Efficient Multi-Party Computation Secure Against a Faulty Minority

(Extended Abstract)

Martin Hirt Jesper Buus Nielsen

ETH Zurich

July 12, 2004

Abstract

We consider the communication complexity of secure multi-party computation protocols in the cryptographic model. In this model, the adversary is allowed to corrupt up to t of the n players, for any $t < n/2$.

The most efficient protocol known for this model requires $\Omega(cn^4\kappa)$ bits of communication for securely evaluating a circuit of size c, where κ denotes a security parameter [CDN01]. We present a new protocol for the same task, which communicates only $\mathcal{O}(cn^2\kappa + n^4\kappa)$ bits.

The proposed protocol combines techniques from the multi-party protocol based on homomorphic encryption [CDN01] with those from the player elimination framework [HMP00].

1 Introduction

The goal of secure multi-party computation is to enable a set of n players to evaluate an agreed circuit in a secure way, where every player holds some input, and every player shall receive some output (see e.g. [Yao82, GMW87, BGW88, CCD88, RB89, Bea91b]).

Since several years, the communication complexity of such protocol is of particular interest. There are two main streams of research in this direction: Protocols considering the round complexity [BB89, BFKR90, FKN94, IK00], and protocols considering the bit complexity [FY92, GRR98, HMP00, CDN01, HM01]. We focus on the latter.

2 Approach

We apply techniques from the player elimination framework [HMP00] to the multi-party protocol of [CDN01].

In [CDN01], a multi-party computation protocol based on a homomorphic public-key encryption scheme is proposed. The players jointly generate the keys such that the public key is commonly known but the secret key is shared among the players. Then, every player encrypts his input and broadcasts this encryption. Afterwards, the players jointly compute encryptions of all intermediate results in the circuit (i.e., the values on the wires). Finally, the outputs of the circuits are jointly decrypted.

The key idea of the player elimination framework [HMP00] is to eliminate misbehaving players from the further protocol execution, and thus preventing them from disturbing (and slowing down) the protocol execution more than once. As misbehavior can in general not be localized exactly (rather there will be a dispute and mutual accusations among two players), a set of players is eliminated with the only guarantee that at least half of the players in the set are faulty players. This technique has proven to be effective in a setting with $t < n/3$, as the non-eliminated players jointly know all intermediate results and hence can go on with the protocol execution after a set of players has been eliminated.

However, in a setting with faulty minority (i.e., $t < n/2$), the non-eliminated players do not necessarily jointly know the so-far computed intermediate results. As an illustrating example, consider $n = 2t + 1$ and a set of $2t$ players to be eliminated. Evidently, the single remaining player does not know the intermediate values of the protocol (this would violate privacy), and hence the protocol cannot be continued after players are eliminated, but must be restarted.

We overcome this problem by using some enhanced techniques: First, the protocol is divided into two parts, a preparation part and a evaluation part [Bea91a]. In the preparation part, a bunch of encrypted triples is generated, where the third value is the product of the first two values. In the evaluation part, the effective circuit is evaluated by using these triples. The evaluation part will be robust, i.e., misbehaving players cannot disturb. The preparation part will be designed in such a way that even when players get eliminated, the so-far prepared values can still be used.

3 Results

As main result, the proposed protocol achieves a total communication complexity of $\mathcal{O}(cn^2\kappa + n^4\kappa)$ bits. This improves on the most efficient protocol for $t < n/2$ known so far [CDN01] by a factor of n^2 for large circuits (at least n^2 gates).

References

[BB89] Judit Bar-Ilan and Donald Beaver. Non-cryptographic fault-tolerant computing in a constant number of rounds of interaction. In *Proc. 8th*

ACM Symposium on Principles of Distributed Computing (PODC), pages 201–210, August 1989.

[Bea91a] Donald Beaver. Efficient multiparty protocols using circuit randomization. In *Advances in Cryptology — CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 420–432, 1991.

[Bea91b] Donald Beaver. Secure multiparty protocols and zero-knowledge proof systems tolerating a faulty minority. *Journal of Cryptology*, pages 75–122, 1991.

[BFKR90] Donald Beaver, Joan Feigenbaum, Joe Kilian, and Phillip Rogaway. Security with low communication overhead. In *Advances in Cryptology — CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*. Springer-Verlag, 1990.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proc. 20th ACM Symposium on the Theory of Computing (STOC)*, pages 1–10, 1988.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proc. 20th ACM Symposium on the Theory of Computing (STOC)*, pages 11–19, 1988.

[CDN01] Ronald Cramer, Ivan Damgård, and Jesper B. Nielsen. Multiparty computation from threshold homomorphic encryption. In *Advances in Cryptology — EUROCRYPT '01*, Lecture Notes in Computer Science, 2001.

[FKN94] Uri Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation. In *Proc. 26th ACM Symposium on the Theory of Computing (STOC)*, pages 554–563, 1994.

[FY92] Matthew K. Franklin and Moti Yung. Communication complexity of secure computation. In *Proc. 24th ACM Symposium on the Theory of Computing (STOC)*, pages 699–710, 1992.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game — a completeness theorem for protocols with honest majority. In *Proc. 19th ACM Symposium on the Theory of Computing (STOC)*, pages 218–229, 1987.

[GRR98] Rosario Gennaro, Michael O. Rabin, and Tal Rabin. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In *Proc. 17th ACM Symposium on Principles of Distributed Computing (PODC)*, pages 101–111, 1998.

[HM01] Martin Hirt and Ueli Maurer. Robustness for free in unconditional multi-party computation. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO '01*, volume 2139 of *Lecture Notes in Computer Science*, pages 101–118. Springer-Verlag, August 2001.

[HMP00] Martin Hirt, Ueli Maurer, and Bartosz Przydatek. Efficient secure multi-party computation. In Tatsuaki Okamoto, editor, *Advances in Cryptology — ASIACRYPT '00*, volume 1976 of *Lecture Notes in Computer Science*, pages 143–161. Springer-Verlag, December 2000.

[IK00] Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *Proc. 41st IEEE Symposium on the Foundations of Computer Science (FOCS)*, October 2000.

[RB89] Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proc. 21st ACM Symposium on the Theory of Computing (STOC)*, pages 73–85, 1989.

[Yao82] Andrew C. Yao. Protocols for secure computations. In *Proc. 23rd IEEE Symposium on the Foundations of Computer Science (FOCS)*, pages 160–164. IEEE, 1982.