases, *Privacy Enhancing Technologies*, pp.75-92, 2010.

[21] P. Mittal, F. G. Olumofin, C. Troncoso, N. Borisov and I. Goldberg, PIR-Tor: Scalable anonymous communication using private information retrieval, *USENIX Security Symposium*, 2011.

[22] H. Kikuchi, Private revocation test using oblivious membership evaluation protocol, *The 3rd Annual PKI R&D Workshop*, 2004.

[23] C. Gentry, Fully homomorphic encryption using ideal lattices, *Proc. of the 41st Annual ACM Symposium on Theory of Computing*, 2009.