This server is overloaded. Try the backup server.

ISIT 2011

#1569419785: *On Unconditionally Secure Multi-Party Sampling from Scratch*

Property	Change Add	Value
Conference and *track*		**2011 IEEE International Symposium on Information Theory** - *2011 IEEE International Symposium on Information Theory*
Authors		Ye Wang 198847 Boston University yw@bu.edu USA Prakash Ishwar 102858 Boston University pi@bu.edu USA
Presenter		presenter not specified
Registration		+
Category		Eligible for ISIT Student Paper Award
Title		*On Unconditionally Secure Multi-Party Sampling from Scratch*
Abstract		In the problem of secure multi-party sampling, n parties wish to securely sample an n-variate joint distribution, with each party receiving a sample of one the correlated variables. The objective is to correctly produces the samples using a distributed message passing protocol, while maintaining privacy against a coalition of passively cheating parties. In the two-party case, we fully characterize the joint distributions that can be securely sampled under perfect correctness and privacy requirements as well as under weakened correctness and privacy requirements. Furthermore, we show that the distributions that can be securely sampled can be produced with a protocol that only uses one round of unidirectional communication. For the n-party case, any distribution can be securely sampled with privacy against a strict minority coalition, due to well-known results in secure multi-party computation. However, when privacy against a majority coalition is required, not all distributions can be securely sampled. We give necessary conditions and sufficient conditions for distributions that can be securely sampled. However, the exact characterization of the distributions that can be securely sampled remains open.
Keywords		secure multi-party computation; secure sampling; unconditional security; common information
Topics		Cryptography and data security
Session		The program is not yet visible (tpc)
DOI		
Status		accepted

Document (show)	Pages	File size	Changed	MD5	Similarity score
Review manuscript	5	142,142	February 15, 2011 23:07:34 EST	f5d82c812d65571334c93f18283d9234	9

Final manuscript — Can upload 5 pages until May 31, 2011 00:00:00 EDT.

Personal notes

+

Reviews

You are a TPC member for this conference.

2 Reviews

Review 1 (Reviewer D)

Importance	Technical Level	Novelty	Presentation	Recommendation
Very Important (4)	Good technical level (4)	Very Novel (4)	Excellent (5)	Strongly Recommend (5)

Strengths (What are the key strengths of this paper?)

Technical rigor and the intuitiveness of the result even though the derivation is not light.

Weaknesses (What are the major weaknesses of this paper?)

The paper solves a problem that, at first glance, is a bit obscure. While prior work was cited, it would be much more enlightening to motivate the work with a real application, i.e., under want scenario do we need multiparty secure computation.

Comments and Recommendation (Please give the reasoning for your overall recommendation and any additional comments you wish to add.)

Paper is well written and the results appear quite intuitive. A few comments:

1. Corollary 1 and the remarks afterwards. As the three notions of common information equals when X1 and X2 (or after suitable transformation) are essentially groups of three independent sources, e.g., X1=(U,V), X2=(U,W) with U, V, W independent, it would be rather informative to use this case as an illustration as to why two party sampling with perfect security is feasible (which becomes apparent in light of the definition of privacy). Also, Lemma 2 becomes rather intuitive for this example with Y=U.

2. The reviewer is not familiar with the topic but it occurs to the reviewer that the message size seems to incur no penalty at all in the formulation?

3. Consider now the problem of, instead of sampling one set of data, sampling i.i.d. sequences at different parties with similar privacy constraints. Would the same solution apply for each snapshot?

4. First sentence of last paragraph: please rephrase to make it more clear that Theorem 3 gives necessary and Theorem 4 gives sufficient conditions.

For TPC eyes only (Write here if you have comments you don't wish the author to see.)

None.

Student Paper Award (This paper is eligible for the student paper award. Do you think it would rank among the top ten papers out of the 500 submitted papers in that category? If so, explain why.)

A strong paper but the reviewer doesn't have a good sample size to rank it.

Review 2 (Reviewer B)

Importance	Technical Level	Novelty	Presentation	Recommendation
Average Importance (3)	Technically sound (3)	Average Novelty (3)	Good (4)	Recommend (4)

Strengths (What are the key strengths of this paper?)

This paper addresses secure multiparty sampling. A set of terminals wish to sample from a given multivariate distribution. They have access to their local randomness (assumed independent of each other) and they can interactively communicate with each other. The objective is to keep the sampling secure, i.e., given the local random variable sampled at a terminal, all the other random variables should be independent of the observations of the terminal. This security condition must also hold for different coalitions (of size bounded by a given c) between the terminals. For the two terminals case the paper gives a simple characterization of the distributions that can be thus securely sampled. For the general case of multiple-terminals, necessary and sufficienct conditions for feasibility of secure sampling are given.

The presentation is very clear and convincing. The proof is based on a observation (reported as Lemma 2) that relates secure sampling condition to difference between W(X;Y) and I(X;Y), which is intuitively appealing.

Weaknesses (What are the major weaknesses of this paper?)

One weakness of the paper is that it reports very initial results and does not go beyond what was clear once Lemma 2 was observed. But perhaps the general problem (of multiparty secure sampling) is much harder.

Comments and Recommendation (Please give the reasoning for your overall recommendation and any additional comments you wish to add.)

I liked the overall presentation. Here are some minor comments:

1.) In the introduction, the term "common information" is used without explaining if it is Wyner's CI or Gacs-Korner CI or some other notion. Maybe it is better to replace it with Wyner's CI as that is the prevalent notion in the paper.

2.)In pg. 2, col 1., line 6:"from the measurement of the setup to the measurement of the output of the protocol". I could not make any sense of it. Perhaps rephrasing is required.

3.) In all the inequalities used in the proofs, please be consistent with the order of terms. It is irritating to see the order changing between lines.

4.) In Theorem 3, \overline{T} is not defined.

5.) Pg. 5, column 2, last line before the last equation,say: "the privacy condition is same as the given condition".

1 Summary review by TPC member

Review 1 (Reviewer A)

TPC recommendation
Strong accept (5)

TPC Recommendation Justification (Please give a justification for your recommendation, especially if the review scores vary widely or your recommendation differs significantly from those of the reviewers.)

A strong and nicely written paper in which multiple parties
seek to sample securely a joint distribution with each part producing
its own sample. Distributed communication with local randomization
are used to this end. The two-party case is fully resolved. Results are
also given for the case with more than two parties with security from
a strict minority or majority coalitions.

A question for the authors: Will their results continue to hold if the
notion of correctness were defined in the (stronger) sense of
KL-divergence rather than variational distance?

For TPC eyes only (Write here if you have comments you don't wish the author to see.)

A strong and well-written paper. An easy accept.
This paper is deserving of the Student Paper Award,
for which I shall submit a separate nomination.

Discussion

Not a reviewer.
Apr 16, 2011 04:18

A TPC MEMBER SUBMITTED THE FOLLOWING NOMINATION OF THIS PAPER FOR THE STUDENT PAPER AWARD:
The authors consider the problem of secure multiparty sampling in which n parties seek to produce an n-variate joint distribution with each party
generating a component random variable, by means of distributed communication among themselves. It is required that the communication be such that it
maintains ``privacy'' in the sense that any coalition of a restricted size cannot infer untoward information regarding sample random variables
generated by noncoalition members.

The authors resolve fully the problem with two parties to show that a bivariate distribution can be securely sampled if and only if the associated
random variables are such that their Wyner common information equals their mutual information. (It is known that mutual information cannot exceed
Wyner common information, in general.) The authors proceed to a model with an arbitrarily number n of terminals and show that an n-variate
distribution can always be sampled securely so as to provide security against a strictly minority coalition. The case of security against a majority
coalition is not fully resolved, and necessary and sufficient conditions for secure sampling are provided.

This paper is a strong contribution to the field of secure function
computation which is at the intersection of information theory and theoretical computer science. It has three commendable attributes. First, it
presents fundamental limits and brings together in a pleasing way the problem of secure computation and reveals points of contact with the classic
notions of
Gacs-Korner common information and Wyner information. Second, the proofs of achievability contain algorithmic structures that are of independent
interest. And, third, the paper is elegantly written.
