Group Structure in Correlations and Its Applications in Cryptography

Guru-Vamsi Policharla
Indian Institute of Technology, Bombay, Mumbai, India

Manoj Prabhakaran
Indian Institute of Technology, Bombay, Mumbai, India

Rajeev Raghunath
Indian Institute of Technology, Bombay, Mumbai, India

Parjanya Vyas
Indian Institute of Technology, Bombay, Mumbai, India

Abstract

Correlated random variables are a key tool in cryptographic applications like secure multi-party computation. We investigate the power of a class of correlations that we term *group correlations*: A group correlation is a uniform distribution over pairs $(x, y) \in G^2$ such that $x + y \in S$, where G is a (possibly non-abelian) group and S is a subset of G. We also introduce bi-affine correlations, and show how they relate to group correlations. We present several structural results, new protocols and applications of these correlations. The new applications include a completeness result for black box group computation, perfectly secure protocols for evaluating a broad class of black box "mixed-groups" circuits with bi-affine homomorphisms, and new information-theoretic results. Finally, we uncover a striking structure underlying OLE: In particular, we show that OLE over $\mathbb{F}_{2^n}$, is isomorphic to a group correlation over $\mathbb{Z}_4^n$.

2012 ACM Subject Classification Security and privacy → Information-theoretic techniques

Keywords and phrases Group correlations, bi-affine correlations, secure computation

Digital Object Identifier 10.4230/LIPIcs.ITC.2021.1

Related Version *Full Version*: `https://eprint.iacr.org/2021/624`

Funding *Manoj Prabhakaran*: Manoj Prabhakaran was supported by the Joint Indo-Israel Project DST/INT/ISR/P-16/2017 and a Ramanujan Fellowship by the Dept. of Science and Technology, India.

Acknowledgements We thank Yuval Ishai and various anonymous reviewers for helpful comments and pointers.

1 Introduction

A central concept in secure multiparty computation (MPC) is that of correlated random variables. If Alice and Bob are given correlated random variables, they can later use them to securely compute any function, with information-theoretic security [22, 20]. This model has been a key ingredient in many theoretical and practical results in MPC. While the class of 2-party correlations that information-theoretically secure computation *can be* based on (i.e., "complete" correlations) is well-understood [23, 24], not all complete correlations *are* used in practical protocols. Instead, several "standard" correlations which have additional structure, like Oblivious Transfer (OT), Oblivious Linear function Evaluation (OLE) and Beaver's Multiplication Triplets (BMT) [2] are used in practice. The main motivation in this work is to systematically study the additional structure that protocols can exploit, and develop a deeper and broader foundation for such correlations.

Apart from uncovering the beautiful mathematical structures from which these correlations derive their power, another motivation for our work is to expand the applicability of correlated random variables to secure computation involving black-box algebraic structures which can be less structured than finite fields or rings. Consider the following seemingly disparate problems of information-theoretically secure 2-party computation:

- **Blackbox Group Computation:** If the function is given as a circuit over a blackbox (non-abelian) group, how can two parties securely compute it with *perfect security*? The complete correlation proposed in [10] (namely, oblivious transfer of group elements), yielded only statistical security.
- **Generating and Processing Correlations over a Blackbox Ring:** If correlated random variables over a blackbox ring (e.g., OLE) are acquired by a pair of parties from a trusted server, can they be efficiently *rerandomized* (e.g., for "forward security" against future corruption of the server)? Efficiency relates to both the use of correlations as well as communication and number of rounds.
  How efficiently can such correlations be generated, using a less structured primitive like string OT?
- **Circuits Using Alternate Algebraic Structures:** Traditionally, MPC literature has considered algebraic circuits to be over fields or rings, and these protocols breakdown if the algebraic structure underlying the circuit has less structure. Can alternate protocols be devised for computation over (say) distributive near-rings or non-associative algebras, or when multiple such algebraic structures are used in the same circuit?

We introduce *bi-affine correlations* as an abstraction of a broad class of cryptographically interesting correlations, and address all of the above problems in terms of them. Perhaps more importantly, we undertake a study of the fundamental properties of bi-affine correlations and the underlying mathematical structure of bi-affine homomorphisms, without being confined to immediate applications. This leads us to the definition of *Group Correlations* and *Subgroups Correlations* as a generalization of bi-affine correlations, that brings out additional hidden structure of bi-affine correlations.

Interestingly, while "additive correlations" (the abelian version of group correlations) and "bilinear correlations" (a special case of bi-affine correlations) have been explicitly considered before in various applications, most notably in the rich line of work on function/homomorphic secret-sharing (F/HSS) and pseudorandom correlation generators (PCG) [8, 9, 5, 7, 6],[1] it was not realized that the former is a generalization of the latter, underlining the need for studying them abstractly.

1.1 Our Contributions

We develop a theory of *group correlations* and *subgroups correlations*, with a focus on the subclass of bi-affine correlations. A group correlation, specified by a group G and a subset $S \subseteq G$, is simply an additive secret-sharing of a random element in S, or equivalently, a uniform distribution over $\{(x, y) \mid x, y \in G, x + y \in S\}$. A subgroups correlation is a restriction of such a group correlation correlation to the universe $G_1 \times G_2$ where G_1 and G_2 are subgroups of G, with a regularity condition on S (so that the resulting correlation has

[1] In these works, bi-linear correlations were often termed *simple bi-linear correlations*. For consistency with the terminology in the current work, we avoid this term. What was termed (general) bi-linear correlations there would correspond to correlations of the form $\mathsf{BA}_{\sigma^{(2)}}$ in this work.

uniform marginal distributions). Within this simple framework, a rich variety of structures arise based on how the groups and the set S are defined. Our contributions include the following:

- **A Theory of Group Correlations**: This includes several new definitions of structures and properties, as well as connections between them. (Section 3).
- **Information-Theoretic Results**: We give new results on information theoretic quantities (specifically, *residual information*) that can be used to analyze the optimality of secure protocols. (Section 4).
- **New Protocol Building-Blocks**: We present a suite of protocols for various functionalities involving bi-affine correlations, with applications to 2-Party secure computation. (Section 5).
- **Applications**: The above building-blocks can be put together to yield various information-theoretically secure computation protocols. In particular, we show:
  - There exists a *complete correlation* for 2-party *perfectly* passive-secure evaluation of a black-box (non-abelian) group circuit – called the Zero Alternating Sum (ZAS) correlation. ZAS is a bi-affine correlation, and hence this could seen as a special case of the following results. In contrast, previously the complete correlation proposed in [10] (namely, OT with group elements), yielded only statistical security.
    When the circuit has logarithmic depth, or is in the form of polynomial-sized formula, we obtain a 2-round UC secure protocol.
  - A GMW-style 2-Party protocol for evaluating a black-box "mixed-group circuit" with homomorphism and bi-affine homomorphism gates, which requires 2 rounds of interaction per layer.
  - 2-Party protocols for rerandomizing and testing bi-affine correlations obtained from a semi-trusted source (who will not collude with either party until after the protocol is over) (Section 5.1, Section 5.4). We also discuss how this can be viewed as a solution to sampling correlations in the single-server version of the commodity based model [4].
  - A 2-Party protocol for securely sampling bi-affine correlations using string OTs, generalizing a protocol of Gilboa [19]. Using our information-theoretic results, we establish its optimality for a class of bi-affine correlations (including the ones considered in [19]). (Section 5.3).
- **A Surprising Structure.** Finally, we uncover a striking structure underlying OLE. In particular, we show that OLE over $\mathbb{F}_{2^n}$, is isomorphic to a group correlation over $\mathbb{Z}_4^n$. Given that OLE has been widely studied and used, it is remarkable that such a structure has remained hidden so far.

Details of the protocols and applications can be found in the full version.

Discussion

Here we elaborate on some of the above contributions.

Hidden Structures. We point out two instances of hidden structure in well-studied objects that are revealed by our abstractions. OLE and BMT are two correlations that have been extensively studied both in terms of their applications, and in terms of protocols generating them. However, while abstracting them as bi-linear correlations (see Footnote 1), they are treated somewhat differently. For instance, in [5], PCGs for bi-linear correlations are given, which directly applies to OLE; and then a PCG for BMT is provided by reducing BMT to OLE. However, a consequence of our results is that BMT is already a (simple) bi-linear correlation, but with a bi-linear operator different from that of OLE: while OLE uses a

map $\sigma(a,b) = ab$, BMT uses $\sigma((a,b),(c,d)) = ad + bc$ (all variables belonging to a ring). This results in a more efficient protocol since reducing one BMT to two OLE correlations is wasteful (a reduction in the opposite direction is not possible).

The second instance of a hidden structure is that of OLE which has a complicated structure due to the interaction of field multiplication with the addition structure of the field. As such, one may not expect OLE (over large fields) to be a group correlation. But we show that every symmetric bi-affine correlation (of which OLE is an example) is in fact a group correlation. Even more surprisingly, for the special case of OLE over the field $\mathbb{F}_{2^n}$, the underlying group turns out to be $\mathbb{Z}_4^n$. Thus OLE over $\mathbb{F}_{2^n}$ can be seen as sampling an element uniformly from a (non-obvious) set $S \subseteq \mathbb{Z}_4^n$, and then simply additively secret-sharing it coordinate-wise. While we do not offer any immediate applications of this particular structure, as a fundamental property of an extremely useful cryptographic primitive, it is an interesting result.

ZAS: A Bi-Affine Correlation in a Group. An interesting application we present is that of a complete correlation for 2-party secure computation over a black-box group, with *perfect security*. In contrast to the prior approach which relied on OT with group elements, and only obtained statistically secure protocols [10], we rely on a deceptively simple correlation, called the Zero Alternating Sum (ZAS) correlation. In a ZAS correlation over a (non-abelian) group G, Alice and Bob get random pairs $(a,c) \in G^2$ and $(b,d) \in G^2$ such that $a + b + c + d = 0$.

Note that defining ZAS does not require anything more than the group operation. This demonstrates the generality of bi-affine homomorphisms, compared to bi-linear maps. While bi-linear maps are used to capture the multiplication operation in a *ring*, bi-affine homomorphisms can equally well capture the alternating sum structure in a group. Concretely, the function $\sigma : G^2 \to G^{\mathrm{op}}$, defined as $\sigma(x,y) = -(x+y)$ where G^{op} is the *opposite group* of G (whose group operation is the same as that of G, but applied to the operands in the opposite order), is a bi-affine homomorphism w.r.t. the subgroups $T = G \times \{0\}$ and $U = \{0\} \times G$ of the group G^2.

Optimality of Gilboa's Reduction. As a corollary of our information-theoretic results pertinent to bi-affine correlations, we show that Gilboa's reduction from OLE over $\mathbb{F}_{2^n}$ to string OT [19] is optimal in the number of string OTs used (n string OTs per OLE instance), and cannot be improved upon even with amortization. In fact, this extends to OLE over $\mathbb{F}_{p^n}$ if Gilboa's protocol is modified to use 1-out-of-p string OTs.

Mixed-Groups Circuit with Bi-Affine Homomorphism Gates. Conventionally, MPC literature has considered boolean or arithmetic circuits over a given ring or field. A variant of this considers the underlying algebraic structure to be given as a black box to the protocol (e.g., [11, 21] for rings and [17, 16, 10] for groups). Motivated by practical applications, MPC protocols for computation that uses multiple representations has received attention (e.g., the ABY framework [15] and subsequent works). More recently, circuits with bi-linear gates over multiple black box groups has been considered in [9].

Our applications use a similar circuit paradigm as [9], and use two types of gates (1) group operations (2) gates for group homomorphisms and bi-affine homomorphisms. Bi-Affine Homomorphisms are quite general, and can correspond to multiplication in distributive near-rings or non-associative rings, or even (negated) addition in a non-abelian group. As such, this is a powerful computational model that subsumes arithmetic circuits over a

ring. Nevertheless, the bi-affine homomorphism structure lets us build perfectly secure 2-party protocols for all such circuits, using bi-affine correlations for the corresponding bi-affine homomorphisms (if necessary, along with "Zero Alternating Sum" correlations for the non-abelian groups).

1.2 Related Work

Correlations have received much attention in cryptography, especially since Beaver's proposal of using them as cryptographic commodities [3] and the emergence of the pre-processing model as a common approach to theoretically and practically efficient MPC. They have been put to great use for MPC, both in the passive and active corruption settings, in theory and practice (see. e.g., the SPDZ family of protocols [14] and subsequent work). All these works develop and use several building blocks like self-reduction and self-testing for their correlations.

The recent line of works on Pseudorandom Correlation Generators and Function Secret Sharing [9, 5, 7, 8, 6], which consider bi-linear and additive correlations are most closely related to our work. Briefly, they answer two important questions. (1) how to perform secure computation over bi-linear gates (2) how to efficiently generate these correlations. In contrast to our work, these results were focussed on exploiting computational hardness, and restricted themselves to bi-linear correlations and abelian groups.

Secure Multi Party Computation over non-abelian Black-Box groups has been well studied in the honest-majority setting [17, 16, 10]. In the two-party setting Cohen et al. [10] gave a passive statistically secure protocol for evaluating circuits over black-box groups in the OT hybrid model and used the IPS compiler [20] to achieve security against active corruption. In this work, we use a stronger primitive – namely Zero Alternating Sum correlations – but are able to obtain a simple perfectly secure protocol against active adversaries without the use of expensive compilers for log-depth circuits.

Protocols for rerandomization and testing of correlations have appeared previously in the literature but their focus has remained on specific correlations such as BMT, squaring tuples etc., [13]. The commodity based model first introduced by Beaver in [4] has been revisited recently in [12, 27] to sample OLE and BMT correlations.

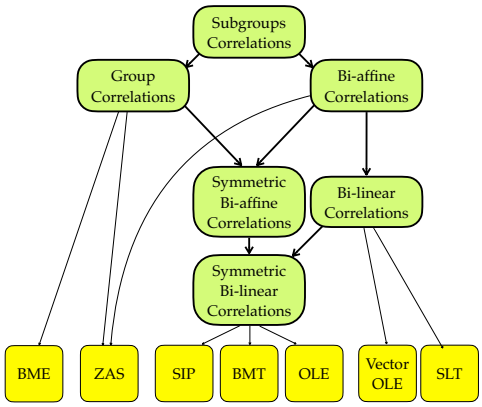
1.3 Technical Overview

In this section we present the highlights of our results, informally. Several additional technical details and generalizations are deferred to the subsequent sections and the full version.

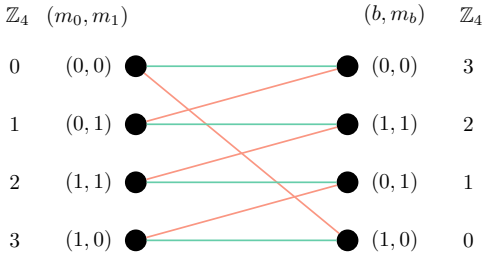
1.3.1 Definitions

We consider several classes of *flat* correlations – i.e., distributions that are uniform over their support. Below we use support and distribution interchangeably.

Group Correlations and Subgroups Correlations. A group correlation defined w.r.t a group G and a subset $S \subseteq G$ is the uniform distribution over all pairs $(g_1, g_2) \in G^2$ such that $g_1 + g_2 \in S$. A subgroups correlation *embedded in* this group correlation is obtained by requiring $g_1 \in G_1$ and $g_2 \in G_2$, where G_1, G_2 are subgroups of G with the property that the marginal distributions of g_1 and g_2 are both uniform. This subgroups correlation is said to be *compact* if $|G| < |G_1||G_2|$.



(a) A taxonomy of correlations.



(b) Bipartite graph of the OT correlation.

Bi-Affine Homomorphisms. A linear function (or a group homomorphism) $\phi : G \to H$ satisfies $\phi(a+b) = \phi(a) + \phi(b)$ (where the addition and subtraction are in the appropriate groups). An "affine" function ψ is such that ϕ defined by $\phi(x) := \psi(x) - \psi(0)$ is linear; i.e., $\psi(a+b) = \psi(a) - \psi(0) + \psi(b)$. A bi-affine function could be defined as a function of two inputs, which is affine in each of them; i.e., for groups T, U, H, a function $e : T \times U \to H$ such that

$$e(t, u+u') = e(t,u) - e(t,0) + e(t,u') \quad \text{and} \quad e(t+t', u) = e(t,u) - e(0,u) + e(t',u). \quad (1)$$

Note that if we required $e(t,0) = e(0,u) = 0$, then the conditions above would collapse to e being *bi-linear*. Examples of functions that satisfy (1) but are not bi-linear include $e : G \times G \to G$ defined as $e(a,b) = a + b$ or as $e(a,b) = -a - b$.

For notational simplicity in our results, we define a *bi-affine homomorphism* as a *unary* function $\sigma : Q \to H$, (Q, H being groups) with respect to subgroups $T, U \leqslant Q$ so that $e : T \times U \to H$ defined as $e(t,u) := \sigma(t+u)$ satisfies (1). An equivalent definition, in terms of group homomorphisms, is given in Definition 7.

Bi-Affine Correlation. Given a bi-affine homomorphism σ as above, the support of the corresponding bi-affine correlation correlation $\mathsf{BA}_\sigma \subseteq (T \times H) \times (U \times H)$ is defined as

$$\mathsf{BA}_\sigma = \{((t,a),(u,b)) \mid \sigma(t+u) = a + b\}.$$

Examples. As shown in Figure 1a, the most commonly used correlations indeed fall under the class of bi-affine correlations.

- Oblivious Linear Evaluation (OLE): Defined over a ring A as $\big((t,a),(u,b)\big)$ such that $a+b = tu$, OLE is isomorphic to a bi-affine correlation with $\sigma(t,u) = tu$, where $\sigma : A^2 \to A$ is a bi-affine homomorphism with respect to $T = A \times \{0\}$ and $U = \{0\} \times A$.
- Beaver's Multiplication Triples (BMT): Defined over a ring A as $\big((t_1,u_1,a),(t_2,u_2,b)\big)$ such that $a + b = (t_1 + t_2)(u_1 + u_2)$, BMT is isomorphic to a bi-affine correlation with $\sigma((t_1,u_1),(t_2,u_2)) = t_1u_2 + t_2u_1$, where $\sigma : A^4 \to A$ is a bi-affine homomorphism with respect to $T = A^2 \times \{0\}^2$ and $U = \{0\}^2 \times A^2$.
- Zero Alternating Sum (ZAS): Defined over a (possibly non-abelian) group D as $\big((a,c),(b,d)\big)$ such that $a + b + c + d = 0$, ZAS is isomorphic to a bi-affine correlation BA_σ, where $\sigma : D^2 \to D^{\mathrm{op}}$ defined as $\sigma(c,d) = -(c+d)$ is a bi-affine homomorphism with respect to $T = D \times \{0\}$ and $U = \{0\} \times D$.

Powers of a Bi-Affine Homomorphism. Given a bi-affine homomorphism $\sigma : Q \to H$ w.r.t. subgroups T, U, we can define new bi-affine homomorphisms as "powers" of σ. There are a few different useful notions of such powers that emerge in the sequel, which we call σ^n, $\sigma^{(n)}$ and $\sigma^{\langle n \rangle}$.

- $\sigma^n : Q^n \to H^n$ is simply the coordinate-wise application of σ.
- $\sigma^{(n)} : Q^n \to H^n$ corresponds to a "vector" variant of σ, generalizing how string-OT or vector-OLE are vector variants of OT and OLE respectively; it is in fact the same as σ^n, but considered as a bi-affine homomorphism w.r.t. T^n and $U^{(n)} = \{(u, \ldots, u) | u \in U\} \subseteq U^n$. $\mathsf{BA}_{\sigma^{(n)}}$.
- $\sigma^{\langle n \rangle} : Q^n \to H$ is an *inner-product* version of σ, generalizing how BMT is isomorphic to $\mathsf{BA}_{\sigma^{\langle 2 \rangle}}$, where σ is the multiplication in a ring (so that BA_σ corresponds to OLE over that ring).

There exists a non-interactive, UC-secure protocol to securely sample one instance of $\mathsf{BA}_{\sigma^{\langle \ell, m \rangle}}$ from $\ell + m$ instances of BA_σ. A special case of this protocol is the reduction of a BMT correlation to two OLE correlations. See full version for details.

1.3.2 Connections

We uncover some surprising connections between the different classes of correlations mentioned above (Theorem 9).

1. Every symmetric bi-affine correlation is a group correlation. In particular, OLE over a ring A is isomorphic to a group correlation w.r.t the group $\mathbb{K}_A$ over $A \times A$ whose group operation is defined as $(a, b) \odot (c, d) = (a + c, b + d - ac)$, and subset $S = \{(a, 0) \mid a \in A\}$.
2. Every bi-affine correlation is a *compact* subgroups correlation. Note that an asymmetric bi-affine correlation, like a vector OLE, cannot be a group correlation. But this result shows that it is a subgroups correlation compactly embedded in a group correlation. In particular, n-dimensional vector OLE over a ring A is embedded in the group correlation over the group $A^n \times A \times A^n$ with subset $S = \{(\boldsymbol{t}, u, \boldsymbol{t}u) | \boldsymbol{t} \in A^n, u \in A\}$. Interestingly, when instantiated for OLE ($n = 1$), it shows that OLE is embedded in the BMT correlation.
3. If σ is a semi-abelian bi-affine homomorphism, then BA_σ is embedded in $\mathsf{BA}_{\sigma^{\langle 2 \rangle}}$. This serves as an alternate way of viewing the embedding of OLE in BMT, since OLE is BA_σ and BMT is $\mathsf{BA}_{\sigma^{\langle 2 \rangle}}$ where σ is the 1multiplication operation in the (possibly non-commutative) ring.

As mentioned, OLE over a ring is a group correlation, over the group $\mathbb{K}_\cdot$. We explore this group and discover more unexpected structure:

- When A has an element η such that $\eta + \eta = 1$, $\mathbb{K}_\sigma$ is isomorphic to the group $A \times A$ (considering only the addition operation in the ring).
- When A is $\mathbb{F}_{2^n}$ then $\mathbb{K}_\sigma$ is isomorphic to $\mathbb{Z}_4^n$. (See Section 1.3.5).

1.3.3 Information-Theoretic Results

Wyner residual information (RI_{W}) (5) is an information theoretic measure which describes how "correlated" two random variables are. This measure is a monotone and cannot be increased through communication. Concretely, Prabhakaran et. al. [25] showed that if m independent instances of one type of correlation (C) can be reduced to n independent instances of another type of correlation (C'), then $m \cdot RI_{\mathrm{W}}(C) \leq n \cdot RI_{\mathrm{W}}(C')$ (Proposition 10).

In this work, we compute the Wyner Residual Information for a subset of bi-affine correlations which satisfy the *non-defective* property (Definition 7). A consequence of our results is that, for any field F, $RI_{\mathrm{W}}(\mathrm{OLE}_F^n) = \log |F|$. In fact, the above result extends to

domains rather than fields. (A domain is a ring with the "zero-product property," i.e., if $ab = 0$ then $a = 0$ or $b = 0$.) These results play a crucial role in later sections where we prove optimality of reductions from bi-affine correlations to oblivious transfer. Furthermore, we show that the bi-partite graph of a group correlation is a single connected component iff the set $\{s - s' \mid s, s' \in S\}$ is a generating set for the group G by appealing to the Gács-Körner common information (Lemma 11).

1.3.4 Constructions

We present several constructions (Section 5), which relate to various conditional sampling functionalities that *complete* a bi-affine correlation. Let $\mathcal{F}_\sigma$ be an ideal sampling functionality that samples an instance of the correlation and gives each party its side of the correlation. Similary, let $\widetilde{\mathcal{F}}_\sigma$ be a biasable sampling functionality (where the adversary is allowed to pick its side of a valid correlation). Now, we define three completion functionalities – depending on how many variables are fixed – for bi-affine correlations.

Conditional Sampling Functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$
(where $\sigma : Q \to H$ is a bi-affine homomorphism w.r.t. $T, U \leqslant Q$)

Inputs: t, a from Alice, and $u \in U$ from Bob, where

$t = a = \perp$ for $\mathcal{F}_{\sigma|\mathrm{U}}$ $\quad$ $t \in T, a = \perp$ for $\mathcal{F}_{\sigma|\mathrm{TU}}$ $\quad$ $t \in T, a \in H$ for $\mathcal{F}_{\sigma|\mathrm{TAU}}$.

Outputs: $(\tilde{t}, \tilde{a})$ to Alice and $(\tilde{u}, \tilde{b})$ to Bob, where $((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})) \leftarrow \mathsf{BA}_\sigma$ conditioned on $\tilde{u} = u$, $\tilde{t} = t$ if $t \neq \perp$, and $\tilde{a} = a$ if $a \neq \perp$.

We then present various protocols that implement the above functionalities (Section 5):

- UC secure protocols for $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ in the $\mathcal{F}_\sigma$-hybrid model (Figure 2). The protocols remain secure even if $\mathcal{F}_\sigma$ is replaced by an "adversarially controlled" version $\widetilde{\mathcal{F}}_\sigma$ (which still only provides instances in the support of the correlation BA_σ).
  - These protocols, denoted as $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$, can be used for multiple purposes. In particular, it allows for *rerandomizing* a sample, and also as a tool for non-destructively checking the validity of a sample (in the protocols TRSamp_σ and $\mathsf{altTRSamp}_\sigma$ below). Our protocols are optimal in multiple ways: there is only one message (or in the case of $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$, two messages) and a single instance of the correlation is "consumed" per instance produced. For the basic forms of these tasks (without the extension to $\widetilde{\mathcal{F}}_\sigma$), similar constructions have been previously developed, but only for specific correlations like OLE, BMT etc., [13].
- We also develop a new set of protocols for realizing the above functionalities using a "tamperable" version $\widehat{\mathcal{F}}_\sigma$ (which, when the two parties are honest, allows the adversary to specify arbitrary pairs, possibly outside the support of BA_σ), instead of $\widetilde{\mathcal{F}}_\sigma$. We present two such protocols, trading-off generality with efficiency.
  - The first protocol, TRSamp_σ (Figure 5) works for all bi-affine homomorphisms σ, but consumes $\omega(\log \lambda)$ (purported) samples of BA_σ to produce a single (good) instance. This protocol relies on an *error-preservation property* of the protocol $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$, whereby it can be checked if two purported samples have identical "error," by consuming only one of them. This allows checking that a set of samples all have the same error, while leaving one of them unconsumed. This still admits the possibility that *all of the samples* have the same non-zero error. To detect this (except with negligible probability), a cut-and-choose step is employed.

- The second protocol, $\mathsf{altTRSamp}_\sigma$ (Figure 6) achieves a rate of $1/2$, but relies on additional algebraic structure in the groups underlying σ. The main component of this protocol is an *error rerandomization* step (Figure 7), which we instantiate for a variety of bi-affine homomorphisms $\sigma : Q \to H$, where:
  - σ corresponds to multiplication in a vector space over a large field (or more generally, a module of appropriate complexity),
  - H is abelian and its order has no small prime factors,
  - H is non-abelian and $|\{r + x - r \mid r \in H\}$ is large for all $x \neq 0$.
- We give a semi-honest secure protocol (Figure 4) for efficiently sampling a bi-affine correlation BA_σ from string-OTs. This protocol relies on additional structure in the groups underlying the σ, and requires (slight) non-blackbox access to them. The additional structure is used to represent every group element as a small sum of elements from a "basis." The protocol is a generalization of a protocol by Gilboa [19] for sampling OLE over a ring using string OTs, to bi-affine correlations over a wide range of groups. We also show, using our results on residual information from above, that when the basis allows a tight representation of the group elements, then, with some additional constraints on σ, the protocol is *optimal in the number of string-OTs used* (Lemma 15).

1.3.5 A Surprising Structure for OLE

It is easy to see that OT (i.e., OLE over $\mathbb{F}_2$) can be written as a group correlation over $\mathbb{Z}_4$, by "drawing" the correlation as a bipartite graph and observing that it forms a cycle (see Figure 1b). A surprising result we obtain is that OLE over $\mathbb{F}_{2^n}$ is in fact a group correlation over $\mathbb{Z}_4^n$. We illustrate this for $n = 2$ in the full version.

We give a detailed description and proof in the full version, but provide a high level overview here. To show that $\text{OLE}_{\mathbb{F}_{2^n}}$ is a group correlation we give an isomorphism $\boldsymbol{\phi}$ from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{Z}_4^n$ along with a subset $S \subset \mathbb{Z}_4^n$ and show that field elements $(t, a), (u, b)$ form an OLE correlation $(a + b = tu)$ iff the sum of elements $g_1 = \boldsymbol{\phi}(t, a), g_2 = \boldsymbol{\phi}(u, b)$ lies within S. The isomorphism itself is highly non-trivial as it needs to handle the interaction of multiplicative and additive operations of the field in a purely additive sense. The isomorphism and subset are given by

$$\boldsymbol{\phi}(x, y) = [\![x]\!] - 2 \cdot \left[\!\!\left[\sqrt{\sum_{i:x_i=1} \xi^{(i)}(x)_i} \right]\!\!\right] + 2 \cdot [\![\sqrt{y}]\!]$$

$$S = \{[\![x]\!] - 2 \cdot \left[\!\!\left[\sqrt{\sum_{i:x_i=1} \xi^{(i)}(x)_i} \right]\!\!\right] \mid x \in \mathbb{F}_{2^n}\}$$

where $[\![x]\!]$ denotes the embedding from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_4^n$, obtained by interpreting $x \in \{0, 1\}^n$ as $x \in \{0, 1, 2, 3\}^n$, $\{\xi^{(i)}\}_{i \in [0,n-1]}$ is an arbitrary basis of $\mathbb{F}_{2^n}$ with $\xi^{(0)} = 1$, and $(x)_i$ is the field element obtained by zeroing out all coordinates greater than or equal to i.

1.3.6 Applications

Using our constructions from Section 5 we show how to perform secure 2-Party computation of "mixed-groups" circuits in the semi-honest setting. The mixed-groups circuit model uses wires which carry group elements and group/bi-affine homomorphism gates in addition to gates implementing standard group operations.

- The first setting is semi-honest 2-Party computation in the $\mathcal{F}_\sigma$, $\mathcal{F}_{ZAS}$ hybrid model, where σ is the bi-affine homomorphism corresponding to the bi-affine homomorphism gate being evaluated. Throughout the evaluation we maintain the invariant that all wires are secret shared between the two parties. At each bi-affine gate, two bi-affine correlations and one ZAS correlation (in the group of the output wire) is consumed and at most two rounds of communication are needed to evaluate each level of the circuit. We achieve perfect security in this setting.
  - As a corollary, we show that the ZAS correlation is complete for passively secure 2-Party secure computation over black-box groups. This is immediate as all group operations can be implemented using ZAS correlations only.
  - For the special case of formulas (or log-depth circuits) we present a two round perfectly secure protocol where the communication is proportional to the number of terms in the formula. Note that a formula can be written as an alternating sum of Alice and Bob's private inputs $f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n}(x_i + y_i)$. Alice pads each term of the formula with randomness and sends terms which contain her input in the clear. Alice and Bob invoke $\mathcal{F}_{ZAS}$ to compute terms containing Bob's inputs. Bob then sums up the terms sent by Alice and his output from $\mathcal{F}_{ZAS}$ invocations to compute $f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n}(x_i + y_i)$.
  - We also show how the same task can be achieved in a different manner using the Function Secret Sharing based approach of Boyle et al. [9].
- The second setting we consider is the commodity based model introduced by Beaver [4]. Here a semi-trusted server which provides Alice and Bob with (possibly incorrect) correlations and is guaranteed to not collude with either party. Incorrect correlations are identified by using either TRSamp_σ or $\mathsf{altTRSamp}_\sigma$, after which the computation can be done in a manner identical to the previous setting.

Full descriptions of these protocols can be found in the full version.

2 Preliminaries

All the sets (and in particular, groups, rings and fields) we consider in this work are finite. For groups, we typically use additive notation. When several groups are used together, we often assign different symbols like $\odot$, $\oplus$ and $+$ for their operators. The unary negation symbol $(-x)$ is used across all groups to indicate the inverse; also, the binary subtraction symbol $(x - y)$ is used to denote $x + (-y)$, when the group operation is $+$. We use upright capital letters to denote random variables, as X, Y etc. Through out the paper, 2-party secure computation, unless otherwise qualified, refers to information-theoretic security against passive corruption.

We recall that given a subgroup T of a group $(G, +)$, its right and left cosets containing an element $g \in G$ are defined as $T + g = \{t + g \mid t \in T\}$, $g + T = \{g + t \mid t \in T\}$. We define "shifted groups" over these cosets, by redefining the group operation.

▶ **Definition 1** (Shifted Group Operation). *Given a group $(G, +)$, and $g \in G$, the operation $+_g$ is defined as $x +_g y = x - g + y$.*

It can be seen that $+_g$ is associative, as $(x +_g y) +_g z = x +_g (y +_g z) = x - g + y - g + z$. For any subgroup $T \subseteq G$, it can be verified that $(T + g, +_g)$ and $(g + T, +_g)$ are both groups with identity element g and the inverse of x given by $g - x + g$. They are both subgroups of $(G, +_g)$.

▶ **Definition 2** (Flat Correlation). *A flat correlation over sets X, Y is defined to be the uniform distribution over a set $C \subseteq X \times Y$. It is said to be* regular *if there are integers d_X, d_Y such that $\forall x \in X$, $|C \cap (\{x\} \times Y)| = d_X$ and $\forall y \in Y$, $|C \cap (X \times \{y\})| = d_Y$.*

Above, C is called the *support* of the correlation, and is also used to denote the correlation itself. Given a flat correlation over X, Y with support C, its graph $\mathbb{G}_C$ is defined as the bipartite graph with vertices $X \dot{\cup} Y$ (disjoint union) and the set of edges C.

▶ **Definition 3** (Isomorphic Correlations). *Flat correlations $C \subseteq X \times Y$ and $C' \subseteq X' \times Y'$ are said to be* isomorphic *to each other if there exist bijections $\alpha : X \to X'$ and $\beta : Y \to Y'$ such that $C' = \{(\alpha(x), \beta(y)) \mid (x, y) \in C\}$.*

▶ **Definition 4** (Sampling Functionalities $\mathcal{F}_C$, $\widetilde{\mathcal{F}}_C$, $\widehat{\mathcal{F}}_C$). *For a flat correlation C, we define three functionalities as follows.*

- ***Sampling Functionality*** $\mathcal{F}_C$*: Uniformly samples a pair $(x, y) \leftarrow C$, and gives x to Alice and y to Bob.*
- ***Biasable Sampling Functionality*** $\widetilde{\mathcal{F}}_C$*: If Alice is corrupt, then it takes $x \in X$ from Alice, and outputs $y \leftarrow \{y' | (x, y') \in C\}$ to Bob; similarly, if Bob is corrupt, it takes y from Bob and outputs $x \leftarrow \{x' | (x', y) \in C\}$ to Alice. But if both parties are honest then it lets the adversary specify a valid sample, i.e., $(x, y) \in C$, instead of sampling one itself.*
- ***Tamperable Sampling Functionality*** $\widehat{\mathcal{F}}_C$*: It behaves like $\widetilde{\mathcal{F}}_C$, but if both Alice and Bob are honest, then it lets the adversary specify an arbitrary pair (x, y) (rather than only a valid pair).*

3 Definitions and Connections

3.1 Group Correlations and Subgroups Correlations

▶ **Definition 5** (Group Correlation). *A flat correlation $C \subseteq X \times Y$ is said to be a* group correlation *if there exists a group G and a subset $S \subseteq G$ such that C is isomorphic to the flat correlation $C' \subseteq G \times G$ given by $C' = \{(x, y) \mid x + y \in S\}$. In this case, we say that C is a group correlation of the form $GC^{G,S}$. A group correlation of the form $GC^{G,S}$ is said to be* abelian *if the group G is abelian.*

Regularity. Let G_1, G_2 be subgroups of G, and $S \subseteq G$. S is said to be *regular* with respect to (G_1, G_2) if, for all $g_2, g_2' \in G_2$, we have $|S \cap (G_1 + g_2)| = |S \cap (G_1 + g_2')|$, and for all $g_1, g_1' \in G_1$, we have $|S \cap (g_1 + G_2)| = |S \cap (g_1' + G_2)|$. We call $\deg_L = |S \cap (g_1 + G_2)|$ and $\deg_R = |S \cap (G_1 + g_2)|$ the left and right degree of the subgroups correlation respectively.

We say that a group correlation $\mathrm{GC}^{G,S}$ is regular w.r.t. a pair of subgroups (G_1, G_2) of G if S is regular w.r.t. (G_1, G_2).

▶ **Definition 6** (Subgroups Correlation). *A flat correlation $C \subseteq X \times Y$ is said to be a* subgroups correlation *if there exists a group correlation C' that is regular w.r.t. a pair of subgroups (G_1, G_2), and C is isomorphic to the correlation $C'' \subseteq G_1 \times G_2$ defined as $C'' = C' \cap (G_1 \times G_2)$. In this case, we say C is of the form $GC^{G,S}_{G_1,G_2}$, and is* embedded in *C'. Further, if $|G| < |X||Y|$, we say that C is a* compact *subgroups correlation.*

If C is a *regular* flat correlation, then it can be seen to be a (non-compact) subgroups correlation of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$ where, identifying X and Y with arbitrary groups of the same sizes (say $\mathbb{Z}_{|X|}$ and $\mathbb{Z}_{|Y|}$), we let $G = X \times Y$, $G_1 = X \times \{0_Y\}$, $G_2 = \{0_X\} \times Y$, and $S = C$. Conversely, a subgroups correlation is a regular flat correlation. Hence, without restricting to being compact, subgroups correlations and regular flat correlations are the same. A compact subgroups correlation entails more structure than just being regular.

3.2 Bi-Affine Correlations

We start by defining a generalization of the notion of a homomorphism, called *bi-affine homomorphism*. Note that the definition below refers to homomorphisms between "shifted" groups, using the shifted group operation (Definition 1).

▶ **Definition 7** (Bi-Affine Homomorphism)**.** *For groups $(Q,+)$ and $(H,\oplus)$, and subgroups $T,U \leqslant Q$, a function $\sigma : Q \to H$ is said to be a* bi-affine homomorphism w.r.t. (T,U)*, if the following are group homomorphisms*

$$\sigma|_{T+u} : (T+u,+_u) \to (H,\oplus_{\sigma(u)}) \qquad \forall u \in U$$
$$\sigma|_{t+U} : (t+U,+_t) \to (H,\oplus_{\sigma(t)}) \qquad \forall t \in T.$$

Further, σ is said to be semi-abelian *if H is an abelian group; it is said to be* abelian *if both Q and H are abelian. It is said to be* symmetric *if it is semi-abelian and $Q = D \times D, T = D \times \{0\}, U = \{0\} \times D$ for some group D. If either $\sigma|_{T+u}$ is surjective for every $u \in U$, or $\sigma|_{t+U}$ is surjective for every $t \in T$, σ is called a* surjective *bi-affine homomorphism. If there is no pair $(t,u) \in (T \setminus \{0\}) \times (U \setminus \{0\})$ such that $\sigma(t+u) = \sigma(t) - \sigma(0) + \sigma(u)$, σ is said be to non-defective*[2]*.*

These homomorphism conditions over the shifted groups can be equivalently written as, $\forall t,t' \in T, u,u' \in U$,

$$\sigma(t+t'+u) = \sigma(t+u) \oplus -\sigma(u) \oplus \sigma(t'+u)$$
$$\sigma(t+u+u') = \sigma(t+u) \oplus -\sigma(t) \oplus \sigma(t+u').$$

(where we used $(t+u)+_u(t'+u) = t+t'+u$ and $(t+u)+_t(t+u') = t+u+u'$).

▶ **Definition 8** (Bi-Affine Correlation)**.** *Given groups $(Q,+)$ and $(H,\oplus)$, and a bi-affine homomorphism $\sigma : Q \to H$ w.r.t. (T,U), the correlation $\mathsf{BA}_\sigma \subseteq (T \times H) \times (U \times H)$ is defined as*

$$\mathsf{BA}_\sigma = \{((t,a),(u,b)) \mid \sigma(t+u) = a \oplus b\}$$

A flat correlation C is said to be a bi-affine correlation *if there exists σ as above such that it is isomorphic to BA_σ. Further, C is said to be* semi-abelian*,* abelian *or* symmetric *if σ has the corresponding property.*

Bi-linear correlations. It is instructive to compare bi-affine homomorphisms with bi-linear maps. For groups $(T,+)$, $(U,+)$ and $(H,\oplus)$, where the last one is abelian, a function $e : T \times U \to H$ is said to be a bi-linear map if e left and right distributes over the group operations: i.e., for all $t_1,t_2 \in T$ and $u_1,u_2 \in U$, $e(t_1+t_2,u_1) = e(t_1,u_1) \oplus e(t_2,u_1)$, and $e(t_1,u_1+u_2) = e(t_1,u_1) \oplus e(t_1,u_2)$.

It is easy to see that a bi-linear map is a special case of a bi-affine homomorphism: Let $Q = T \times U$, $T' = T \times \{0_U\}$ and $U' = \{0_T\} \times U$. Then, $\sigma : Q \to H$ is a bi-linear map iff it is a semi-abelian bi-affine homomorphism w.r.t. (T',U'), with the additional property that $\sigma(x) = 0$ for all $x \in T' \cup U'$. If a bi-affine homomorphism σ is a bi-linear map, then we say that a correlation of the form BA_σ is a *bi-linear correlation*. For bi-linear σ, non-defective

[2] This condition corresponds to $K_{2,2}$ freeness of the bi-affine correlation. Proof can be found in the full version.

reduces to not having non-zero $t \in T, u \in U$ such that $\sigma(t+u) = 0$. An example of such a bi-affine correlation is given by OLE (or vector OLE) over a *domain*. A domain is a ring with the "zero-product property," i.e., if $ab = 0$ then $a = 0$ or $b = 0$ (with fields being a special case of domains).

3.3 Powers of Bi-Affine Homomorphisms

Given a bi-affine homomorphism σ, one can define related bi-affine homomorphisms as various "powers". In this section, we describe some standard transformations to do this, and in Section 3.5 give some important examples of correlations in the literature that illustrate these transformations. Let $\sigma : Q \to H$ be a bi-affine homomorphism w.r.t subgroups T, U.

- We define $\sigma^n : Q^n \to H^n$ as simply the coordinate-wise application of σ. That is, $\sigma^n(q_1, ..., q_n) = (\sigma(q_1), ..., \sigma(q_n))$. If σ is a bi-affine homomorphism w.r.t. subgroups $T, U \leqslant Q$, then σ^n is readily seen to be a bi-affine homomorphism w.r.t. subgroups $T^n, U^n \leqslant Q^n$.
- It is interesting to view σ^n as a bi-affine homomorphism w.r.t. other subgroups within T^n, U^n. In particular, we define $\sigma^{(n)}$ to be the same as σ^n but considered as a bi-affine homomorphism w.r.t. $T^n, U^{(n)}$, where $U^{(n)} = \{(u, \ldots, u) | u \in U\} \subseteq U^n$.
- When H is abelian, we also define an aggregating version $\sigma^{\langle \ell, m \rangle} : Q^{\ell+m} \to H$, as $\sigma^{\langle \ell, m \rangle}(q_1, \ldots, q_\ell, q'_1, \ldots, q'_m) = \sum_{i=1}^{\ell} \sigma(q_i) \oplus \sum_{i=1}^{m} \sigma(-q'_i)$ where the summations refer to the operation $\oplus$ in the group H. $\sigma^{\langle \ell, m \rangle}$ can be seen to be a bi-affine homomorphism w.r.t. $(T^\ell \times U^m,\ U^\ell \times T^m)$. We shall simply write $\sigma^{\langle n \rangle}$ for the symmetric bi-affine homomorphism $\sigma^{\langle \lceil n/2 \rceil, \lfloor n/2 \rfloor \rangle}$.

These powers of a bi-affine homomorphism are in fact bi-affine homomorphisms. We prove this in the full version. We can now define BA_{σ^n}, $\mathsf{BA}_{\sigma^{(n)}}$ and $\mathsf{BA}_{\sigma^{\langle n \rangle}}$ as the bi-affine correlations corresponding to σ^n, $\sigma^{(n)}$ and $\sigma^{\langle n \rangle}$ respectively.

3.4 Group Structure of Bi-Affine Correlations

In this section we show connections between (sub)group correlations and bi-affine correlations, which can be summarized as follows:

▶ **Theorem 9.** *For any bi-affine homomorphism σ,*

1. BA_σ *is a compact subgroups correlation;*
2. *if σ is symmetric, then BA_σ is a group correlation;*
3. *if σ is semi-abelian, then BA_σ is embedded in $\mathsf{BA}_{\sigma^{\langle 2 \rangle}}$, and more generally, $\mathsf{BA}_{\sigma^{\langle \ell, m \rangle}}$ is embedded in $\mathsf{BA}_{\sigma^{\langle 2m' \rangle}}$ for all $m' \geq \max(\ell, m)$.*

We present the key ingredients of the above connections here. Details omitted from here can be found in the full version.

Groups $\mathbb{J}$ and $\mathbb{K}$. To capture the structure of bi-affine correlations as (sub)group correlations, we define two groups.

- If $\sigma : Q \to H$ is a bi-affine homomorphism w.r.t. (T, U), the group $\mathbb{J}_\sigma$ is defined as the direct product $T \times U \times H$. Then it is easy to see that BA_σ is a subgroups correlation of the form $\mathrm{GC}^{G,S}_{G_1,G_2}$ where $G = \mathbb{J}_\sigma$ and $S = \{(t, u, \sigma(t+u)) \mid t \in T, u \in U\}$, with $G_1 = T \times \{0\} \times H, G_2 = \{0\} \times U \times H$. This is a compact subgroups correlation because $|G_1||G_2| = |T||U||H|^2 > |T||U||H| = |G|$.
- If $\sigma : D \times D \to H$ is a symmetric bi-affine homomorphism, then $\mathbb{K}_\sigma$ is defined as $(D \times H, \odot)$, where $\odot$ is given by $(d, h) \odot (d', h') = (d + d', h \oplus h' \oplus \sigma(d, 0) \oplus \sigma(0, d') \oplus -\sigma(d, d'))$. It can now be shown that BA_σ is a group correlation of the form $\mathrm{GC}^{\mathbb{K}_\sigma, S}$, where $S = \{(d + d', \sigma(d, 0) \oplus \sigma(0, d')) | d, d' \in D\}$.

In particular, if $\sigma : A \times A \to A$ for a ring A, with $\sigma(a,b) = ab$ (multiplication in the ring), then the operation $\odot$ is defined as $(t,a)\odot(u,b) = (t+u, a+b-tu)$. This group, which we denote as $\mathbb{K}_A$, encodes both the addition and multiplication operations in the ring (as $(0,a)\odot(0,a') = (0,a+a')$, and $(a,0)\odot(a',0) = (a+a',-aa')$).

3.5 Some Noteworthy Examples

Here we consider several cryptographically interesting examples and show that they are (sub) group correlations and also explore connections between them. More examples along with a tabular summary can be found in the full version.

Oblivious Linear function Evaluation and Beaver's Multiplication Triples. OLE and BMT over an arbitrary ring A are defined as follows:

$$\text{OLE}_A := \{\big((p,a),(q,b)\big) \mid a+b = pq\},$$
$$\text{BMT}_A := \{\big((a_1,b_1,c_1),(a_2,b_2,c_2)\big) \mid c_1+c_2 = (a_1+a_2)(b_1+b_2)\}.$$

Consider the symmetric bi-affine homomorphism $\sigma : A \times A \to A$ defined with respect to subgroups $T = A \times \{0\}$ and $U = \{0\} \times A$ as $\sigma(p,q) = pq$. It can be seen that the bi-linear correlation BA_σ is isomorphic to OLE_A. OLE_A is also a group correlation (Theorem 9).

It is straightforward to see that BMT is a group correlation with $G = A \times A \times A$ and $S = \{(a,b,ab) \mid a,b \in A\}$. Furthermore, BMT is isomorphic to the bi-linear correlation

$$\mathsf{BA}_{\sigma\langle 2\rangle} := \{\big((\tilde{a}_1,0),(0,\tilde{b}_2),\tilde{c}_1\big),\big((0,\tilde{b}_1),(\tilde{a}_2,0),\tilde{c}_2\big) \mid \tilde{a}_1\tilde{b}_1 + \tilde{a}_2\tilde{b}_2 = \tilde{c}_1+\tilde{c}_2\},$$

This can be seen by defining isomorphisms

$$\alpha(a_1,b_1,c_1) = \big((a_1,0),(0,b_1),c_1-a_1b_1\big) \text{ and } \beta(a_2,b_2,c_2) = \big((0,b_2),(a_2,0),c_2-a_2,b_2\big).$$

It can now be checked that

$$\big((a_1,b_1,c_1),(a_2,b_2,c_2)\big) \in \text{BMT}_A \Leftrightarrow \big(\alpha(a_1,b_1,c_1),\beta(a_2,b_2,c_2)\big) \in \mathsf{BA}_{\sigma\langle 2\rangle}.$$

Zero-Alternating Sum Correlation. We introduce an important correlation, called Zero Alternating Sum (ZAS) correlation over any (possibly non-abelian) group $(D,+)$. ZAS is a flat correlation $\text{ZAS}_D \subseteq D^2 \times D^2$, defined as

$$\text{ZAS}_D := \{\big((a,c),(b,d)\big) \mid a+b+c+d = 0\}.$$

We remark that if D is an abelian group, then ZAS_D is a trivial correlation.[3]

zas_D as a Bi-Affine Correlation. Somewhat surprisingly, ZAS turns out to be a bi-affine correlation. We define the corresponding bi-affine homomorphism $\sigma : D \times D \to H$, where $H = D^{\text{op}}$, the *opposite group* of D (i.e., H has the same elements as D and has a group operation $\oplus$ defined by $a \oplus b = b+a$). We let $\sigma(x,y) = -(x+y)$. Then, clearly, ZAS is isomorphic to the flat correlation $\{((c,a),(d,b)) \mid \sigma(c,d) = a+b\}$. It is straightforward to verify that σ is indeed a bi-affine homomorphism. For completeness, we present a proof in the full version. Later, we refer to the bi-affine homomorphism σ defined above as σ_D^{ZAS}.

[3] A secure protocol for sampling from ZAS_D, when D is abelian, is as follows: Alice samples $x \leftarrow D$ to Bob; Alice then picks a random $a \leftarrow D$ and outputs $(a, x-a)$; Bob samples $b \leftarrow D$ and outputs $(b, -x-b)$.

zas_D as a Group Correlation. When D is not abelian, σ defined above is not semi-abelian, and hence ZAS_D is *not* symmetric. As such, Theorem 9 *does not* apply to ZAS_D. Nevertheless, we show below that ZAS_D over any group D is a group correlation of the form $\text{GC}^{G,S}$, where the group G is $D \times D$, with coordinate-wise addition, and $S = \{(g, -g) \mid g \in D\}$.

$$((a,c),(b,d)) \in \text{ZAS}_D \Leftrightarrow a+b+c+d=0 \Leftrightarrow a+b=-(c+d)$$
$$\Leftrightarrow (a+b, c+d) \in S \Leftrightarrow (a,c)+(b,d) \in S.$$

4 Information Theoretic Results

Common-Information. For a pair of correlated random variables (X, Y), two important information-theoretic measures of correlation are the well-known quantity of *mutual information* $I(\mathrm{X};\mathrm{Y})$ [26] and the lesser known notions of *common information*. Specifically, there are two measures of common information due to Gács and Körner [18] and due to Wyner [28], which can defined as below:

$$CI_{\text{GK}}(\mathrm{X};\mathrm{Y}) = I(\mathrm{X};\mathrm{Y}) - RI_{\text{GK}}(\mathrm{X};\mathrm{Y}) \tag{2}$$
$$CI_{\text{W}}(\mathrm{X};\mathrm{Y}) = I(\mathrm{X};\mathrm{Y}) + RI_{\text{W}}(\mathrm{X};\mathrm{Y}) \tag{3}$$
$$RI_{\text{GK}}(\mathrm{X};\mathrm{Y}) = \inf_{\mathrm{Q}} I(\mathrm{X};\mathrm{Y}|\mathrm{Q}), \text{ such that } H(\mathrm{Q}|\mathrm{X}) = H(\mathrm{Q}|\mathrm{Y}) = 0 \tag{4}$$
$$RI_{\text{W}}(\mathrm{X};\mathrm{Y}) = \inf_{\mathrm{Q}} I(\mathrm{Y};\mathrm{Q}|\mathrm{X}) + I(\mathrm{X};\mathrm{Q}|\mathrm{Y}), \text{ such that } I(\mathrm{X};\mathrm{Y}|\mathrm{Q}) = 0 \tag{5}$$

where the infimum is over all random variables Q that are jointly distributed with (X, Y). Here RI_{GK} and RI_{W} are (respectively) Gács-Körner and Wyner *residual information*.

We shall write $RI_{\text{W}}(C)$ etc. as a short hand for $RI_{\text{W}}(\mathrm{X};\mathrm{Y})$, where the random variables (X, Y) are uniformly distirbuted over C. We will use the following proposition that is a special case of a "monotonicity" result in [25].

▶ **Proposition 10** ([25]). *If m independent instances of $\mathcal{F}_C$ can be securely computed using n independent instances of $\mathcal{F}_{C'}$, then $m \cdot RI_{\text{W}}(C) \le n \cdot RI_{\text{W}}(C')$.*

Also, C is a trivial correlation – i.e., there exists an information theoretically secure 2-party protocol to sample from C – iff $RI_{\text{W}}(C) = 0$ (or equivalently, $RI_{\text{GK}}(C) = 0$).

▶ **Lemma 11.** *Suppose C is a group correlation of the form $GC^{G,S}$. Then:*

1. *C is trivial iff S is a (left or right) coset of a subgroup of G.*
2. *$CI_{\text{GK}}(C) = 0$ iff the set $\{s - s' \mid s, s' \in S\}$ is a generating set for the group G.*
3. *If for all $s_1, s_2, s_3, s_4 \in S$, $s_1 - s_2 + s_3 - s_4 = 0 \Rightarrow \{s_1, s_3\} = \{s_2, s_4\}$, then $RI_{\text{W}}(C) = \log|S|$ viz. C is $K_{2,2}$ free.*

Now, we state our main technical result in this section. Recall that in a non-defective bi-affine homomorphism, there is no pair $(t,u) \in (T \setminus \{0\}) \times (U \setminus \{0\})$ such that $\sigma(t+u) = \sigma(t) - \sigma(0) + \sigma(u)$.

▶ **Lemma 12.** *If σ is a non-defective bi-affine homomorphism w.r.t. (T, U), then $RI_{\text{W}}(\mathsf{BA}_\sigma) = \log\min(|T|, |U|)$.*

An example of a non-defective bi-affine homomorphism is multiplication in a *domain*. As a result, we have $RI_{\text{W}}(\text{OLE}_A^n) = \log|A|$ if A is a domain.

5 Protocols for Bi-Affine Correlations

In this section, we present several protocols pertinent to bi-affine correlations. These protocols realize several basic functionalities related to "completing" a correlation (i.e., sampling from a correlation conditioned on certain variables being fixed), given access to a random instance of the same correlation which could be obtained from a semi-trusted source modeled by the biasable sampling functionality. The same protocols can also be used to "rerandomize" for forward security. Missing details of the constructions and their proofs can be found in the full version.

In the following, let $\sigma : Q \to H$ be a bi-affine homomorphism from a group $(Q, +)$ to group $(H, \oplus)$ w.r.t subgroups $T, U \leqslant Q$.

5.1 Completing a Bi-Affine Correlation

We first define the conditional sampling functionality that *completes* a bi-affine correlation, by sampling an instance of the correlation conditioned on its inputs.

Conditional Sampling Functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$
(where $\sigma : Q \to H$ and $T, U \leqslant Q$)

Inputs: $t \in T, a \in H$ from Alice, and $u \in U$ from Bob, where

$t = a = \perp$ for $\mathcal{F}_{\sigma|\mathrm{U}}$ $\quad$ $t \in T, a = \perp$ for $\mathcal{F}_{\sigma|\mathrm{TU}}$ $\quad$ $t \in T, a \in H$ for $\mathcal{F}_{\sigma|\mathrm{TAU}}$.

Outputs: $(\tilde{t}, \tilde{a})$ to Alice and $(\tilde{u}, \tilde{b})$ to Bob, where $((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})) \leftarrow \mathsf{BA}_\sigma$ conditioned on $\tilde{u} = u$, $\tilde{t} = t$ if $t \neq \perp$, and $\tilde{a} = a$ if $a \neq \perp$.

Functionalities $\mathcal{F}_{\sigma|\mathrm{T}}$ and $\mathcal{F}_{\sigma|\mathrm{TUB}}$ are defined symmetric to $\mathcal{F}_{\sigma|\mathrm{U}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$, respectively. All functionalities allow the adversary to selectively abort output delivery to honest parties (after seeing its own output, if any).

Figure 2 contains UC secure protocols for the functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model (Definition 4) with only one invocation of $\widetilde{\mathcal{F}}_\sigma$. The first two protocols require one round of communication while $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ needs two rounds of communication.

▶ **Lemma 13.** *$\mathsf{Comp}_{\sigma|\mathrm{U}}$, $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ (Figure 2) UC-securely realize functionalities $\mathcal{F}_{\sigma|\mathrm{U}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ respectively in the $\widetilde{\mathcal{F}}_\sigma$ hybrid.*

We prove this lemma in the full version. Here, we point out that if both parties are honest, then Alice and Bob output (t, a) and (u, b) such that:

$$\begin{aligned} a \oplus b &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\tilde{a} \oplus \tilde{b}] \oplus [-\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})] \\ &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\sigma(\tilde{t} + \tilde{u})] \oplus [-\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})] \\ &= [\sigma(t + \Delta_u) \oplus -\sigma(t)] \oplus [\sigma((\tilde{t} + \tilde{u}) +_{\tilde{u}} (\Delta_t + \tilde{u})] \\ &= \sigma((t + \Delta_u) +_t (t + \tilde{u})) \\ &= \sigma(t + u) \end{aligned}$$

where, we use the properties of σ (Definition 7) and the fact that $\tilde{a} \oplus \tilde{b} = \sigma(\tilde{t} + \tilde{u})$. Also note that to prove $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ realizes $\mathcal{F}_{\sigma|\mathrm{TAU}}$, it is sufficient to show that Π_σ is a secure realization of $\mathcal{F}_{\sigma|\mathrm{TAU}}$ (and then appeal to the UC theorem to implement $\mathcal{F}_{\sigma|\mathrm{TU}}$ with protocol $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model). Correctness of Π_σ, when the parties are honest, follows from the fact that $a \oplus b = a \oplus \Delta_a \oplus \tilde{b} = \tilde{a} \oplus \tilde{b} = \sigma(t + u)$. UC security follows from the observation that in Π_σ, the inputs to $\mathcal{F}_{\sigma|\mathrm{TU}}$ and the message that Alice sends to Bob can be arbitrary and would still correspond to valid input choices of the parties (or aborting).

Protocols $\mathsf{Comp}_{\sigma|\mathrm{U}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model

- **Inputs:** Bob receives $u \in U$. In $\mathsf{Comp}_{\sigma|\mathrm{TU}}$, Alice receives $t \in T$, as well.
- **Invocation of $\widetilde{\mathcal{F}}_\sigma$:** Alice gets $(\tilde{t}, \tilde{a})$ and Bob gets $(\tilde{u}, \tilde{b})$ from $\widetilde{\mathcal{F}}_\sigma$, s.t. $\tilde{a} \oplus \tilde{b} = \sigma(\tilde{t} + \tilde{u})$.
- In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, Alice sets $t = \tilde{t}$.
- **Alice $\leftrightarrow$ Bob:**
  - Alice sends Δ_t to Bob, where $\Delta_t := -\tilde{t} + t$. (In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $\Delta_t = 0_T$ and this message can be omitted.)
  - Bob sends Δ_u to Alice, where $\Delta_u := u - \tilde{u}$.
- **Output:** Alice outputs (a, t) where $a := \sigma(t + \Delta_u) \oplus -\sigma(t) \oplus \tilde{a}$, and Bob outputs (u, b) where $b := \tilde{b} \oplus -\sigma(\tilde{u}) \oplus \sigma(\Delta_t + \tilde{u})$. (In $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $b = \tilde{b}$.)

Protocol Π_σ in the $\mathcal{F}_{\sigma|\mathrm{TU}}$ hybrid model

- **Inputs:** Alice receives $(t, a) \in T \times H$, and Bob receives $u \in U$.
- **Invocation of $\mathcal{F}_{\sigma|\mathrm{TU}}$:** Alice inputs t, Bob inputs u to $\mathcal{F}_{\sigma|\mathrm{TU}}$, and receive outputs $(t, \tilde{a})$ and $(u, \tilde{b})$ respectively s.t. $\tilde{a} \oplus \tilde{b} = \sigma(t + u)$.
- **Alice $\rightarrow$ Bob:** Alice sends Δ_a to Bob, where $\Delta_a := -a \oplus \tilde{a}$.
- **Output:** Alice outputs (t, a) and Bob outputs (u, b), where $b := \Delta_a \oplus \tilde{b}$.

Protocol $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model

$\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ is obtained by composing Π_σ with $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ (as an implementation of $\mathcal{F}_{\sigma|\mathrm{TU}}$).

Figure 2 UC-secure protocols for $\mathcal{F}_{\sigma|\mathrm{T}}$, $\mathcal{F}_{\sigma|\mathrm{TU}}$ and $\mathcal{F}_{\sigma|\mathrm{TAU}}$ in the $\widetilde{\mathcal{F}}_\sigma$ hybrid model. All protocols use a single invocation to the functionality $\widetilde{\mathcal{F}}_\sigma$. The first two protocols have a single round of message exchange, while the latter requires two rounds.

5.2 Inner-Product Bi-Affine Correlations from Bi-Affine Correlations

If Alice and Bob hold $\ell + m$ instances of any semi-abelian bi-affine correlation BA_σ (in appropriate directions), they can non-interactively extract an instance of $\mathsf{BA}_{\sigma\langle \ell+m \rangle}$.

Protocol to sample $\mathsf{BA}_{\sigma\langle \ell,m \rangle}$ in the $\mathcal{F}_\sigma$ hybrid model

- **Invocation of $\mathcal{F}_\sigma$:**
  - $\mathcal{F}_\sigma$ is invoked ℓ times, at the end of which Alice holds $(r_1, \ldots, r_\ell, x_1, \ldots, x_\ell)$ and Bob holds $(s_1, \ldots, s_\ell, y_1, \ldots, y_\ell)$ such that $\sigma(r_i + s_i) = x_i \oplus y_i$ where $r_i \in T, s_i \in U$ and $x_i, y_i \in H$ for all $i \in [\ell]$.
  - $\mathcal{F}_\sigma$ is invoked m times in the opposite direction, at the end of which Alice receives $(s'_1, \ldots, s'_m, y'_1, \ldots, y'_m)$ and Bob receives $(r'_1, \ldots, r'_m, x'_1, \ldots, x'_m)$, such that $\sigma(r'_i + s'_i) = x'_i \oplus y'_i$ where $r'_i \in T, s'_i \in U$ and $x'_i, y'_i \in H$ for all $i \in [m]$.
- **Outputs:** Alice outputs $t_i = r_i, u'_j = -s'_j, h_1 = \sum_{k=1}^{\ell} x_k \oplus \sum_{k=1}^{m} y'_k$ and Bob outputs $t'_j = -r'_j, u_i = s_i, h_2 = \sum_{k=1}^{\ell} y_k \oplus \sum_{k=1}^{m} x'_k$ for all $i \in [\ell]$, $j \in [m]$.

Figure 3 A protocol for sampling $\mathsf{BA}_{\sigma\langle \ell,m \rangle}$ in the $\mathcal{F}_\sigma$, $\mathcal{F}_{ZAS|\mathrm{TU}}$ hybrid model.

The correctness of the protocol in Figure 3 can be seen as follows. Recall that the support of $\sigma^{\langle \ell, m \rangle}$ is defined as $\big((t_1, \ldots, t_\ell, u'_1, \ldots, u'_m, h_1), (u_1, \ldots, u_\ell, t'_1, \ldots, t'_m, h_2)\big)$ satisfying

$$\sigma^{\langle \ell, m \rangle}(t_1 + u_1, \ldots, t_\ell + u_\ell, u'_1 + t'_1, \ldots, u'_m + t'_m) = h_1 \oplus h_2 \tag{6}$$

The L.H.S of (6) can be expanded to verify correctness.

$$\begin{aligned}\sum_{i=1}^{\ell} \sigma(t_i + u_i) + \sum_{i=1}^{m} \sigma(-t'_i - u'_i) &= \sum_{i=1}^{\ell} \sigma(r_i + s_i) + \sum_{i=1}^{m} \sigma(r'_i + s'_i) \\ &= \sum_{i=1}^{\ell} (x_i + y_i) + \sum_{i=1}^{m} (x'_i + y'_i) \\ &= h_1 \oplus h_2.\end{aligned}$$

5.3 Bi-Affine Correlations from String OT

We sample bi-affine correlations by first constructing a protocol for $\mathcal{F}_{\sigma|\text{TAU}}$ in the string OT hybrid model. This implies a semi-honest secure protocol for $\mathcal{F}_\sigma$ when Alice and Bob sample their inputs uniformly at random. As the first step in a protocol for $\mathcal{F}_{\sigma|\text{TAU}}$, Alice and Bob agree upon a *generator matrix* M_U of dimensions $k \times d$ such that every element $u \in U$ can be expressed as $u = \sum_{i=1}^{k} M_U(i, c_i)$ where $M_U(i, j)$ denotes the element in the i-th row and j-th column and the vector $\boldsymbol{c}$ is the decomposition of element u w.r.t the generator matrix M_U. Given such an generator matrix, our protocol needs k instances of $\binom{d}{1}$-OT$^\ell$ string OTs.[4] Figure 4 describes the protocol for $\mathcal{F}_{\sigma|\text{TAU}}$ in the string OT hybrid model.

Protocol $\mathsf{Comp}_{\sigma|\text{TAU}}$ in the $\binom{d}{1}$-ot$^\ell$ Hybrid model

Parameters: Groups $(T, +), (U, +), (H, \oplus)$ and a generator matrix of U, $M_U \in U^{k \times d}$.

- **Inputs:** Alice has input $t \in T, a \in H$ and Bob has input $u \in U$.
  - Alice samples $\{r_i\}_{i \in [2,k]} \leftarrow H$ and sets $r_1 = a$.
  - For each $i \in [k-1]$, Alice and Bob invoke $\binom{d}{1}$-OT$^\ell$. Alice's input is the tuple $\{-r_i \oplus \sigma(t + M_U(i,j)) \oplus -\sigma(t) \oplus r_{i+1}\}_{j \in [d]}$ and Bob's input is a choice integer $c_i \in [d]$ such that $u = \sum_{j=1}^{k} M_U(j, c_j)$ where $M_U(i, j)$. Bob receives $m_i = -r_i \oplus \sigma(t + M_U(i, c_i)) \oplus -\sigma(t) \oplus r_{i+1}$.
  - For $i = k$, Alice's input is the tuple $\{-r_k \oplus \sigma(M_U(i,j))\}_{j \in [d]}$ and Bob's input is the choice integer $c_k \in [d]$. Bob receives $m_k = -r_k \oplus \sigma(t + M_U(k, c_k))$.
- Bob combines the messages he received to compute $b = \sum_{i=1}^{k} m_i$

Figure 4 A semi-honest secure protocol realising $\mathcal{F}_{\sigma|\text{TAU}}$ in the $\binom{m}{1}$-OT$^\ell$-Hybrid model.

▶ **Lemma 14.** $\mathsf{Comp}_{\sigma|\text{TAU}}$ *(Figure 4) is a semi-honest secure protocol realising* $\mathcal{F}_{\sigma|\text{TAU}}$.

Note that $|U| \leq d^k$, since every element in U can be represented as the summation of k elements, each chosen from a d-dimensional row of M_U. The following lemma considers the case when this representation is tight.

[4] Effectively, we require oblivious transfer over group elements and hence the length of strings must be long enough to send the description of an element.

▶ **Lemma 15.** *If σ is non-defective and $|U| = d^k \leq |T|$, then $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ is optimal in the number of instances of $\binom{d}{1}$-OT^ℓ used (for any length ℓ) for semi-honest securely realizing one instance of BA_σ.*

▶ **Lemma 16.** *If C is a regular correlation then $RI_{\mathrm{W}}(C) \leq \log \min(\deg_L(C), \deg_R(C))$. Further, if C is $K_{2,2}$-free, then $RI_{\mathrm{W}}(C) = \log \min(\deg_L(C), \deg_R(C))$.*

Lemma 15 follows from the fact that $RI_{\mathrm{W}}(\binom{d}{1}\text{-}\mathrm{OT}^\ell) \leq \log(d)$.[5] Also, by Lemma 12, $RI_{\mathrm{W}}(\mathsf{BA}_\sigma) \leq \log |U| = k \log d$. Then, by Proposition 10, at least k instances of $\binom{d}{1}$-OT^ℓ are needed to securely sample one instance of BA_σ, proving the lemma.

Comparison with Gilboa's protocol. In [19], Gilboa gave a protocol to generate OLE correlations over a ring A. Their protocol requires the ring to have a bit-decomposition which is equivalent to demanding the existence of a generator matrix M_A of dimension $\log |A| \times 2$. When $A = \mathbb{F}_{(2^n)}$, Gilboa's protocol uses n instances of $\binom{2}{1}$-OT^ℓ. By appealing to Lemma 16, Proposition 10 and the fact that $RI_{\mathrm{W}}(\binom{2}{1}\text{-}\mathrm{OT}^\ell) = 1$, it can be argued that this is the minimum number of OTs that must be invoked (in either direction and per correlation if amortised) to obtain an information-theoretically secure 2-Party protocol that samples $\mathrm{OLE}_{\mathbb{F}_{2^n}}$ correlations.

5.4 Biasable Correlations from Tamperable Correlations

The protocol TRSamp_σ in Figure 5 gives a secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$ hybrid model. With no assumptions on the structure of the correlation, Alice and Bob can consume $\log(\lambda)$ correlations and output one correlation which they are guaranteed is correct with overwhelming probability. The main insight in our tamper resistant protocols is to use the following error preservation property of $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ to check correlations against each other in a "tournament" style and thereby amplify the probability of catching incorrect correlations.

Error-Preservation Property. When $\mathsf{Comp}_{\sigma|\mathrm{U}}$, $\mathsf{Comp}_{\sigma|\mathrm{TU}}$ and $\mathsf{Comp}_{\sigma|\mathrm{TAU}}$ are instantiated in the $\widehat{\mathcal{F}}_\sigma$-hybrid, errors in the correlation output by parties is related to the error in the correlation which parties receive from $\widehat{\mathcal{F}}_\sigma$. Recall that when both Alice and Bob are honest, $\widehat{\mathcal{F}}_\sigma$ allows the adversary to feed an arbitrary pair $((\hat{t}, \hat{a}), (\hat{u}, \hat{b}))$ to the parties. Suppose, $\hat{a} \oplus \hat{b} = \sigma(\hat{t}+\hat{u}) \oplus \hat{e}$. In this case, the outputs (t, a) and (b, u) are such that $a \oplus b = \sigma(t+u) \oplus e$, where $e = x \oplus \hat{e} \oplus -x$ (for $x = -\sigma(t+\hat{u}) \oplus \sigma(\hat{t}+\hat{u})$). In particular, $e = 0_H$ iff $\hat{e} = 0_H$; further, when H is abelian, $e = \hat{e}$.

▶ **Lemma 17.** TRSamp_σ *(Figure 5) securely realizes the functionality $\widetilde{\mathcal{F}}_\sigma$ against passive corruption, with statistical security.*

A More Efficient Version. While applicable to all bi-affine correlations, TRSamp_σ has a *rate* of $o(1/\log \lambda)$ in the security parameter λ. Here we present a template which can be used to obtain (a much better) constant rate (in our instantiations, 1/2, without amoritization) in many common examples of bi-affine correlations over large groups. This template is in the form of a passive-secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $(\widehat{\mathcal{F}}_\sigma, \mathcal{E}_\sigma)$-hybrid, where $\mathcal{E}_\sigma$ is an "error

[5] An upperbound on $\binom{d}{1}$-OT^ℓ can be computed by setting $\mathrm{Q} = \mathrm{Y}$ in (5), where $\mathrm{X} = (m_1, \ldots, m_d)$ and $\mathrm{Y} = (b, m_b)$. Then $I(\mathrm{Y}; \mathrm{Y}|\mathrm{X}) = H(\mathrm{Y}|\mathrm{X}) = \log(d)$ since the only remaining entropy in Y given X is the d different choices of b.

Protocol TRSamp_σ in the $\widehat{\mathcal{F}}_\sigma$ hybrid model

Parameter: Let $n := \omega(\log \lambda)$.

- **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets $\{(t^i, a^i)\}_{i\in[n]}$ and Bob gets $\{(u^i, b^i)\}_{i\in[n]}$ from n invocations of $\widehat{\mathcal{F}}_\sigma$.
- **[Cut-and-Choose] Bob $\to$ Alice:**
  - Bob samples a random permutation $\sigma \in S_n$, and sends σ to Alice. Both reorder their correlations as per σ: in the following, we let $t_i := t^{\sigma(i)}$, etc.
  - Bob sends $\{(u_i, b_i)\}_{1\le i\le \frac{n}{2}}$ to Alice. Alice aborts if for any $i \le \frac{n}{2}$, $((t_i, a_i), (u_i, b_i)) \notin C$.
- **[Consistency Check]** For each i such that $\frac{n}{2}+1 < i \le n$, Alice and Bob check the instances i and $i-1$ for consistency:
  - Alice and Bob invoke $\mathsf{Comp}_{\sigma|\mathrm{TAU}}^{(t_{i-1},a_{i-1}),(u_{i-1},b_{i-1})}$ on inputs (t_i, a_i) and u_i respectively, and Bob gets output b_i^*.
  - Bob aborts if $b_i^* \neq b_i$.
- **Output**: Alice outputs (t_n, a_n) and Bob outputs (u_n, b_n).

Figure 5 A passive secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$ hybrid model.

randomization" functionality. Then, $\mathcal{E}_\sigma$ itself is securely realized in the $\widehat{\mathcal{F}}_\sigma$-hybrid, depending on the specifics of the map σ. We implement this latter step only for large groups which satisfy one of three different structural properties.

▶ **Lemma 18.** $\mathsf{altTRSamp}_\sigma$ *(Figure 6) passive-securely realizes the functionality $\widetilde{\mathcal{F}}_\sigma$, in the $\widehat{\mathcal{F}}_\sigma$, $\mathcal{E}_\sigma$ hybrid model*

Error Randomization Functionality. The error randomization functionality $\mathcal{E}_\sigma$ outputs two instances of the correlation $((t_1, a_1), (u_1, b_1))$ and $((t_2, a_2), (u_2, b_2))$ such that either the latter is a valid correlation in BA_σ, or the former has a "high min-entropy error". Relying on this $\mathsf{altTRSamp}_\sigma$ checks one correlation against the other and catches erroneous correlations with overwhelming probability. In our instantiations of $\mathcal{E}_\sigma$, the latter is obtained through an invocation of $\widehat{\mathcal{F}}_\sigma$ and the former is a "randomised" version of the latter such that the new error (if non-zero) has large min-entropy. For details of the error randomization functionality see Figure 7. Depending on the structure of the bi-affine homomorphism $\sigma : Q \to H$, the instantiations need different algebraic properties from the group H:

- **Modules:** A group H is said to be a right-module of a ring R if there is a bi-linear map $\sigma : H \times R \to H$ (i.e., $\sigma((h+h'), r) = \sigma(h, r)+\sigma(h', r)$ and $\sigma(h, (r+r')) = \sigma(h, r)+\sigma(h, r')$) with the additional properties that $\sigma(\sigma(h, r), r') = \sigma(h, (rr'))$ (where the multiplication rr' is from the ring) and $\sigma(h, 1) = h$, where 1 stands for the multiplicative identity in R. Let units(R) denote the set of ring elements $r \in R$ that have a multiplicative inverse in the ring. We define $\mathrm{minimg}_R(H)$ to be the minimum size of the image of units(R) under the map $r \mapsto x \cdot r$, over all non-zero elements x in the module H. i.e.,

  $$\mathrm{minimg}_R(H) = \min_{x\in H\setminus\{0_H\}} |\{x \cdot r | r \in \mathrm{units}(R)\}|.$$

  We require that $\mathrm{minimg}_R(H)$ is super-polynomial in the security parameter. An example is the case when R is a large enough field and H is a vector-space over R, then $\mathrm{minimg}_R(H) = |R| - 1$.

- **Semi-Abelian Bi-affine correlations:** For a group H, we define minord(H) as the order of the smallest non-trivial subgroup of H. Consequently, for all $0 < k <$ minord(H), for all $h \in H \setminus \{0_H\}$, we have $\underbrace{h + \cdots + h}_{k \text{ times}} \neq 0$. minord$(H)$ equals the smallest prime factor of the order of H. For security we require that minord(H) is super-polynomial in the security parameter. An example is a large prime order group H, where minord$(H) = |H|$.
- **Surjective Bi-affine Correlations:** For a (non-abelian) group D, we define minorbit(D) to be the size of the smallest conjugacy class of D, excluding $\{0\}$. That is,

$$\text{minorbit}(D) := \min_{x \in D \setminus \{0\}} |\{r + x - r | r \in D\}|.$$

This instantiation requires the minorbit(D) must be super-polynomial in security parameter. As an example consider the group $\text{SL}(2, 2^n)$[6] – i.e., 2×2 matrices over $\mathbb{F}_{2^n}$, with determinant 1, where minorbit$(\text{SL}(2, 2^n)) \geq 2^n$ [1].

Descriptions of instantiations for the above algebraic objects can be found in the full version.

Protocol $\mathsf{altTRSamp}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$, $\mathcal{E}_\sigma$ hybrid model

- **Invocation of $\widehat{\mathcal{F}}_\sigma$:** Alice gets (t_0, a_0) and Bob gets (u_0, b_0) from $\widehat{\mathcal{F}}_\sigma$.
- **Error-Rerandomization:** Alice and Bob invoke $\mathcal{E}_\sigma$ and receive (t_1, a_1), (t_2, a_2) and (u_1, b_1), (u_2, b_2) respectively.
- **Verification:**
  - Alice and Bob invoke $\mathsf{Comp}_{\sigma|\text{TAU}}^{(t_0,a_0),(u_0,b_0)}$ on inputs (t_1, a_1) and u_1 respectively, and Bob gets output b^*.
  - Bob aborts if $b^* \neq b_1$.
- **Output**: Alice outputs (t_2, a_2) and Bob outputs (u_2, b_2).

Figure 6 A passive-secure protocol for $\widetilde{\mathcal{F}}_\sigma$ in the $\widehat{\mathcal{F}}_\sigma$, $\mathcal{E}_\sigma$ hybrid model.

References

1 Edith Adan-Bante and John M Harris. On conjugacy classes of gl (n, q) and sl (n, q). *arXiv preprint arXiv:0904.2152*, 2009.

2 Donald Beaver. Efficient multiparty protocols using circuit randomization. In *Annual International Cryptology Conference*, pages 420–432. Springer, 1991.

3 Donald Beaver. Foundations of secure interactive computing. In *Annual International Cryptology Conference*, pages 377–391. Springer, 1991.

4 Donald Beaver. Commodity-based cryptography. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 446–455, 1997.

5 Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators: Silent OT extension and more. In *CRYPTO*, volume 11694, pages 489–518. Springer, 2019.

6 Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Correlated pseudorandom functions from variable-density lpn. Cryptology ePrint Archive, Report 2020/1417, 2020.

[6] Every element in the group also has a succinct representation using $O(n)$ bits.

Functionality $\mathcal{E}_\sigma$

Parameters: $\ell = \omega(\log \lambda)$, groups $(H, \oplus), (Q, +)$ and $T, U \subseteq Q$, bi-affine $\sigma : Q \to H$ w.r.t T, Q

- If Alice and Bob are both honest:
  - Adversary specifies a distribution $\mathcal{D}$ over $(T \times H) \times (U \times H)$, and a pair $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big)$.
  - Define the distribution E_{u_0}, for each $u_0 \in U$, as

$$E_{u_0} := \{-x \oplus e \oplus x\}_{\big((t,a),(u,b)\big) \leftarrow \mathcal{D}, e := -\sigma(t+u) \oplus a \oplus b, x := \sigma(t+u_0)}$$

    - If $\big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big) \in \mathsf{BA}_\sigma$ or, $\forall u_0 \in U$, $\mathrm{H}_\infty(E_{u_0}) \geq \ell$, then let $\big((t_2, a_2), (u_2, b_2)\big) := \big((\tilde{t}, \tilde{a}), (\tilde{u}, \tilde{b})\big)$.
    - Else sample $\big((t_2, a_2), (u_2, b_2)\big) \leftarrow \mathsf{BA}_\sigma$.
  - Sample $\big((t_1, a_1), (u_1, b_1)\big) \leftarrow \mathcal{D}$.
- If Alice is corrupt:
  - Adversary specifies (t_1, a_1) and $(t_2, a_2) \in T \times H$ along with a function $\xi : T \times H \to T \times H$
  - Sample $u_2 \leftarrow U$ and let $b_2 := -a_2 \oplus \sigma(t_2 + u_2)$. Compute $(u_1, b_1) = \xi(u_2, b_2)$.
  - Check if $\big((t_1, a_1), (u_1, b_1)\big) \in \mathsf{BA}_\sigma$. If not, then sample $u_1 \leftarrow U$ and set $b_1 = -a_1 \oplus \sigma(t_1 + u_1)$
- If Bob is corrupt:
  - Adversary specifies (u_1, b_1) and $(u_2, b_2) \in U \times H$ along with a function $\xi : U \times H \to U \times H$
  - Sample $t_2 \leftarrow T$ and let $a_2 := \sigma(t_2 + u_2) \oplus -b_2$. Compute $(t_1, a_1) = \xi(t_2, a_2)$.
  - Check if $\big((t_1, a_1), (u_1, b_1)\big) \in \mathsf{BA}_\sigma$. If not, then sample $t_1 \leftarrow T$ and set $a_1 = \sigma(t_1 + u_1) \oplus -b_1$
- Send (t_1, a_1) and (t_2, a_2) to Alice and (u_1, b_1) and (u_2, b_2) to Bob.

Figure 7 The error randomization functionality for bi-affine homomorphism σ.

7 Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators from ring-lpn. In *CRYPTO*, pages 387–416. Springer, 2020.

8 Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, and Michele Orrù. Homomorphic secret sharing: optimizations and applications. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 2105–2122, 2017.

9 Elette Boyle, Niv Gilboa, and Yuval Ishai. Secure computation with preprocessing via function secret sharing. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2019.

10 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. In *Annual Cryptology Conference*, pages 185–202. Springer, 2013.

11 Ronald Cramer, Serge Fehr, Yuval Ishai, and Eyal Kushilevitz. Efficient multi-party computation over rings. In *EUROCRYPT*, pages 596–613, 2003. URL: `http://link.springer.de/link/service/series/0558/bibs/2656/26560596.htm`.

12 Ivan Damgård, Helene Haagh, Michael Nielsen, and Claudio Orlandi. Commodity-based 2pc for arithmetic circuits. In *IMA International Conference on Cryptography and Coding*, pages 154–177. Springer, 2019.

13 Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P Smart. Practical covertly secure mpc for dishonest majority–or: breaking the spdz limits. In *European Symposium on Research in Computer Security*, pages 1–18. Springer, 2013.

14 Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Annual Cryptology Conference*, pages 643–662. Springer, 2012.

15 Daniel Demmler, Thomas Schneider, and Michael Zohner. ABY - A framework for efficient mixed-protocol secure two-party computation. In *NDSS*. The Internet Society, 2015.

16 Yvo Desmedt, Josef Pieprzyk, and Ron Steinfeld. Active security in multiparty computation over black-box groups. In *International Conference on Security and Cryptography for Networks*, pages 503–521. Springer, 2012.

17 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. *J. Cryptology*, 25(4):557–600, 2012.

18 P. Gács and J. Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973.

19 Niv Gilboa. Two party rsa key generation. In *CRYPTO*, pages 116–129, 1999. URL: `http://link.springer.de/link/service/series/0558/bibs/1666/16660116.htm`.

20 Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In *CRYPTO*, pages 572–591, 2008. `doi:10.1007/978-3-540-85174-5_32`.

21 Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Secure arithmetic computation with no honest majority. In *TCC*, pages 294–314, 2009. `doi:10.1007/978-3-642-00457-5_16`.

22 Joe Kilian. Founding cryptography on oblivious transfer. In *STOC*, pages 20–31, 1988.

23 Joe Kilian. More general completeness theorems for secure two-party computation. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 316–324, 2000.

24 Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. A unified characterization of completeness and triviality for secure function evaluation. In *INDOCRYPT*, pages 40–59, 2012.

25 Vinod M Prabhakaran and Manoj M Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Transactions on Information Theory*, 60(6):3413–3434, 2014.

26 Claude Shannon. A mathematical theory of communications. *Bell System Technical Journal*, 27:379–423, July 1948.

27 Nigel P Smart and Titouan Tanguy. Taas: Commodity mpc via triples-as-a-service. In *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*, pages 105–116, 2019.

28 A. D. Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975.