# Impossibility of Secure Multi-Party Products in Non-Abelian Groups*

Jessica Covington[1], Megan Golbek[2] and Mike Rosulek[3]

[1]College of Charleston, covingtonjg@g.cofc.edu
[2]University of California, San Diego, mgolbek@ucsd.edu
[3]Oregon State University, rosulekm@eecs.oregonstate.edu

**Abstract**

Suppose $n$ parties have respective inputs $x_1, \ldots, x_n \in \mathbb{G}$, where $\mathbb{G}$ is a finite group. The parties would like to privately compute $x_1 x_2 \cdots x_n$ (where multiplication refers to the group operation in $\mathbb{G}$). There is a well-known secure protocol that works for any number of parties $n$ when $\mathbb{G}$ is abelian. In this note we consider private group-product protocols for *non-abelian* groups. We show that such protocols are possible for if and only if $n$ (the number of parties) is less than 4.

## 1 Introduction

In a *multi-party group product protocol*, $n$ parties have respective inputs $x_1, \ldots, x_n$ from some group $\mathbb{G}$ (written multiplicatively), and interact to learn the group-product $\prod_i x_i$, without revealing any additional information about the inputs.

Benaloh [Ben87] introduced the notion of homomorphic secret sharing, which lends itself to a natural secure protocol for multi-party group product. If the $n$ parties have private inputs $x_1, \ldots, x_n$, then they can securely compute the product $\prod_i x_i$ as follows:

- Each party $P_i$ chooses a random secret sharing $\{x_{i,j}\}_j$ of their input $x_i$, such that $x_i = x_{i,1} x_{i,2} \cdots x_{i,n}$. Party $P_i$ then privately sends $x_{i,j}$ to party $P_j$.
- Each party $P_i$ has now received a share $x_{j,i}$ from each party $P_j$. Party $P_i$ broadcasts $y_i = x_{1,i} x_{2,i} \cdots x_{n,i}$.
- From these broadcasts, all parties can compute the final output $\prod_i y_i$.

When the underlying group is abelian, the protocol is correct because:

$$\prod_i y_i = \prod_i \left( \prod_j x_{j,i} \right) = \prod_j \left( \prod_i x_{j,i} \right) = \prod_j x_j$$

The fact that the shares-of-shares are homomorphic implies that the protocol is secure, and leaks no more than the desired product.

However it is not clear how to adapt the approach for a non-abelian group. Yet non-abelian groups (e.g., permutations or matrices) are common and fundamental in many applications. In this work we show that secure multi-party group products in non-abelian groups are possible only with 3 or fewer parties.

*Work done while first two authors were participants in an NSF REU Site program at Oregon State University (#1359173)

**Other related work** Frankel, Desmedt & Burmester [FDB93] find that homomorphic secret sharing does not exist for non-abelian groups. This implies that a straight-forward adaptation of Benaloh's product protocol is impossible for non-abelian groups. But it does not rule out the possibility of some other way of securely computing a multi-party group product.

# 2 Preliminaries

## 2.1 Semi-Honest Security for MPC

In this work we use the standard simulation-based definition of security in the presence of semi-honest adversaries. We consider adversaries that corrupt *any* number of parties; *i.e.*, we do not restrict to the honest majority setting. Indeed, in the honest majority setting, it is well-known that *every* function can be securely realized [BOGW88, CCD88].

**Definition 1.** *Let $\pi$ be an $n$-party protocol, and let $S \subseteq \{1, \ldots, n\}$ be a set of parties.*

*Then $\text{VIEW}_S^\pi(1^\kappa, x_1, \ldots, x_n)$ denotes the random variable describing the (joint) view of parties $\{P_i \mid i \in S\}$ in an execution of $\pi$ on inputs $x_1, \ldots, x_n$. This view consists of (1) The inputs of these parties: $\{x_i \mid i \in S\}$, (2) the random tapes of these parties, (3) all protocol messages sent from $P_i$ to $P_j$ for $i \notin S$ and $j \in S$.*

In the following definition, let $\Delta(\mathcal{A}, \mathcal{B})$ denote the statistical distance between two distributions $\mathcal{A}$ and $\mathcal{B}$.

**Definition 2.** *An $n$-party protocol $\pi$ for function $f$ is **secure** in the presence of semi-honest adversaries if there exists a simulator $\mathsf{Sim}$ such that for all $S \subseteq \{1, \ldots, n\}$ and all inputs $x_1, \ldots, x_n$, the following quantity is negligible in $\kappa$.*

$$\Delta\Big(\text{VIEW}_S^\pi(1^\kappa, x_1, \ldots, x_n),\ \mathsf{Sim}(1^\kappa, S, \{x_i \mid i \in S\}, f(x_1, \ldots, x_n))\Big)$$

*In other words, the view of (corrupt) parties $S$ can be simulated given given only their inputs and the output of $f$.*

## 2.2 Characterization of 2-party MPC

In concurrent works [Bea89, Kus89], Beaver & Kushilevitz characterized the 2-party functions that have secure protocols (in the presence of semi-honest adversaries). The characterization holds for protocols with *perfect* security (i.e., the simulated views and real views are *identically* distributed). The same characterization was later extended to the case of statistical security in [MPR09].

**Definition 3.** *Let $f : X \times Y \to Z$ be a 2-party function. Then $f$ is **decomposable** if:*

- *$f$ is constant function over $X \times Y$*
- *Or, there is a partition $X = X_1 \cup X_2$ such that:*
  - *For all $x_1 \in X_1, x_2 \in X_2, y \in Y$ we have $f(x_1, y) \neq f(x_2, y)$*
  - *The restrictions $f_1 : X_1 \times Y \to Z$ and $f_2 : X_2 \times Y \to Z$ are decomposable.*
- *Or, there is a partition $Y = Y_1 \cup Y_2$ such that:*
  - *For all $x \in X, y_1 \in Y_1, y_2 \in Y_2$ we have $f(x, y_1) \neq f(x, y_2)$*

– *The restrictions $f_1 : X \times Y_1 \to Z$ and $f_2 : X \times Y_2 \to Z$ are decomposable.*

**Theorem 4** ([Bea89, Kus89, MPR09])**.** *Let $f$ be a 2-party function. There is a secure protocol (against semi-honest adversaries) for $f$ if and only if $f$ is decomposable.*

## 3 Three-party Non-abelian Group Products

Let $\mathbb{G}$ be an associative but not necessarily abelian group, which we write with multiplicative notation. In Figure 1 we present an extremely simple protocol for 3-party group product $(a, b, c) \mapsto abc$.

**Parameters:** multiplicative group $\mathbb{G}$
**Inputs:** Parties $P_1, P_2, P_3$ have inputs $a, b, c \in \mathbb{G}$, respectively.

**Protocol:**
1. $P_1$ chooses $r \leftarrow \mathbb{G}$ and sends $s = ra$ to $P_2$
2. $P_2$ sends $t = sb$ to $P_3$
3. $P_3$ sends $u = tc$ to $P_1$
4. $P_1$ broadcasts $v = r^{-1}u$ to all parties
5. All parties output $v$

Figure 1: 3-party group-product protocol for non-abelian $\mathbb{G}$

**Lemma 5.** *The protocol in Figure 1 is secure against semi-honest adversaries.*

*Proof.* Correctness of the protocol follows from the associativity of the group. All parties output:

$$v = r^{-1}u = r^{-1}(tc) = r^{-1}(sb)c = r^{-1}(ra)bc = abc.$$

Note that given $abc$ and any two of $\{a, b, c\}$, it is possible to solve for the missing input. (This argument does not require the group to be abelian.) Hence, security in the presence of two corrupt parties is trivial, since they are allowed to learn the honest party's input.

We therefore focus on the case of a single corrupt party. The protocol is asymmetric with respect of the parties' roles, so the analysis proceeds in 3 distinct cases:

- $P_1$'s view consists of its input $a$, its randomness $r \in \mathbb{G}$, and a protocol message $u = rabc$. This joint distribution can be perfectly simulated given just the ideal view $(a, v = abc)$ by sampling random $r$ and setting $u = rv$.

- $P_2$'s view consists of its input $b$ and messages $s = ra$ and $v = abc$ from $P_1$. This joint distribution can be perfectly simulated in the ideal world by sampling $s$ uniformly. The distributions are identical because in any group the distribution over $ra$ for uniform $r$ and *any fixed* $a$ is uniform.

- $P_3$'s view consists of its input $c$ and messages $t = rab$ from $P_2$ and $v = abc$ from $P_1$. This joint distribution can be perfectly simulated in the ideal world by sampling $t$ uniformly. □

**Related work.** Another way to derive a secure protocol for 3-party product in a non-abelian group is as follows: First, observe that for *every* 3-party function, there is a secure protocol that tolerates a *single* corrupt party [BOGW88, CCD88]. But in the case of 3-party group product, such a protocol will also be secure in the presence of 2 corrupt parties. This follows from the argument used in the above proof, that 3-party group product has no privacy requirement in the case of 2 corrupt parties.

Of particular interest are protocols from the line of work on MPC over black-box groups [DPSW07, DPS+12, CDI+13]. In these works, the parties securely evaluate an arithmetic circuit expressed in terms of operations in a (possibly non-abelian) group. Clearly group product can be expressed in such a way. Importantly, these results would yield a protocol that treats the group itself as a black-box; i.e., the protocol is in some sense "the same" for any group.

# 4 Impossibility of Non-abelian Group Product for $n \geq 4$

We now show that secure $n$-party group products are not possible for $n \geq 4$, unless the group is abelian. We leverage the characterization of 2-party secure MPC from Section 2.2 and use the following simple observation:

**Proposition 6.** *Let $f$ be an $n$-party function. If there is a secure protocol for $f$ then for any $S \subseteq \{1, \ldots, n\}$ there is a secure protocol for the 2-party function*

$$f_S\Big(\{x_i \mid i \in S\}, \{x_i \mid i \notin S\}\Big) = f(x_1, \ldots, x_n)$$

**Theorem 7.** *If there is a protocol for 4-party $\mathbb{G}$-product, secure in the presence of semi-honest adversaries, then $\mathbb{G}$ is abelian.*

*Proof.* By partitioning the parties into two sets, we obtain a secure 2-party protocol for the function $f\Big((a,c),(b,d)\Big) = abcd$ where $a, b, c, d \in \mathbb{G}$. The function $f$ is therefore decomposable.

Each step in the decomposition is associated with a restriction of $f$ to domain $X \times Y$, where $X, Y \subseteq \mathbb{G}^2$. We claim that for each such step in the decomposition, the following properties hold:

$$\begin{aligned} \forall a \in \mathbb{G}: &\text{ there is an element of the form } (a, \cdot) \in X \\ \forall b \in \mathbb{G}: &\text{ there is an element of the form } (b, \cdot) \in Y \\ (a,c) \in X &\implies (c,a) \in X \\ (b,d) \in Y &\implies (d,b) \in Y \end{aligned}$$

The claim is true for the top-most step of the decomposition because in that case $X = Y = \mathbb{G}^2$.

Now we proceed by induction and consider a decomposition step, in which $f : X \times Y \to \mathbb{G}$ is decomposed (without loss of generality) as $X = X_1 \cup X_2$. We will show that the inductive hypothesis holds with respect to $X_1$ — a symmetric argument holds with respect to $X_2$ (and for the case where the decomposition is on $Y$ instead of $X$). Start by taking an arbitrary $(a,c) \in X_1$.

- Take an arbitary $r \in \mathbb{G}$, and (by the inductive hypothesis on $Y$) any element of the form $(1,d) \in Y$ (where 1 refers to the identity in $\mathbb{G}$). Observe that

  $$f\Big((a,c),(1,d)\Big) = acd = a(rr^{-1})cd = (ar)1(r^{-1}c)d = f\Big((ar, r^{-1}c),(1,d)\Big)$$

  This implies that $(a,c)$ and $(ar, r^{-1}c)$ must be in the same part $X_1$ of the decomposition. Hence $X_1$ contains an element of the form $(ar, \cdot)$ for all $r \in \mathbb{G}$.

- By the inductive hypothesis on $Y$, take any element of the form $(a^{-1}, d) \in Y$. Observe that:

$$f\Big((a,c),(a^{-1},d)\Big) = aa^{-1}cd = cd = ca^{-1}ad = f\Big((c,a),(a^{-1},d)\Big)$$

  This implies that $(a,c)$ and $(c,a)$ must be in the same part $X_1$ of the decomposition. That is, $(c,a) \in X_1$ as well.

We now claim that $\mathbb{G}$ must be abelian. Take an arbitrary $s,t \in \mathbb{G}$. By the decomposability of $f$, there is a restriction $X \times Y \subseteq \mathbb{G}^2 \times \mathbb{G}^2$ where $(s,t) \in X$ and $(1,1) \in Y$ and $f$ is constant over $X \times Y$. By the property we just proved, we also have $(t,s) \in X$. Since $f$ is constant over $X \times Y$, we must have $f\Big((t,s),(1,1)\Big) = ts = st = f\Big((s,t),(1,1)\Big)$. Since this argument holds for arbitrary $s,t \in \mathbb{G}$, the group is abelian. □

**Corollary 8.** *If there is a protocol for $n$-party $\mathbb{G}$-product, secure in the presence of semi-honest adversaries, and $n \geq 4$, then $\mathbb{G}$ is abelian.*

*Proof.* Suppose there is such a protocol $\pi$ for $n \geq 4$ parties. Consider the following 4-party protocol $\pi'$: Each party simply runs $\pi$ on its input, except for $P_4$ who plays the role of parties $P_4, \ldots, P_n$ in $\pi$, and runs the parties $P_5, \ldots, P_n$ each with input $1 \in \mathbb{G}$. The resulting protocol $\pi'$ is a secure 4-party $\mathbb{G}$-product protocol, so $\mathbb{G}$ is abelian. □

## References


[Bea89] Donald Beaver. Perfect privacy for two-party protocols. In Joan Feigenbaum and Michael Merritt, editors, *Proceedings of DIMACS Workshop on Distributed Computing and Cryptography*, volume 2, pages 65–77. American Mathematical Society, 1989.

[Ben87] Josh Cohen Benaloh. Secret sharing homomorphisms: Keeping shares of a secret sharing. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 251–260. Springer, Heidelberg, August 1987.

[BOGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, May 1988.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *20th ACM STOC*, pages 11–19. ACM Press, May 1988.

[CDI+13] Gil Cohen, Ivan Bjerre Damgård, Yuval Ishai, Jonas Kölker, Peter Bro Miltersen, Ran Raz, and Ron D. Rothblum. Efficient multiparty protocols via log-depth threshold formulae - (extended abstract). In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 185–202. Springer, Heidelberg, August 2013.

[DPS+12] Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld, Xiaoming Sun, Christophe Tartary, Huaxiong Wang, and Andrew Chi-Chih Yao. Graph coloring applied to secure computation in non-abelian groups. *Journal of Cryptology*, 25(4):557–600, October 2012.

[DPSW07] Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld, and Huaxiong Wang. On secure multi-party computation in black-box groups. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 591–612. Springer, Heidelberg, August 2007.

[FDB93] Yair Frankel, Yvo Desmedt, and Mike Burmester. Non-existence of homomorphic general sharing schemes for some key spaces (extended abstract). In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 549–557. Springer, Heidelberg, August 1993.

[Kus89] Eyal Kushilevitz. Privacy and communication complexity. In *30th FOCS*, pages 416–421. IEEE Computer Society Press, October / November 1989.

[MPR09] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 256–273. Springer, Heidelberg, March 2009.