A Communication Network Preserves the Privacy of the user using Unique IDs

Kiran B.T
M.Tech, CNE student
T.John Institute Of Technology
Banglore, India

Anju Abraham
Assistant Professor, Dept. of CSE
T.John Institute Of Technology
Banglore, India

Abstract— **An algorithm for anonymous sharing of private data among parties is developed. This technique is used to assign these n ID numbers ranging from 1 to N.The popularity of internet as a communication medium whether for personal or business use depends in part on its support for anonymous communication. Businesses engage in anonymous communication and avoid the consequences of identity revelation. Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements.**

Keywords— Privacy Preservation, File Sharing, data sharing, key-aggregate encryption,Secure sum.

I.INTRODUCTION

The popularity of internet as a communication medium whether for personal or business use depends in part on its support for anonymous interaction. Businesses also have legitimate reasons to engage in anonymous communication and avoid the consequences of identity. For example, to allow dissemination of summary data without revealing the identity of the entity the underlying data is associated with whistle-blower’s right to be anonymous and free from political or economic retributions. Cloud based web-site management tools provide capabilities for a server to anonymously capture the visitor’s actions. The problem of sharing privately held data so that the individuals who are the subjects of the data cannot be identified. Researchers have also investigated the relevance of anonymity and/or privacy in various application.

Another form of anonymity, as used in secure computation, allows multiple parties on a network to jointly carry out a global computation that depends on data from each party while the data held by each party remains unknown to the other parties. A secure function widely used in the literature is secure sum that allows parties to compute the sum of their individual inputs without disclosing the inputs to one another. This function is popular in data applications and also helps characterize the complexities of the secure multiparty computation.

This work deals with efficient algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are anonymous using a distributed computation with no central authority. Given nodes, this assignment is essentially a per-mutation of the integer with each ID being known only to the node to which it is assigned. Our algorithm is based on a method for anonymously sharing simple data and results in methods for efficient sharing of data. There are many applications that require dynamic unique IDs for nodes. Such IDs can be used as part of schemes for sharing/dividing communications bandwidth, data storage, and other re anonymously and with no conflict. The IDs are needed in sensor networks for security or for administrative tasks requiring reliable, such as configuration and monitoring of each nodes. An application where IDs need to be anonymous is grid computing where one may seek services without divulging the identity of the service requester.

To differentiate anonymous ID assignment from anonymous communication a situation where parties wish to display their data collectively, but anonymously, assign slots on a third party site. The IDs can be used to assign the IDs to users, while anonymous communication, can allow the parties to identities from the third party.

In another application, it is possible to use secure sum to use secure sum to allow one to opt-out of a computation beforehand on the basis of certain rules in statistical disclosure limitation or during a computation and even to do so in an anonymous type. However, very little is known with respect to methods allowing agencies to opt-out of a secure computation based on the results of the analysis, should feel that those results are too informative about their data.

The work reported in this paper further explores the connection between sharing secrets in an anonymous way, distributed secure multiparty computation and anonymous ID assignment. The use of the term “anonymous” here differs from its meaning in research dealing with symmetry breaking and leader election in anonymous network. Our network is not anonymous and the participants are identifiable in that they are known to and can be addressed by the others.

Methods for assigning and using sets of pseudonym, have been developed for anonymous communication in mobile network. The methods developed in these works generally require a trusted administrator, written, and their end products generally differ from ours in form and/or in statistical properties.

This paper builds an algorithm for sharing simple integer data on top of secure summation. The sharing algorithm will be used at each iteration of the algorithm for anonymous ID assignment (AIDA). This AIDA algorithm, and the variants that we discussed, can require a variable and unbounded number of iterations. Finitely-bounded algorithms for AIDA are discussed in Section IX. Increasing a parameter in the algorithm will reduce the number of expected round. However, our central algorithm requires solving a polynomial with coefficients taken from a finite field of integers modulo a prime. We show how to obtain the average number of required rounds, and in the Appendix detail a method for solving the polynomial, which can be distributed among the participants.

II. A REVIEW OF SECURE SUM

Suppose that a group of hospitals with individual databases wish to compute and share only the average of a data item, such as the number of hospital acquired infections, without revealing the value of this data item for any member of the group. Should all pairs of nodes have a secure communication channels available, a simple, but resource intensive, secure sum algorithm has been constructed. In the following algorithm, it is useful to interpret the values as being integer on first reading:

TABLE I
RANDOM NUMBERS TRANSMITTED BY A SECURE SUM EXECUTION

$Nodes$	$\hat{r}_{i,1}$	$r_{i,1}$	$r_{i,2}$	$r_{i,3}$	$\boldsymbol{r_{i,4}}$	d_i	$\hat{d}_i$
$n_{i=1}$:	$13-6+8=15$	13	−10	6	**−3**	6	8
$n_{i=2}$:	$7-10+9=6$	7	3	−5	**5**	10	9
$n_{i=3}$:	$-8-6+5=-9$	−8	11	12	**−9**	6	5
$\boldsymbol{n_{i=4}}$:	**6**	**6**	**−8**	**−5**	9	**2**	**2**
$s_i =$	**18**	**18**	**−4**	**8**	**2**	$T=$ **24**	**24**

Algorithm 1 (Secure Sum): Given nodes each holding an data item from a finitely representable abelian group, share the value among the nodes without re-vealing the values .

1) Each node, chooses random values.

2) Each "random" value is transmitted from node to node. The sum of all these random numbersis, of course,the desired total.

3) Each node totals all the random values.

4) Now each node simply broadcasts to all other nodes so that each node can compute:

The secure sum method of Algorithm 1 is input permutation resistant to the collusion of any subset of the participating nodes.

Other secure sum algorithms certainly can be used with physically or cryptographically secured communications channels. For example, it is easy to see that secure sum using a single Hamiltonian cycle is input permutation collusion resistant provided that the coalition is trapped in a connected region of the cycle. Such results can also be extended to provide privacy guarantees for the algorithms in subsequent sections should they utilize.

III. TRANSMITTING SIMPLE DATA WITH POWER SUMS

Suppose that our group of nodes wishes to share actual data values from their databases rather than relying on only statistical information as shown in the previous section.However, the data is to remain anonymous. We develop a collusion resistant method for this task using secure sum as our underlying communication mechanism. The power sums can be collected and shared using a single round of secure sum by sending them as an array and applying the method to the vectors transmitted and received.

TABLE II
POWERS OF DATA VALUES d_i CHOSEN BY EACH NODE $= 11$MODULO P

d_i^e	$e=1$	$e=2$	$e=3$	$e=4$
$n_{i=1}$:	6	3	7	9
$n_{i=2}$:	10	1	10	1
$n_{i=3}$:	6	3	7	9
$n_{i=4}$:	2	4	8	5
$\sum d_i^e$	$P_1=2$	$P_2=0$	$P_3=10$	$P_4=2$

Theorem 4 (Power Sum Data Sharing is -Private): The data sharing method of Algorithm 2 is resistant to the collusion of any subset of the participating nodes when based on the secure sum Algorithm 1.

Because the input data is present as a multiset in the output of every party and all parties are semi-honest the result is implied by our previous discussions of the secure sum Algorithm 1. The data sharing is anonymous in the sense that the sources of the data items cannot be traced. Of course, it is possible that a given data value would make sense only for a certain participant due to some factor such as the relative sizes of the participants. The paper shows how anonymous opt-out can be used to address some of these concerns.

IV. SHARING COMPLEX DATA WITH AIDA

Now consider the possibility that more complex data is to be shared amongst the participating node. Each node has a data item of length bits which it wishes to make public anonymously to the other participants.

As the number of bits per data item and the number of nodes becomes larger, the method of the previous section become infeasible. Instead, to accomplish this sharing, we will utilize an indexing of the nodes. Methods for finding such an indexing are developed in subsequent sections.

TABLE III
TRACE OF AN AIDA ALGORITHM EXECUTION

R	Step	A	r_1	r_2	r_3	r_4	q_1	q_2	q_3	q_4	s_1	s_2	s_3	s_4
1	2	0	6	10	6	2								
1	3	0	6	10	6	2	2	6	6	10				
1	4	0	6	10	6	2	2	10				2		1
1	5	2										2		1
2	2	2	5	0	6	0						2		1
2	3	2	5	0	6	0	0	0	5	6		2		1
2	4	2	5	0	6	0	5	6			3	2	4	1

IV. COMPARISON OF AIDA VARIANTS

In the previous section the algorithm to find an AIDA required that the random numbers be shared anonymously at step. We now look at three methods which are variants of that procedure. The parameter S must be chosen in each case. The expected number of rounds depends only on the selection of S and not on the variant chosen.

A. Prime Modulus AIDA

A prime is chose. Generally, will be chosen as small as possible subject to this restriction. The random numbers chosen are distributed at step (3) using the field to compute the required power sum, the Newton polynomial, and the polynomial roots. This variant will be seen to result in shorter message lengths for communication between nodes. Again, the computation required to find the roots of the Newton polynomial is addressed. However, note that this computation can be delayed and thus overlaps any additional required rounds.

Additional rounds of the AIDA algorithm can proceed almost immediately as it is not necessary to solve before proceeding to the next round. Each node merely computes the derivative polynomial and evaluates that polynomial at its chosen random value.

V. ALGEBRAIC COMPLETION STATISTICS

For many purposes, the formulae of Section VII provide a satisfaction answer. However, the rich literature on absorbing Markov chains and the availability of computer algebra packages provide many other possibilities for analysis. To determine a desirable value for the number of slots " S=S " one can take advantage of the fact that the probabilities are representable as rational functions of the number of slots . In fact is the by the upper, left-hand corner of an infinite matrix. When is small, the entries, which have no discernible patterns, can be calculated by a computer algebra package from the recurrence relations yielding:

VI. FINITE TERMINATION

Although the algorithms developed here terminate with probability 1, there is never absolute upper bound on the number of rounds required. Under some assumption, it has been proven that finite termination cannot be guaranteed for the simpler leader election issue. While there may be extreme conditions under which no algorithm for AIDA can be guaranteed to finitely terminate, we conjecture only that at least sequential communications are required in such an algorithm. On the other hand, the algorithms of ,are already no collision , but do not generate a permutation chosen at random from all possible permutations. For the current problem, the number of rounds is typically small and we do not recommend seeking finitely bounded termination.

For completeness, we sketch a cryptography approach,that could guarantee finitely bounded termination, even without a trusted authority.

VII. CONCLUDING REMARKS

Each algorithm compared in Section VI can be reasonably implemented and each has it is advantages. Our use of the Newton identities greatly decrease the communication overhead. That can enable the use of a larger number of "slots" with a consequent reduction in the number of round is required. The solution of a polynomial can be avoided at some expense by using Sturms theorem. The development of a result similar to the Sturm's method over a finite field is an enticing possibility.

REFERENCES

[1] D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms," Commune. ACM, vol. 24, Feb. 1981.
[2] R. Canetti, "Security and composition of multi-party cryptographic protocols," vol. 13, no. 1, 2000.
[3] A.Shamir, "How to share a secret," Commun. ACM, vol. 22, 2005.
[4] W. Fokkink and J. Pang, "Variations on leader election for anonymous rings and their analysis in prism,", vol. 12, no. 8, Aug. 2006.
[5] A. Friedman, R. Wolff, and A. Schuster, "Providing k-anonymity in Data mining,"VLDB Journal, vol. 17, Jul. 2008.
[6] J. Smith, "Distributing identity," IEEE 2009.
[7] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," 2009.
[8] D. Jana, A. Chaudhuri, and B. B. Bhaumik, "Privacy and anonymity protection in computational grid services," 2010.
[9]Q.Xie and U.Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," Jul. 2011.
[10] J. W. Yoon and H. Kim, "A perfect collision-free pseudonym system,"IEEE, vol. 15, no. 6, pp. 686–688, Jun. 2011.
[11] J. Wang, T. Fukasama, S. Urabe, and T. Takata, "A collusion-resistant approach to privacy-preserving distributed data mining," Jan 2013.