Multiparty Computation with Faulty Majority*

Donald Beaver
Harvard University

Shafi Goldwasser
MIT

Abstract. We address the problem of performing a multiparty computation when more than half of the processors are cooperating Byzantine faults. We show how to compute any boolean function of n inputs distributively, preserving the privacy of inputs held by nonfaulty processors, and ensuring that faulty processors obtain the function value "if and only if" the nonfaulty processors do. If the nonfaulty processors do not obtain the correct function value, they detect cheating with high probability. Our solution is based on a new type of verifiable secret sharing in which the secret is revealed not all at once but in small increments. This slow-revealing process ensures that all processors discover the secret at roughly the same time. Our solution assumes the existence of an oblivious transfer protocol and uses broadcast channels. We do not require that the processors have equal computing power.

1 Introduction

Consider a network of n processors, each holding a private input x_i. Given a function $f(x_1, \ldots, x_n)$, the processors must compute f while maintaining the privacy of the local inputs. The problem of achieving correct and private computation of f in the presence of malicious processor faults has recently received much attention in [10], [5], [6]. [1], [3], [2] , [7], [4] among others.

In this paper we consider the case that *more than half* the network consists of cooperating Byzantine faults. The faulty processors are allowed probabilistic polynomial time. We assume broadcast channels are available. Our main result is a completeness theorem for multiparty boolean protocols tolerating any number of faults.

Let n be the total number of players in the network and $t \leq n$ be the number of faulty players. Let $f : D_1 \times \cdots \times D_n \rightarrow GF(2)$ be any polynomial-time boolean function.Our solution satisfies four essential properties (formal definitions can be found in the full version of the paper in the proceedings of FOCS89.):

- **Independence of Inputs:** The faulty players choose and commit to their inputs x_i independently of the honest players inputs.
- **Privacy:** At the the end of the execution of the protocol, t Byzantine faults cannot to compute any more information about honest players inputs than already implied by the faulty players' private inputs and outputs.

[1]The first author was supported in part under NSF grant CCR-870-4513. The second author was supported in part by NSF grant CCR-8657527 with IBM matching funds, and US-Israel binational grant. A full version of the paper appears in the proceeding of the FOCS89 conference.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 589-590, 1990.

- **Validity:** The honest players will either output the value CHEATING (if the number of active Byzantine faults is greater than $n - t$), or output v such that $v = f(x_1, ..., x_n)$.
- **Fairness:** The speed in which the faulty players and the non-faulty players learn the result of the computation is the same (at any time duing the of the computation.)

Theorem 1 *Let f be a boolean function of n variables represented by a polynomial size arithmetic circuit family. Let the number of faults t satisfy $t < n$. Assume that a protocol for two party oblivious transfer exists. Then there exists a protocol to compute f which achieves independence of inputs, privacy, validity and fairness.*

The assumption of an oblivious transfer protocol is necessary.

Acknowledgements Many friends helped us, especially in discussions on the nature of fairness. We are particularly grateful to Richard Cleve, Oded Goldreich and Yishai Mansour. The observations about the necessity of an oblivious transfer protocol were obtained with Yishai. Thanks also to Benny Chor (via Otto), Phil Klein, Nati Linial, and Ron Rivest.

References

[1] M. Ben-Or, S. Goldwasser, A. Wigderson. "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation." Proc. of 20^{th} STOC (1988), 1-10.

[2] M. Ben-Or, T. Rabin. "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority." Proc. of 21^{st} STOC (1989).

[3] D. Chaum, C. Crépeau , I. Damgård . "Multiparty Unconditionally Secure Protocols." Proc. of 20^{th} STOC (1988), 11-19.

[4] D. Chaum. "Multi Party Protocols with Disruptors and Colluders." CRYPTO88 Rump Session.

[5] Goldreich, O., Micali, S., A. Wigderson. "How to Play Any Mental Game, or A Completeness Theorem for Protocols with Honest Majority." Proc. of 19^{th} STOC (1987), 218-229.

[6] Z. Galil, S. Haber, M. Yung. "Cryptographic Computation: Secure Faulty-Tolerant Protocols and the Public Key Model." Proc. of CRYPTO 1989.

[7] J. Kilian. "Founding Cryptography on Oblivious Transfer." Proc. of 20^{th} STOC (1988), 20-29.

[8] M. Luby, S. Micali, C. Rackoff. "How to Simultaneously Exchange a Secret Bit by Flipping a Symmetrically Biased Coin." Proc. of 24^{th} FOCS (1983).

[9] A. Shamir. "How to Share a Secret." CACM 22 (1979), 612-613.

[10] A. Yao. "How to Generate and Exchange Secrets." Proc. of 27^{th} FOCS (1986), 162-167.