Actively Secure Half-Gates with Minimum Overhead Under Duplex Networks

Hongrui Cui[1], Xiao Wang[2], Kang Yang[3](✉), and Yu Yu[1,4]

[1] Shanghai Jiao Tong University, Shanghai, China
{rickfreeman,yyuu}@sjtu.edu.cn
[2] Northwestern University, Evanston, USA
wangxiao@cs.northwestern.edu
[3] State Key Laboratory of Cryptology, Beijing, China
yangk@sklc.org
[4] Shanghai Qi Zhi Institute, Shanghai, China

Abstract. Actively secure two-party computation (2PC) is one of the canonical building blocks in modern cryptography. One main goal for designing actively secure 2PC protocols is to reduce the communication overhead, compared to semi-honest 2PC protocols. In this paper, we propose a new actively secure constant-round 2PC protocol with one-way communication of $2\kappa+5$ bits per AND gate (for κ-bit computational security and any statistical security), essentially matching the one-way communication of semi-honest half-gates protocol. This is achieved by two new techniques:

1. The recent compression technique by Dittmer et al. (Crypto 2022) shows that a relaxed preprocessing is sufficient for authenticated garbling that does not reveal masked wire values to the garbler. We introduce a new form of authenticated bits and propose a new technique of generating authenticated AND triples to reduce the one-way communication of preprocessing from $5\rho + 1$ bits to 2 bits per AND gate for ρ-bit statistical security.
2. Unfortunately, the above compressing technique is only compatible with a less compact authenticated garbled circuit of size $2\kappa + 3\rho$ bits per AND gate. We designed a new authenticated garbling that does not use information theoretic MACs but rather dual execution without leakage to authenticate wire values in the circuit. This allows us to use a more compact half-gates based authenticated garbled circuit of size $2\kappa + 1$ bits per AND gate, and meanwhile keep compatible with the compression technique. Our new technique can achieve one-way communication of $2\kappa + 5$ bits per AND gate.

Our technique of yielding authenticated AND triples can also be used to optimize the two-way communication (i.e., the total communication) by combining it with the authenticated garbled circuits by Dittmer et al., which results in an actively secure 2PC protocol with two-way communication of $2\kappa + 3\rho + 4$ bits per AND gate.

Keywords: Actively secure 2PC · Garbled circuit · Correlated oblivious transfer

1 Introduction

Based on garbled circuits (GCs) [44], constant-round secure two-party computation (2PC) has obtained huge practical improvements in recent years in both communication [5,30,35,45] and computation [6,22,23]. However, compared to passively secure (a.k.a., semi-honest) 2PC protocols, their actively secure counterparts require significant overhead. Building upon the authenticated garbling framework [29,36,37,42] and, more generally, working in the BMR family [5,24,26,31,32], the most recent work by Dittmer, Ishai, Lu and Ostrovsky [16] (denoted as DILO hereafter) is able to bring down the communication cost to $2\kappa + 8\rho + O(1)$ bits per AND gate, where κ and ρ are the computational and statistical security parameters, respectively.

Although huge progress, there is still a gap between actively secure and passively secure 2PC protocols based on garbled circuits. In particular, the size of a garbled circuit has been recently reduced from 2κ bits (half-gates [45]) to 1.5κ bits (three-halves [35]) per AND gate, while even the latest authenticated garbling cannot reach the communication efficiency of half-gates. It is possible to close this gap between active and passive security using the GMW compiler [21], and its concrete efficiency was studied in [1]. However, it requires non-black-box use of the underlying garbling scheme and thus requires prohibitive overhead.

Bringing down the cost of authenticated garbling at this stage requires overcoming several challenges. First of all, we need the authenticated GC itself to be as small as the underlying GC construction. This could be achieved for half-gates as Katz et al. [29] (denoted as KRRW hereafter) proposed an authenticated half-gates construction in the two-party setting. However, when it comes to three-halves, there is no known construction. These authenticated GCs are usually generated in some preprocessing model, and thus the second challenge is to instantiate the preprocessing with only *constant additive overhead*. Together with recent works on pseudorandom correlation generators (PCGs) [9–11,13,43], Katz et al. [29] can achieve $O(\kappa)$ bits per AND gate, while Dittmer et al. [16] can achieve $O(\rho)$ bits per AND gate. However, the latest advancement by Dittmer et al. [16] is not compatible with the optimal authenticated half-gates construction and requires an authenticated GC of size $2\kappa + 3\rho$ bits per AND gate.

1.1 Our Contribution

We make significant progress in closing the communication gap between passive and active GC-based 2PC protocols by proposing a new actively secure 2PC protocol with constant rounds and one-way communication essentially the same as the half-gates 2PC protocol in the semi-honest setting.

1. We manage to securely instantiate the preprocessing phase with $O(1)$ bits per AND gate. Our starting point is the compression technique by Dittmer et al. [16], who showed that in authenticated garbling, the random masks of the evaluator need not be of full entropy and can be compressed with entropy sublinear to the circuit size. This observation leads to an efficient construction

Table 1. Comparing our protocol with prior works in terms of round and communication complexity. Here κ, ρ denote the computational and statistical security parameters instantiated by 128 and 40 respectively. Round complexity is counted in the random COT/VOLE-hybrid model. One-way communication is the greater of the two parties' communication; two-way communication is the sum of all communication. For the KRRW and HSS protocol we take the bucket size as $B = 3$.

Security	2PC	Correlation	Rounds		Communication per AND gate	
			Prep.	Online	one-way (bits)	two-way (bits)
Passive	Half-gates	OT	1	2	2κ	2κ
Active	HSS-PCG [25]	OT	8	2	$8\kappa + 11$ ($4.04\times$)	$16\kappa + 22$ ($8.09\times$)
Active	KRRW-PCG [29]	COT	4	4	$5\kappa + 7$ ($2.53\times$)	$8\kappa + 14$ ($4.05\times$)
Active	DILO [16]	VOLE	7	2	$2\kappa + 8\rho + 1$ ($2.25\times$)	$2\kappa + 8\rho + 5$ ($2.27\times$)
Active	This work	COT	8	3	$2\kappa + 5$ ($\approx \mathbf{1}\times$)	$4\kappa + 10$ ($2.04\times$)
Active	This work+DILO	COT	8	2	$2\kappa + 3\rho + 2$ ($1.48\times$)	$2\kappa + 3\rho + 4$ ($\approx \mathbf{1.48}\times$)

from vector oblivious linear evaluation (VOLE) to the desired preprocessing functionality. This reduces the communication overhead of preprocessing to $5\rho + 1$ bits per AND gate. To further reduce their communication, we introduce a new tool called "dual-key authentication". Intuitively this form of authentication allows two parties to commit to a value that can later be checked against subsequent messages by both parties. Together with a new technique of generating authenticated AND triples from correlated oblivious transfer (COT), we avoid the ρ-time blow-up of the DILO protocol, and the one-way communication cost is reduced to 2 bits per AND gate.

2. As mentioned earlier, the above compression technique is not compatible with KRRW authenticated half-gates; this is because the compression technique requires that the garbler does not learn the masked values since the entropy of wire masks provided by the evaluator is low. We observe that the dual-execution protocol [27,28] can essentially be used for this purpose, and it is highly compatible with the authenticated garbling technique. In particular, the masked value of each wire is implicitly authenticated by the garbled label. Therefore we can perform two independent executions and check the actual value of each wire against each other. Since every wire is checked, we are able to eliminate the 1-bit leakage in ordinary dual-execution protocols. The overall one-way communication is $2\kappa + 5$ bits per AND gate.

We note that this is only a partial solution because dual execution requires both parties to send GCs. Under full-duplex networks (e.g., most wired communication) where communication in both directions can happen simultaneously, this effectively imposes no slow down; however, for half-duplex networks (e.g., most wireless communication), it would not be a preferable option. Nevertheless, our preprocessing protocol can be combined with the construction of authenticated garbled circuits by Dittmer et al. [16] to achieve the best two-way communication of $2\kappa + 3\rho + 4$ bits per AND gate, leading to a $1.53\times$ improvement. We provide a detailed comparison in Table 1.

We do not compare our actively secure 2PC protocol with the protocol (denoted by DILOv2) by Dittmer et al. [16] building on doubly authenticated multiplication triples. Compared to DILO, the DILOv2 protocol is less efficient, as DILOv2 requires quasi-linear computational complexity. Moreover, DILOv2 can only generate authenticated triples over $\mathbb{F}_{2^\rho}$, while authenticated garbling requires triples over $\mathbb{F}_2$. This incurs a ρ-time overhead when utilizing such triples.

2 Preliminaries

2.1 Notation

We use κ and ρ to denote the computational and statistical security parameters, respectively. We use log to denote logarithms in base 2. We write $x \leftarrow S$ to denote sampling x uniformly at random from a finite set S. We define $[a, b) = \{a, \ldots, b-1\}$ and write $[a, b] = \{a, \ldots, b\}$. We use bold lower-case letters like $\boldsymbol{a}$ for column vectors, and bold upper-case letters like $\mathbf{A}$ for matrices. We let a_i denote the i-th component of $\boldsymbol{a}$ (with a_1 the first entry). We use $\{x_i\}_{i \in S}$ to denote the set that consists of all elements with indices in set S. When the context is clear, we abuse the notation and use $\{x_i\}$ to denote such a set. For a string x, we use $\mathsf{lsb}(x)$ to denote the least significant bit (LSB) and $\mathsf{msb}(x)$ to denote the most significant bit (MSB).

For an extension field $\mathbb{F}_{2^\kappa}$ of a binary field $\mathbb{F}_2$, we fix some monic, irreducible polynomial $f(X)$ of degree κ and then write $\mathbb{F}_{2^\kappa} \cong \mathbb{F}_2[X]/f(X)$. Thus, every element $x \in \mathbb{F}_{2^\kappa}$ can be denoted uniquely as $x = \sum_{i \in [0,\kappa)} x_i \cdot X^i$ with $x_i \in \mathbb{F}_2$ for all $i \in [0, \kappa)$. We could view elements over $\mathbb{F}_{2^\kappa}$ equivalently as vectors in $\mathbb{F}_2^\kappa$ or strings in $\{0, 1\}^\kappa$, and consider a bit $x \in \mathbb{F}_2$ as an element in $\mathbb{F}_{2^\kappa}$. Depending on the context, we use $\{0, 1\}^\kappa$, $\mathbb{F}_2^\kappa$ and $\mathbb{F}_{2^\kappa}$ interchangeably, and thus addition in $\mathbb{F}_2^\kappa$ and $\mathbb{F}_{2^\kappa}$ corresponds to XOR in $\{0, 1\}^\kappa$. We also define two macros to convert between $\mathbb{F}_{2^\kappa}$ and $\mathbb{F}_2^\kappa$.

- $x \leftarrow \mathsf{B2F}(\boldsymbol{x})$: Given $\boldsymbol{x} = (x_0, ..., x_{\kappa-1}) \in \mathbb{F}_2^\kappa$, output $x := \sum_{i \in [0,\kappa)} x_i \cdot X^i \in \mathbb{F}_{2^\kappa}$.
- $\boldsymbol{x} \leftarrow \mathsf{F2B}(x)$: Given $x = \sum_{i \in [0,\kappa)} x_i \cdot X^i \in \mathbb{F}_{2^\kappa}$, output $\boldsymbol{x} = (x_0, ..., x_{\kappa-1}) \in \mathbb{F}_2^\kappa$.

A Boolean circuit $\mathcal{C}$ consists of a list of gates in the form of (i, j, k, T), where i, j are the indices of input wires, k is the index of output wire and $T \in \{\oplus, \wedge\}$ is the type of the gate. In the 2PC setting, we use $\mathcal{I}_\mathsf{A}$ (resp., $\mathcal{I}_\mathsf{B}$) to denote the set of circuit-input wire indices corresponding to the input of P_A (resp., P_B). We also use $\mathcal{W}$ to denote the set of output-wire indices of all AND gates, and $\mathcal{O}$ to denote the set of circuit-output wire indices in the circuit $\mathcal{C}$. We denote by $\mathcal{C}_\mathsf{and}$ the set of all AND gates in the form of (i, j, k, T).

Our protocol in the two-party setting is proven secure against static and malicious adversaries in the standard simulation-based security model [12,20]. We recall the security model, a relaxed equality-check functionality $\mathcal{F}_\mathsf{EQ}$ and the coin-tossing functionality $\mathcal{F}_\mathsf{Rand}$ as well as the summary of the notations and macros used in our protocols in the full version [14].

2.2 Information-Theoretic Message Authentication Codes

We use information-theoretic message authentication codes (IT-MACs) [7,34] to authenticate bits or field elements in $\mathbb{F}_{2^\kappa}$. Specifically, let $\varDelta \in \mathbb{F}_{2^\kappa}$ be a *global key*. We adopt $[x] = (\mathsf{K}[x], \mathsf{M}[x], x)$ to denote that an element $x \in \mathbb{F}$ (where $\mathbb{F} \in \{\mathbb{F}_2, \mathbb{F}_{2^\kappa}\}$) known by one party can be authenticated by the other party who holds $\varDelta \in \mathbb{F}_{2^\kappa}$ and a *local key* $\mathsf{K}[x] \in \mathbb{F}_{2^\kappa}$, where an MAC tag $\mathsf{M}[x] = \mathsf{K}[x] + x \cdot \varDelta \in \mathbb{F}_{2^\kappa}$ is given to the party holding x. For a vector $\boldsymbol{x} \in \mathbb{F}^\ell$, we denote by $[\boldsymbol{x}] = ([x_1], ..., [x_\ell])$ a vector of authenticated values. We refer to $([x], [y], [z])$ with $z = x \cdot y$ as an authenticated multiplication triple. If $x, y, z \in \{0, 1\}$, this tuple is also called authenticated AND triple. For a constant value $c \in \mathbb{F}_{2^\kappa}$, it is easy to define $[c] = (c \cdot \varDelta, 0^\kappa, c)$. It is well-known that IT-MACs are additively homomorphic. That is, given public coefficients $c_0, c_1, \ldots, c_\ell \in \mathbb{F}_{2^\kappa}$, two parties can *locally* compute $[y] := c_0 + \sum_{i=1}^{\ell} c_i \cdot [x_i]$.

When applying IT-MACs into 2PC, secret values are authenticated by either $\mathsf{P_A}$ or $\mathsf{P_B}$. We use subscripts A and B in authenticated values to distinguish which party ($\mathsf{P_A}$ or $\mathsf{P_B}$) holds the secret values. For example, $[x]_\mathsf{A} = (\mathsf{K_B}[x], \mathsf{M_A}[x], x)$ denotes that $\mathsf{P_A}$ holds $(x, \mathsf{M_A}[x])$ and $\mathsf{P_B}$ holds $(\varDelta_\mathsf{B}, \mathsf{K_B}[x])$. In the case that other global keys are used, we explicitly add a subscript to keys and MAC tags. For example, when $G \in \mathbb{F}_{2^\kappa}$ is used and held by $\mathsf{P_B}$, we write $[x]_{\mathsf{A},G} = (\mathsf{K_B}[x]_G, \mathsf{M_A}[x]_G, x)$ and $\mathsf{M_A}[x]_G = \mathsf{K_B}[x]_G + x \cdot G$. When the context is clear, we will omit the subscripts A and B for the sake of simplicity.

Batch Opening of Authenticated Values. In the following, we describe the known procedure [15,34] to open authenticated values in a batch. Here we always assume that $\mathsf{P_A}$ holds the values and MAC tags, and $\mathsf{P_B}$ holds the global and local keys. In this case, we write $[x]$ instead of $[x]_\mathsf{A}$. For the case that $\mathsf{P_B}$ holds the values authenticated by $\mathsf{P_A}$, these procedures can be defined similarly. We first define the following procedure (denoted by $\mathsf{CheckZero}$) to check that all values are zero in constant small communication.

- $\mathsf{CheckZero}([x_1], \ldots, [x_\ell])$: On input authenticated values $[x_1], \ldots, [x_\ell]$, $\mathsf{P_A}$ convinces $\mathsf{P_B}$ that $x_i = 0$ for all $i \in [1, \ell]$ as follows:
  1. $\mathsf{P_A}$ sends $h := \mathsf{H}(\mathsf{M_A}[x_1], \ldots, \mathsf{M_A}[x_\ell])$ to $\mathsf{P_B}$, where $\mathsf{H} : \{0,1\}^* \to \{0,1\}^\kappa$ is a random oracle.
  2. $\mathsf{P_B}$ computes $h' := \mathsf{H}(\mathsf{K_B}[x_1], \ldots, \mathsf{K_B}[x_\ell])$ and checks that $h = h'$. If the check fails, $\mathsf{P_B}$ aborts.

Following previous works [15,38], we have the following lemma.

Lemma 1. *If $\varDelta \in \mathbb{F}_{2^\kappa}$ is sampled uniformly at random, then the probability that there exists some $i \in [1, \ell]$ such that $x_i \neq 0$ and $\mathsf{P_B}$ accepts in the $\mathsf{CheckZero}$ procedure is bounded by $\frac{2}{2^\kappa}$.*

The above lemma can be relaxed by allowing that $\varDelta$ is sampled uniformly from a set $\mathcal{R} \subset \mathbb{F}_{2^\kappa}$. In this case, the success probability for a cheating party $\mathsf{P_A}$ is at most $\frac{1}{|\mathcal{R}|} + \frac{1}{2^\kappa}$. Based on the $\mathsf{CheckZero}$ procedure, we define the following batch-opening procedure (denoted by Open):

Functionality $\mathcal{F}_{\mathsf{bCOT}}^{L}$

This functionality is parameterized by an integer $L \geq 1$. Running with a sender $\mathsf{P_A}$, a receiver $\mathsf{P_B}$ and an ideal adversary, it operates as follows.

Initialize. Upon receiving $(\mathsf{init}, sid, \Delta_1, ..., \Delta_L)$ from $\mathsf{P_A}$ and (init, sid) from $\mathsf{P_B}$ where $\Delta_i \in \mathbb{F}_{2^\kappa}$ for all $i \in [1, L]$, store $(sid, \Delta_1, ..., \Delta_L)$ and then ignore all subsequent (init, sid) commands.

Extend. Upon receiving $(\mathsf{extend}, sid, \ell)$ from $\mathsf{P_A}$ and $\mathsf{P_B}$, do the following:

- For $i \in [1, L]$, if $\mathsf{P_A}$ is honest, sample $\mathsf{K_A}[\boldsymbol{u}]_{\Delta_i} \leftarrow \mathbb{F}_{2^\kappa}^{\ell}$; otherwise, receive $\mathsf{K_A}[\boldsymbol{u}]_{\Delta_i} \in \mathbb{F}_{2^\kappa}^{\ell}$ from the adversary.
- If $\mathsf{P_B}$ is honest, sample $\boldsymbol{u} \leftarrow \mathbb{F}_2^{\ell}$ and compute $\mathsf{M_B}[\boldsymbol{u}]_{\Delta_i} := \mathsf{K_A}[\boldsymbol{u}]_{\Delta_i} + \boldsymbol{u} \cdot \Delta_i \in \mathbb{F}_{2^\kappa}^{\ell}$ for $i \in [1, L]$. Otherwise, receive $\boldsymbol{u} \in \mathbb{F}_2^{\ell}$ and $\mathsf{M_B}[\boldsymbol{u}]_{\Delta_i} \in \mathbb{F}_{2^\kappa}^{\ell}$ for $i \in [1, L]$ from the adversary, and recomputes $\mathsf{K_A}[\boldsymbol{u}]_{\Delta_i} := \mathsf{M_B}[\boldsymbol{u}]_{\Delta_i} + \boldsymbol{u} \cdot \Delta_i \in \mathbb{F}_{2^\kappa}^{\ell}$ for $i \in [1, L]$.
- For $i \in [1, L]$, output $(sid, \mathsf{K_A}[\boldsymbol{u}]_{\Delta_i})$ to $\mathsf{P_A}$ and $(sid, \boldsymbol{u}, \mathsf{M_B}[\boldsymbol{u}]_{\Delta_i})$ to $\mathsf{P_B}$.

Fig. 1. Functionality for block correlated oblivious transfer.

- $\mathsf{Open}([x_1], \ldots, [x_\ell])$: On input authenticated values $[x_1], \ldots, [x_\ell]$ defined over field $\mathbb{F}_{2^\kappa}$, $\mathsf{P_A}$ opens these values as follows:
  1. $\mathsf{P_A}$ sends $(x_1, \ldots, x_\ell)$ to $\mathsf{P_B}$, and then both parties set $[y_i] := [x_i] + x_i$ for each $i \in [1, \ell]$.
  2. $\mathsf{P_A}$ runs $\mathsf{CheckZero}([y_1], \ldots, [y_\ell])$ with $\mathsf{P_B}$. If $\mathsf{P_B}$ does not abort, it outputs $(x_1, \ldots, x_\ell)$.

2.3 Correlated Oblivious Transfer

Our 2PC protocol will adopt the standard functionality [10,43] of correlated oblivious transfer (COT) to generate random authenticated bits. This functionality (denoted by $\mathcal{F}_{\mathsf{COT}}$) is shown in Fig. 1 by setting a parameter $L = 1$, where the extension phase can be executed multiple times for the same session identifier *sid*. Based on Learning Parity with Noise (LPN) [8], the recent protocols [9,10,13,43] with *sublinear* communication and *linear* computation can securely realize the COT functionality in the presence of malicious adversaries. In particular, these protocols can generate a COT correlation with amortized communication cost of about $0.1 \sim 0.4$ bits.

We also generalize the COT functionality into block COT (bCOT) [16], which allows to generate authenticated bits with the same choice bits and different global keys. Functionality $\mathcal{F}_{\mathsf{bCOT}}^{L}$ shown in Fig. 1 is the same as the standard COT functionality, except that L vectors (rather than a single vector) of authenticated bits $[\boldsymbol{u}]_{\mathsf{B},\Delta_1}, \ldots, [\boldsymbol{u}]_{\mathsf{B},\Delta_L}$ are generated. Here the vector of choice bits $\boldsymbol{u}$ is required to be identical in different vectors of authenticated bits. It is easy to see that $\mathcal{F}_{\mathsf{COT}}$ is a special case of $\mathcal{F}_{\mathsf{bCOT}}^{L}$ with $L = 1$. The protocol that securely realizes functionality $\mathcal{F}_{\mathsf{bCOT}}^{L}$ is easy to be constructed by extending the LPN-based COT protocol as described above. Specifically, we set $\Delta = (\Delta_1, \ldots, \Delta_L) \in \mathbb{F}_{2^\kappa}^{L} \cong \mathbb{F}_{2^{\kappa L}}$ as the global key in the LPN-based COT protocol, and the resulting choice-bits are authenticated over extension field $\mathbb{F}_{2^{\kappa L}}$.

Functionality $\mathcal{F}_{\mathsf{DVZK}}$

This functionality runs with a prover $\mathcal{P}$ and a verifier $\mathcal{V}$, and operates as follows:

- Upon receiving $(\mathsf{dvzk}, sid, \ell, \{[x_i], [y_i], [z_i]\}_{i \in [1,\ell]})$ from $\mathcal{P}$ and $\mathcal{V}$ where $x_i, y_i, z_i \in \mathbb{F}_{2^\kappa}$ for all $i \in [1, \ell]$, if there exists some $i \in [1, \ell]$ such that one of $[x_i], [y_i], [z_i]$ is not valid, output (sid, false) to $\mathcal{V}$ and abort.
- Check that $z_i = x_i \cdot y_i \in \mathbb{F}_{2^\kappa}$ for all $i \in [1, \ell]$. If the check passes, then output (sid, true) to $\mathcal{V}$, else output (sid, false) to $\mathcal{V}$.

Fig. 2. Functionality for DVZK proofs of authenticated multiplication triples.

Note that the protocol to generate block COTs still has *sublinear* communication, if L is sublinear to the number of the resulting COT correlations.

While the COT functionality outputs random authenticated bits, we can convert them into chosen authenticated bits via the following procedure (denoted by Fix), which is also used in the recent DVZK protocol [4].

- $([\boldsymbol{x}]_{\mathsf{B},\Delta_1}, \ldots, [\boldsymbol{x}]_{\mathsf{B},\Delta_L}) \leftarrow \mathsf{Fix}(sid, \boldsymbol{x})$: On input a session identifier sid of $\mathcal{F}_{\mathsf{bCOT}}$, and a vector $\boldsymbol{x} \in \mathbb{F}_2^\ell$ from $\mathsf{P_B}$, two parties $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the following:
  1. Both parties call $\mathcal{F}_{\mathsf{bCOT}}^L$ on input $(\mathsf{extend}, sid, \ell)$ to obtain $([\boldsymbol{r}]_{\mathsf{B},\Delta_1}, \ldots, [\boldsymbol{r}]_{\mathsf{B},\Delta_L})$ with a random vector $\boldsymbol{r} \in \mathbb{F}_2^\ell$ held by $\mathsf{P_B}$, where $\mathcal{F}_{\mathsf{bCOT}}^L$ has been initialized by sid and $(\Delta_1, \ldots, \Delta_L)$.
  2. $\mathsf{P_B}$ sends $\boldsymbol{d} := \boldsymbol{x} \oplus \boldsymbol{r}$ to $\mathsf{P_A}$.
  3. For each $i \in [1, L]$, both parties set $[\boldsymbol{x}]_{\mathsf{B},\Delta_i} := [\boldsymbol{r}]_{\mathsf{B},\Delta_i} \oplus \boldsymbol{d}$.

For a field element $x \in \mathbb{F}_{2^\kappa}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ can run $\boldsymbol{x} \leftarrow \mathsf{F2B}(x)$, $([\boldsymbol{x}]_{\mathsf{B},\Delta_1}, \ldots, [\boldsymbol{x}]_{\mathsf{B},\Delta_L}) \leftarrow \mathsf{Fix}(sid, \boldsymbol{x})$ and $([x]_{\mathsf{B},\Delta_1}, \ldots, [x]_{\mathsf{B},\Delta_L}) \leftarrow \mathsf{B2F}([\boldsymbol{x}]_{\mathsf{B},\Delta_1}, \ldots, [\boldsymbol{x}]_{\mathsf{B},\Delta_L})$ to obtain the corresponding authenticated values. Note that $\mathsf{B2F}$ only involves the operations multiplied by public elements $X, \ldots, X^{\kappa-1} \in \mathbb{F}_{2^\kappa}$, and thus $([x]_{\mathsf{B},\Delta_1}, \ldots, [x]_{\mathsf{B},\Delta_L})$ can be computed locally by running $\mathsf{B2F}$. For simplicity, we abuse the Fix notation, and use $([x]_{\mathsf{B},\Delta_1}, \ldots, [x]_{\mathsf{B},\Delta_L}) \leftarrow \mathsf{Fix}(sid, x)$ to denote the conversion procedure. The Fix procedure is easy to be generalized to support that the values are defined over any field $\mathbb{F}$ such as $\mathbb{F} = \mathbb{F}_{2^\rho}$. The Fix procedure is totally similar for generating authenticated bits $[\boldsymbol{x}]_{\mathsf{A},\Delta_1}, \ldots, [\boldsymbol{x}]_{\mathsf{A},\Delta_L}$ from random authenticated bits, where here $\mathsf{P_B}$ holds $(\Delta_1, \ldots, \Delta_L)$. When the context is clear, we just write $([\boldsymbol{x}]_{\Delta_1}, \ldots, [\boldsymbol{x}]_{\Delta_L}) \leftarrow \mathsf{Fix}(sid, \boldsymbol{x})$ for simplicity. We further extend Fix to additionally allow to input vectors of random authenticated bits instead of calling $\mathcal{F}_{\mathsf{bCOT}}^L$, which is denoted by $[\boldsymbol{x}] \leftarrow \mathsf{Fix}(\boldsymbol{x}, [\boldsymbol{r}])$ for the case of $L = 1$.

2.4 Designated-Verifier Zero-Knowledge Proofs

Based on IT-MACs, a family of streamable designated-verifier zero-knowledge (DVZK) proofs with fast prover time and a small memory footprint has been proposed [2–4,17,18,38–41]. While these DVZK proofs can prove arbitrary circuits, we only need them to prove a simple multiplication relation. Specifically, given a set of authenticated triples $\{([x_i], [y_i], [z_i])\}_{i \in [1,\ell]}$ over $\mathbb{F}_{2^\kappa}$, these DVZK protocols can enable a prover $\mathcal{P}$ to convince a verifier $\mathcal{V}$ that $z_i = x_i \cdot y_i$ for all $i \in [1, \ell]$. This is modeled by an ideal functionality shown in Fig. 2. In this functionality, an authenticated value $[x]$ is input by two parties $\mathcal{P}$ and $\mathcal{V}$, meaning that $\mathcal{P}$ inputs (x, M) and $\mathcal{V}$ inputs $(\mathsf{K}, \varDelta)$. We say that $[x]$ is valid, if $\mathsf{M} = \mathsf{K} + x \cdot \varDelta$. Using the recent DVZK proofs, this functionality can be *non-interactively* realized in the random-oracle model using constant small communication (e.g., 2κ bits in total [41]).

3 Technical Overview

In this section, we give an overview of our techniques. The detailed protocols and their formal proofs are described in later sections. Firstly, we recall the basic approach in the state-of-the-art solution [16].

3.1 Overview of the State-of-the-Art Solution

Recently, Dittmer, Ishai, Lu and Ostrovsky [16] constructed the state-of-the-art 2PC protocol with malicious security (denoted by DILO) from simple VOLE correlations.[1] For one-way communication, this protocol takes $5\rho + 1$ bits to generate a single authenticated AND triple and $2\kappa + 3\rho$ bits per AND gate to produce one distributed garbled circuit. Their approach is outlined as follows.

In the framework of authenticated garbling [36], for each AND gate $(i, j, k, \wedge)$, the garbler $\mathsf{P_A}$ and evaluator $\mathsf{P_B}$ need to generate one authenticated triple $([a_i], [b_i], [a_j], [b_j], [\hat{a}_k], [\hat{b}_k])$ such that $\hat{a}_k \oplus \hat{b}_k = (a_i \oplus b_i) \wedge (a_j \oplus b_j)$. Let $\boldsymbol{b} \in \mathbb{F}_2^n$ (resp., $\boldsymbol{b}_{\mathcal{I}} \in \mathbb{F}_2^m$) be the vector of random masks $\{b_i\}$ held by $\mathsf{P_B}$ on the output wires of all AND gates (resp., on all circuit-input wires associated with the $\mathsf{P_B}$'s input), where n is the number of all AND gates and m is the number of all circuit-input gates. The key observation by Dittmer et al. [16] is that only evaluator $\mathsf{P_B}$ can compute masked wire values (i.e., the XOR of actual wire values and random masks), and thus $\boldsymbol{b}$ is unnecessary to be uniformly random if the masked wire values are *not* revealed to $\mathsf{P_A}$. In particular, when these masked wire values are not revealed by $\mathsf{P_B}$, a malicious garbler $\mathsf{P_A}$ can only guess some masked wire values by performing a selective-failure attack. This means that for each masked wire value, $\mathsf{P_A}$ can guess correctly with probability 1/2, and the protocol execution will abort for an incorrect guess. In this case, $\mathsf{P_A}$ can guess at most $\rho - 1$ masked wire values, and otherwise the protocol will abort with probability at least $1 - 1/2^\rho$. The core idea of DILO is to compress vector $\boldsymbol{b}$ by defining $\boldsymbol{b} = \mathbf{M} \cdot \boldsymbol{b}^*$, where $\mathbf{M} \in \mathbb{F}_2^{n \times L}$ is a public matrix such that any ρ rows of $\mathbf{M}$ are linearly independent, $\boldsymbol{b}^* \in \mathbb{F}_2^L$ is a uniform vector and $L = O(\rho \log(n/\rho))$. Since IT-MACs are additively homomorphic, two parties only need to generate $[\boldsymbol{b}^*]$ (instead of $[\boldsymbol{b}]$) for a much shorter vector $\boldsymbol{b}^*$, and then compute $[\boldsymbol{b}] := \mathbf{M} \cdot [\boldsymbol{b}^*]$.

[1] VOLE is an arithmetic generalization of COT, and enables $\mathsf{P_A}$ to obtain $(\varDelta, \mathsf{K}[\boldsymbol{u}]) \in \mathbb{F} \times \mathbb{F}^\ell$ and $\mathsf{P_B}$ to get $(\boldsymbol{u}, \mathsf{M}[\boldsymbol{u}]) \in \mathbb{F}^\ell \times \mathbb{F}^\ell$ such that $\mathsf{M}[\boldsymbol{u}] = \mathsf{K}[\boldsymbol{u}] + \boldsymbol{u} \cdot \varDelta$, where $\mathbb{F}$ is a large field such as $\mathbb{F} = \mathbb{F}_{2^\rho}$.

Dittmer et al. [16] assume that $\boldsymbol{b}_{\mathcal{I}}$ is uniform and authenticated AND triples related to $\boldsymbol{b}_{\mathcal{I}}$ are generated using the previous approach such as [29]. Therefore, we only show how to generate compressed authenticated AND triples, where random masks held by $\mathsf{P_B}$ are compressed. Two parties can first generate compressed authenticated AND triple $([a_i],[b_i],[a_j],[b_j],[\hat{a}_k],[\hat{b}_k])$ for each AND gate with $\varDelta_{\mathsf{A}} \leftarrow \mathbb{F}_{2^\rho}$, and then convert them into that with $\varDelta'_{\mathsf{A}} \leftarrow \mathbb{F}_{2^\kappa}$ using extra 2 bits of communication per AND gate, where a ρ-bit global key can guarantee that communication only depends on ρ rather than κ and $\varDelta'_{\mathsf{A}} \in \mathbb{F}_{2^\kappa}$ is required for garbled circuits. In the following, we give an overview of Dittmer et al. 's approach on how to generate circuit-dependent compressed authenticated AND triples $\{([a_i],[b_i],[a_j],[b_j],[\hat{a}_k],[\hat{b}_k])\}$ with $\varDelta_{\mathsf{A}}, \varDelta_{\mathsf{B}} \in \mathbb{F}_{2^\rho}$.

1. $\mathsf{P_A}$ and $\mathsf{P_B}$ generates a vector of authenticated bits $[\boldsymbol{b}^*]$ with a uniform $\boldsymbol{b}^* \in \mathbb{F}_2^L$ by calling $\mathcal{F}_{\mathsf{COT}}$. Then, both parties define $[\boldsymbol{b}] := \mathbf{M} \cdot [\boldsymbol{b}^*]$.
2. Both parties compute authenticated bit $[b_{i,j}]$ for each AND gate $(i,j,k,\wedge)$ via running the Fix procedure with input $\{b_{i,j}\}$ where $b_{i,j} := b_i \cdot b_j$.
3. $\mathsf{P_B}$ samples $\varDelta_{\mathsf{B}}, \gamma \leftarrow \mathbb{F}_{2^\rho}$. Then, both parties initializes two functionalities $\mathcal{F}_{\mathsf{bCOT}}^{L+2}$ and $\mathcal{F}_{\mathsf{bVOLE}}^{L+2}$ with the same global keys $(b_1^* \cdot \varDelta_{\mathsf{B}} + \gamma, \ldots, b_L^* \cdot \varDelta_{\mathsf{B}} + \gamma, \varDelta_{\mathsf{B}} + \gamma, \gamma)$, where $\mathcal{F}_{\mathsf{bVOLE}}^{L+2}$ is the same as $\mathcal{F}_{\mathsf{bCOT}}^{L+2}$ except that the outputs are VOLE correlations over $\mathbb{F}_{2^\rho}$ instead of COT correlations. Here γ is necessary to mask $b_i^* \cdot \varDelta_{\mathsf{B}}$. In particular, a consistency check in DILO lets $\mathsf{P_B}$ send a hashing of values related to $b_i^* \cdot \varDelta_{\mathsf{B}}$ to the malicious party $\mathsf{P_A}$, which may leak the bit b_i^* to $\mathsf{P_A}$. This attack would be prevented by using a uniform γ to mask $b_i^* \cdot \varDelta_{\mathsf{B}}$. Given $[a]_{b_i^* \varDelta_{\mathsf{B}} + \gamma}$ and $[a]_\gamma$ for any bit a held by $\mathsf{P_A}$, it is easy to locally compute $[ab_i^*]_{\varDelta_{\mathsf{B}}}$ from the additive homomorphism of IT-MACs. Similarly, given $[a]_{\varDelta_{\mathsf{B}}+\gamma}$ and $[a]_\gamma$, two parties can locally compute $[a]_{\varDelta_{\mathsf{B}}}$.
4. $\mathsf{P_A}$ and $\mathsf{P_B}$ calls $\mathcal{F}_{\mathsf{bCOT}}^{L+2}$ to generate the vectors of authenticated bits $[\boldsymbol{a}], [\hat{\boldsymbol{a}}]$ as well as $[a_i \boldsymbol{b}^*]_{\varDelta_{\mathsf{B}}}$ for each $i \in [1,n]$, where $\boldsymbol{a} \in \mathbb{F}_2^n$ (resp., $\hat{\boldsymbol{a}} \in \mathbb{F}_2^n$) is used as the vector of random masks $\{a_i\}$ (resp., $\{\hat{a}_k\}$) held by $\mathsf{P_A}$ on the output wires of all AND gates. Then, they can locally compute $[a_i b_j]_{\varDelta_{\mathsf{B}}}$ and $[a_j b_i]_{\varDelta_{\mathsf{B}}}$ for each AND gate $(i,j,k,\wedge)$ by calculating $\mathbf{M} \cdot [a_i \boldsymbol{b}^*]_{\varDelta_{\mathsf{B}}}$. Both parties run the Fix procedure with input $\{a_{i,j}\}$ to obtain $\{[a_{i,j}]\}$, where $a_{i,j} = a_i \wedge a_j$ for each AND gate $(i,j,k,\wedge)$.
5. $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_{\mathsf{bVOLE}}^{L+2}$ to get a vector of authenticated values $[\tilde{\boldsymbol{a}}]$ with a uniform vector $\tilde{\boldsymbol{a}} \in \mathbb{F}_{2^\rho}^n$. Both parties run the Fix procedure with input $(\varDelta_{\mathsf{A}} \cdot \boldsymbol{a}, \varDelta_{\mathsf{A}} \cdot \hat{\boldsymbol{a}}, \{\varDelta_{\mathsf{A}} \cdot a_{i,j}\}, \varDelta_{\mathsf{A}})$ to obtain authenticated values $[\varDelta_{\mathsf{A}} \cdot \boldsymbol{a}]$, $[\varDelta_{\mathsf{A}} \cdot \hat{\boldsymbol{a}}]$, $\{[\varDelta_{\mathsf{A}} \cdot a_{i,j}]\}$ and $[\varDelta_{\mathsf{A}}]_{\varDelta_{\mathsf{B}}}$. The Fix procedure corresponds to calling $\mathcal{F}_{\mathsf{bVOLE}}^{L+2}$, and also outputs $[\varDelta_{\mathsf{A}} a_i \boldsymbol{b}^*]_{\varDelta_{\mathsf{B}}}$ for each $i \in [1,n]$ and $[\varDelta_{\mathsf{A}}]_{b_i^* \varDelta_{\mathsf{B}}}$ for each $i \in [1,L]$ to both parties. Note that $[\varDelta_{\mathsf{A}}]_{\varDelta_{\mathsf{B}}}$ and $[\varDelta_{\mathsf{A}}]_{b_i^* \varDelta_{\mathsf{B}}}$ can be written as $[\varDelta_{\mathsf{B}}]$ and $[b_i^* \varDelta_{\mathsf{B}}]$ respectively, where we also use $[B_i^*]$ to denote $[b_i^* \varDelta_{\mathsf{B}}]$. Furthermore, $\mathsf{P_A}$ and $\mathsf{P_B}$ can locally compute $[\varDelta_{\mathsf{A}} a_i b_j]_{\varDelta_{\mathsf{B}}}$ and $[\varDelta_{\mathsf{A}} a_j b_i]_{\varDelta_{\mathsf{B}}}$ for each AND gate $(i,j,k,\wedge)$ by computing $\mathbf{M} \cdot [\varDelta_{\mathsf{A}} a_i \boldsymbol{b}^*]_{\varDelta_{\mathsf{B}}}$ for each $i \in [1,n]$.
6. Parties $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_{\mathsf{DVZK}}$ to prove the following relations:
   - For each AND gate $(i,j,k,\wedge)$, given $([b_i],[b_j],[b_{i,j}])$, prove $b_{i,j} = b_i \wedge b_j$.
   - For each AND gate $(i,j,k,\wedge)$, given $([a_i],[a_j],[a_{i,j}])$, prove $a_{i,j} = a_i \wedge a_j$.
   - For each $i \in [1,L]$, given $([b_i^*],[\varDelta_{\mathsf{B}}],[B_i^*])$, prove $B_i^* = b_i^* \cdot \varDelta_{\mathsf{B}}$.

7. $\mathsf{P_B}$ also executes an efficient verification protocol to convince $\mathsf{P_A}$ that the same global keys are input to different functionalities $\mathcal{F}_{\mathsf{bCOT}}^{L+2}$ and $\mathcal{F}_{\mathsf{bVOLE}}^{L+2}$. It is unnecessary to check the consistency of $\Delta_\mathsf{A} \cdot \boldsymbol{a}$, $\Delta_\mathsf{A} \cdot \hat{\boldsymbol{a}}$, $\{\Delta_\mathsf{A} \cdot a_{i,j}\}$, Δ_A input to Fix w.r.t. $\mathcal{F}_{\mathsf{bVOLE}}^{L+2}$. The resulting VOLE correlations on these inputs are used to compute the MAC tags of $\mathsf{P_B}$ on its shares. If these inputs are incorrect, this only leads to these MAC tags, which will be authenticated by $\mathsf{P_A}$, being incorrect. This is harmless for security.
8. For each AND gate $(i, j, k, \wedge)$, $\mathsf{P_A}$ and $\mathsf{P_B}$ locally compute $[\tilde{b}_k]_{\Delta_\mathsf{B}} := [a_{i,j}] + [a_i b_j] + [a_j b_i] + [\hat{a}_k]$ and $[\tilde{B}_k]_{\Delta_\mathsf{B}} := [\Delta_\mathsf{A} a_{i,j}] + [\Delta_\mathsf{A} a_i b_j] + [\Delta_\mathsf{A} a_j b_i] + [\Delta_\mathsf{A} \hat{a}_k] + [\tilde{a}_k]$, where all values are authenticated under Δ_B. Then, $\mathsf{P_A}$ sends a pair of MAC tags $(\mathsf{M_A}[\tilde{b}_k], \mathsf{M_A}[\tilde{B}_k])$ to $\mathsf{P_B}$, who computes the following over $\mathbb{F}_{2^\kappa}$

$$\tilde{b}_k := (\mathsf{K_B}[\tilde{b}_k] + \mathsf{M_A}[\tilde{b}_k]) \cdot \Delta_\mathsf{B}^{-1} \text{ and } \tilde{B}_k := (\mathsf{K_B}[\tilde{B}_k] + \mathsf{M_A}[\tilde{B}_k]) \cdot \Delta_\mathsf{B}^{-1}.$$

   It is easy to see that $\tilde{b}_k = a_{i,j} \oplus a_i b_j \oplus a_j b_i \oplus \hat{a}_k \in \{0, 1\}$ and $\tilde{B}_k = (a_{i,j} + a_i b_j + a_j b_i + \hat{a}_k) \cdot \Delta_\mathsf{A} + \tilde{a}_k \in \mathbb{F}_{2^\rho}$, where the randomness $\tilde{a}_k \in \mathbb{F}_{2^\rho}$ is crucial to prevent that $\tilde{B}_k$ directly reveals Δ_A in the case of $\tilde{b}_k = 1$. We observe that both parties now obtain an authenticated bit $[\tilde{b}_k]_{\Delta_\mathsf{A}}$ by defining its local key $\mathsf{K_A}[\tilde{b}_k] = \tilde{a}_k$ and MAC tag $\mathsf{M_B}[\tilde{b}_k] = \tilde{B}_k$.
9. For each AND gate $(i, j, k, \wedge)$, $\mathsf{P_A}$ and $\mathsf{P_B}$ locally compute an authenticated bit $[\hat{b}_k]_{\Delta_\mathsf{A}} := [\tilde{b}_k]_{\Delta_\mathsf{A}} \oplus [b_{i,j}]_{\Delta_\mathsf{A}}$. Now, both parties obtain an authenticated triple $([a_i], [b_i], [a_j], [b_j], [\hat{a}_k], [\hat{b}_k])$ for each AND gate $(i, j, k, \wedge)$.

3.2 Our Solution for Generating Authenticated AND Triples

In the DILO protocol [16], the one-way communication cost of generating the authenticated triple $([a_i], [b_i], [a_j], [b_j], [\hat{a}_k], [\hat{b}_k])$ for each AND gate $(i, j, k, \wedge)$ is brought about by producing an authenticated bit $[\tilde{b}_k]$ under Δ_A that is in turn used to locally compute $[\hat{b}_k]$ with $\hat{b}_k = \tilde{b}_k \oplus b_i b_j$. DILO generates the authenticated bit $[\tilde{b}_k] = (\mathsf{K_A}[\tilde{b}_k], \mathsf{M_B}[\tilde{b}_k], \tilde{b}_k)$ under Δ_A by computing authenticated values on $\tilde{b}_k$ and $\mathsf{M_B}[\tilde{b}_k]$ under Δ_B. Specifically, we have the following two parts:

- $\mathsf{P_B}$ computes the bit $\tilde{b}_k$ from the authenticated bit on $\tilde{b}_k$ under Δ_B and corresponding MAC tag sent by $\mathsf{P_A}$ in communication of $\rho + 1$ bits.
- $\mathsf{P_B}$ computes the MAC tag $\mathsf{M_B}[\tilde{b}_k]$ by generating the authenticated value on $\mathsf{M_B}[\tilde{b}_k]$ under Δ_B and corresponding MAC tag sent by $\mathsf{P_A}$ in communication of 4ρ bits.

We observe that the communication cost of the first part can be further reduced to only 2 bits by setting $\mathsf{lsb}(\Delta_\mathsf{B}) = 1$. In particular, $\mathsf{P_A}$ can send the LSB x_k of the MAC tag w.r.t. $[\tilde{b}_k]_{\Delta_\mathsf{B}}$ to $\mathsf{P_B}$ who can compute $\tilde{b}_k$ by XORing x_k with the LSB of the local key w.r.t. $[\tilde{b}_k]_{\Delta_\mathsf{B}}$. The authentication of $\{\tilde{b}_k\}$ can be done in a batch by hashing the MAC tags on these bits. However, the communication cost of the second part is inherent due to the DILO approach of generating the MAC tag $\mathsf{M_B}[\tilde{b}_k]$. This leaves us a challenge problem: *how to generate authenticated bit $[\tilde{b}_k]_{\Delta_\mathsf{A}}$ without the ρ-time blow-up in communication.*

The crucial point for solving the above problem is to generate the MAC tag $\mathsf{M}_{\mathsf{B}}[\tilde{b}_k]$ with constant communication per triple. In a straightforward way, P_{A} and P_{B} can run the Fix procedure to generate $[\tilde{b}_k]_{\Delta_{\mathsf{A}}}$ by taking one-bit communication after P_{B} has obtained $\tilde{b}_k$. However, P_{A} has no way to check the correctness of $\tilde{b}_k$ implied in $[\tilde{b}_k]_{\Delta_{\mathsf{A}}}$, where $[\tilde{b}_k]_{\Delta_{\mathsf{B}}}$ generated by both parties only allow P_{B} to check the correctness of $\tilde{b}_k$. We introduce the notion of dual-key authentication to allow both parties to check the correctness of $\tilde{b}_k$, where the bit $\tilde{b}_k$ is authenticated under global key $\Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}}$ and thus no party can change the bit $\tilde{b}_k$ without being detected. We present an efficient approach to generate the dual-key authenticated bit $\langle \tilde{b}_k \rangle$ with communication of only one bit. By checking the consistency of all values input to the block-COT functionality, we can guarantee the correctness of $\langle \tilde{b}_k \rangle$, i.e., $\tilde{b}_k$ is a valid bit authenticated by both parties. When setting $\mathsf{lsb}(\Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}}) = 1$, P_{B} can obtain the bit $\tilde{b}_k$ by letting P_{A} send one-bit message to P_{B} (see below for details). By using Fix, P_{A} and P_{B} can generate $[\tilde{b}_k]$ under Δ_{A}. Now, P_{B} can check the correctness of $\tilde{b}_k$ obtained, and P_{A} can verify the correctness of $\tilde{b}_k$ implied in $[\tilde{b}_k]$, by using the correctness of $\langle \tilde{b}_k \rangle$. Particularly, we propose a batch-check technique that enables both parties to check the correctness of $\{\tilde{b}_k\}$ in all triples with essentially no communication. In addition, we present two new checking protocols to verify the correctness of global keys and the consistency of values across different functionalities (see below for an overview). Overall, our techniques allow to achieve one-way communication of only 2 bits per triple, and are described below.

Dual-key Authentication. We propose the notion of dual-key authentication, meaning that a bit is authenticated by two global keys $\Delta_{\mathsf{A}}, \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$ held by P_{A} and P_{B} respectively. In particular, a dual-key authenticated bit $\langle x \rangle = (\mathsf{D}_{\mathsf{A}}[x], \mathsf{D}_{\mathsf{B}}[x], x)$ lets P_{A} hold $\mathsf{D}_{\mathsf{A}}[x]$ and P_{B} hold $\mathsf{D}_{\mathsf{B}}[x]$ such that $\mathsf{D}_{\mathsf{A}}[x] + \mathsf{D}_{\mathsf{B}}[x] = x \cdot \Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$, where $x \in \{0,1\}$ can be known by either P_{A} or P_{B}, or unknown for both parties. From the definition, we have that dual-key authenticated bits are also *additively homomorphic*, which enables us to use the random-linear-combination approach to perform consistency checks associated with such bits. We are also able to generalize dual-key authenticated bits to dual-key authenticated values in which x is defined over any field $\mathbb{F}$ and $\mathsf{D}_{\mathsf{A}}[x], \mathsf{D}_{\mathsf{B}}[x], \Delta_{\mathsf{A}}, \Delta_{\mathsf{B}}$ are defined over an extension field $\mathbb{K}$ with $\mathbb{F} \subseteq \mathbb{K}$. This generalization may be useful for the design of subsequent protocols. A useful property is that $\langle x \rangle$ can be *locally* converted into $[x\Delta_{\mathsf{A}}]_{\Delta_{\mathsf{B}}}$ or $[x\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$ and vice versa.

We consider that the bit x is shared as (a, b) with $x = a \wedge b$, where P_{A} holds $a \in \{0,1\}$ and P_{B} holds $b \in \{0,1\}$. Without loss of generality, we focus on the case that a is a secret bit. The bit b can be either a secret bit or a public bit 1, where the former means that no party knows x and the latter means that only P_{A} knows x. The DILO protocol [16] implicitly generates a dual-key authenticated bit by running $\mathsf{Fix}(a\Delta_{\mathsf{A}})$ w.r.t. global keys $b\Delta_{\mathsf{B}} + \gamma, \gamma$ to obtain $[a\Delta_{\mathsf{A}}]_{b\Delta_{\mathsf{B}}} = \langle ab \rangle = \langle x \rangle$, which incurs ρ-time blow-up in communication (even if a allows to be a random bit). Our approach can reduce the communication cost to at most one bit. In particular, we first let P_{A} and P_{B} generate a dual-key authenticated bit $\langle b \rangle = (\alpha, \beta)$ with $\alpha + \beta = b \cdot \Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$, where P_{A} gets α

and $\mathsf{P_B}$ obtains β. Then, both parties initialize functionality $\mathcal{F}_{\mathsf{bCOT}}$ with a global key β. If $a \in \{0,1\}$ allows to be random, both parties call $\mathcal{F}_{\mathsf{bCOT}}$ to generate $[a]_\beta$ without communication. Otherwise, both parties run Fix with input a to generate $[a]_\beta$ in communication of one bit. Given $[a]_\beta = (\mathsf{K_B}[a]_\beta, \mathsf{M_A}[a]_\beta, a)$, $\mathsf{P_A}$ and $\mathsf{P_B}$ can *locally* compute a dual-key authenticated bit $\langle a \rangle$ by letting $\mathsf{P_A}$ compute $\mathsf{D_A}[x] := \mathsf{M_A}[a]_\beta + a \cdot \alpha \in \mathbb{F}_{2^\kappa}$ and $\mathsf{P_B}$ set $\mathsf{D_B}[x] := \mathsf{K_B}[a]_\beta \in \mathbb{F}_{2^\kappa}$. We have that $\mathsf{D_A}[x] + \mathsf{D_B}[x] = (\mathsf{M_A}[a]_\beta + \mathsf{K_B}[a]_\beta) + a \cdot \alpha = a \cdot (\alpha + \beta) = a \cdot b \cdot \varDelta_\mathsf{A} \cdot \varDelta_\mathsf{B} \in \mathbb{F}_{2^\kappa}$. To guarantee correctness of $\langle x \rangle$, we need to check the consistency of β input to $\mathcal{F}_{\mathsf{bCOT}}$ and a input to Fix, which will be shown below.

Sampling Global Keys with Correctness Checking. As described above, we need to generate two global keys $\varDelta_\mathsf{A}$ and $\varDelta_\mathsf{B}$ such that $\mathsf{lsb}(\varDelta_\mathsf{A} \cdot \varDelta_\mathsf{B}) = 1$, which allows one party to get the bit $x = \mathsf{lsb}(\mathsf{D_A}[x]) \oplus \mathsf{lsb}(\mathsf{D_B}[x])$ from a dual-key authenticated bit $\langle x \rangle$. To do this, we let $\mathsf{P_A}$ sample $\varDelta_\mathsf{A} \leftarrow \{0,1\}^\kappa$ such that $\mathsf{lsb}(\varDelta_\mathsf{A}) = 1$. Then, we let $\mathsf{P_B}$ sample $\varDelta_\mathsf{B} \leftarrow \{0,1\}^\kappa$, and make $\mathsf{P_A}$ and $\mathsf{P_B}$ run the Fix procedure w.r.t. $\varDelta_\mathsf{A}$ with input $\varDelta_\mathsf{B}$ to generate $[\varDelta_\mathsf{B}]_{\varDelta_\mathsf{A}}$ (i.e., $\langle 1 \rangle$), where $\alpha_0 \oplus \beta_0 = \varDelta_\mathsf{A}\varDelta_\mathsf{B}$. $\mathsf{P_A}$ and $\mathsf{P_B}$ can exchange $\mathsf{lsb}(\alpha_0)$ and $\mathsf{lsb}(\beta_0)$ to decide whether $\mathsf{lsb}(\alpha_0) \oplus \mathsf{lsb}(\beta_0) = 0$. If yes, then $\mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B}) = \mathsf{lsb}(\alpha_0) \oplus \mathsf{lsb}(\beta_0) = 0$. In this case, we let $\mathsf{P_B}$ update $\varDelta_\mathsf{B}$ as $\varDelta_\mathsf{B} \oplus 1$, which makes $\varDelta_\mathsf{A}\varDelta_\mathsf{B}$ be updated as $\varDelta_\mathsf{A}\varDelta_\mathsf{B} \oplus \varDelta_\mathsf{A}$, where $\mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B} \oplus \varDelta_\mathsf{A}) = \mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B}) \oplus \mathsf{lsb}(\varDelta_\mathsf{A}) = 1$. Since $\varDelta_\mathsf{B}$ is changed as $\varDelta_\mathsf{B} \oplus 1$, α_0 needs to be updated as $\alpha_0 \oplus \varDelta_\mathsf{A}$ in order to keep correct correlation.

While we adopt the KRRW authenticated garbling [29] in dual executions, some bit of global keys $\varDelta_\mathsf{A}, \varDelta_\mathsf{B} \in \{0,1\}^\kappa$ is required to be fixed as 1. We often choose to define $\mathsf{lsb}(\varDelta_\mathsf{A}) = 1$ and $\mathsf{lsb}(\varDelta_\mathsf{B}) = 1$. While $\mathsf{lsb}(\varDelta_\mathsf{A}) = 1$ has been satisfied, $\mathsf{lsb}(\varDelta_\mathsf{B}) = 1$ does not always hold, as $\mathsf{P_B}$ may flip $\varDelta_\mathsf{B}$ depending on if $\mathsf{lsb}(\alpha_0) \oplus \mathsf{lsb}(\beta_0) = 0$. Thus, we let $\mathsf{P_B}$ set $\mathsf{msb}(\varDelta_\mathsf{B}) = 1$ for ease of remembering. More importantly, $\mathsf{msb}(\varDelta_\mathsf{B}) = 1$ has no impact on setting $\mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B}) = 1$.

To achieve active security, we need to guarantee that $\varDelta_\mathsf{A} \cdot \varDelta_\mathsf{B} \neq 0$ in the case that either $\mathsf{P_A}$ or $\mathsf{P_B}$ is corrupted. This can be assured by checking $\varDelta_\mathsf{A} \neq 0$ and $\varDelta_\mathsf{B} \neq 0$. We choose to check $\mathsf{lsb}(\varDelta_\mathsf{A}) = 1$ and $\mathsf{msb}(\varDelta_\mathsf{B}) = 1$ to realize the checking of $\varDelta_\mathsf{A} \neq 0$ and $\varDelta_\mathsf{B} \neq 0$. To enable $\mathsf{P_B}$ to check $\mathsf{lsb}(\varDelta_\mathsf{A}) = 1$, both parties can generate random authenticated bits $[r_1]_\mathsf{B}, \ldots, [r_\rho]_\mathsf{B}$, and then $\mathsf{P_A}$ sends $\mathsf{lsb}(\mathsf{K_A}[r_i])$ for $i \in [1,\rho]$ to $\mathsf{P_B}$ who checks that $\mathsf{lsb}(\mathsf{K_A}[r_i]) \oplus \mathsf{lsb}(\mathsf{M_B}[r_i]) = r_i$ for all $i \in [1,\rho]$. A malicious $\mathsf{P_A}$ can cheat successfully if and only if it guesses correctly all random bits $r_1, \ldots, r_\rho$, which happens with probability $1/2^\rho$. The correctness check of $\mathsf{msb}(\varDelta_\mathsf{B}) = 1$ can be done in a totally similar way. Furthermore, we need also to check $\mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B}) = 1$, and otherwise a selective failure attack may be performed on secret bit $\tilde{b}_k$. We first let $\mathsf{P_B}$ check $\mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B}) = 1$ by interacting with $\mathsf{P_A}$. We make $\mathsf{P_A}$ and $\mathsf{P_B}$ generate random dual-key authenticated bits $\langle s_1 \rangle, \ldots, \langle s_\rho \rangle$. Then, the check of $\mathsf{lsb}(\varDelta_\mathsf{A}\varDelta_\mathsf{B}) = 1$ can be done similarly, by letting $\mathsf{P_A}$ send $\mathsf{lsb}(\mathsf{D_A}[s_i])$ to $\mathsf{P_B}$ who checks that $\mathsf{lsb}(\mathsf{D_A}[s_i]) \oplus \mathsf{lsb}(\mathsf{D_B}[s_i]) = s_i$ for all $i \in [1,\rho]$. To produce $\langle s_1 \rangle, \ldots, \langle s_\rho \rangle$, $\mathsf{P_A}$ and $\mathsf{P_B}$ can call $\mathcal{F}_{\mathsf{COT}}$ to generate random authenticated bits $[s_1]_{\varDelta_\mathsf{A}}, \ldots, [s_\rho]_{\varDelta_\mathsf{A}}$, and then run the Fix procedure w.r.t. $\varDelta_\mathsf{A}$ on input $(s_1\varDelta_\mathsf{B}, \ldots, s_\rho\varDelta_\mathsf{B})$ to generate $[s_1\varDelta_\mathsf{B}]_{\varDelta_\mathsf{A}}, \ldots, [s_\rho\varDelta_\mathsf{B}]_{\varDelta_\mathsf{A}}$ that are equivalent to $\langle s_1 \rangle, \ldots, \langle s_\rho \rangle$. Then, the correctness of the input $(s_1\varDelta_\mathsf{B}, \ldots, s_\rho\varDelta_\mathsf{B})$ needs to be verified by $\mathsf{P_A}$ via letting $\mathsf{P_B}$ prove that $([s_i]_{\varDelta_\mathsf{A}}, [\varDelta_\mathsf{B}]_{\varDelta_\mathsf{A}}, [s_i\varDelta_\mathsf{B}]_{\varDelta_\mathsf{A}})$ for all $i \in [1,\rho]$

satisfy the multiplication relationship using $\mathcal{F}_{\mathsf{DVZK}}$. Due to the dual execution, $\mathsf{P_A}$ needs also to symmetrically check $\mathsf{lsb}(\varDelta_{\mathsf{A}}\varDelta_{\mathsf{B}}) = 1$ by interacting with $\mathsf{P_B}$.

Generating Compressed Authenticated AND Triples. As described above, for generating a compressed authenticated AND triple $([a_i], [b_i], [a_j], [b_j], [\hat{a}_k], [\hat{b}_k])$, the crucial step is to generate a dual-key authenticated bit $\langle \tilde{b}_k \rangle$ with $\tilde{b}_k = \hat{b}_k \oplus b_i b_j$. From the definition of $\tilde{b}_k$, we know that $\langle \tilde{b}_k \rangle = \langle a_{i,j} \rangle \oplus \langle a_i b_j \rangle \oplus \langle a_j b_i \rangle \oplus \langle \hat{a}_k \rangle$. We use the above approach to generate the dual-key authenticated bits $\langle a_{i,j} \rangle, \langle \hat{a}_k \rangle$ and $\langle a_i \boldsymbol{b}^* \rangle$ for $i \in [1, n]$ that can be locally converted to $\langle a_i b_j \rangle, \langle a_j b_i \rangle$ by multiplying a public matrix $\mathbf{M}$. Then, we combine all the dual-key authenticated bits to obtain $\langle \tilde{b}_k \rangle$. From $\mathsf{lsb}(\varDelta_{\mathsf{A}}\varDelta_{\mathsf{B}}) = 1$, we can let $\mathsf{P_A}$ send $\mathsf{lsb}(\mathsf{D_A}[\tilde{b}_k])$ to $\mathsf{P_B}$ who is able to recover $\tilde{b}_k = \mathsf{lsb}(\mathsf{D_A}[\tilde{b}_k]) \oplus \mathsf{lsb}(\mathsf{D_B}[\tilde{b}_k])$. By running the Fix procedure with input $\tilde{b}_k$, both parties can generate $[\tilde{b}_k]$, which can be in turn locally converted into $[\hat{b}_k]$. More details are shown as follows.

1. As in the DILO protocol [16], we let $\mathsf{P_A}$ and $\mathsf{P_B}$ obtain $[\boldsymbol{b}^*]$ and $\{[b_{i,j}]\}$ by calling $\mathcal{F}_{\mathsf{COT}}$ and running Fix with input $b_{i,j} = b_i b_j$. Then, both parties compute $[\boldsymbol{b}] := \mathbf{M} \cdot [\boldsymbol{b}^*]$ to obtain $[b_i], [b_j]$ for each AND gate $(i, j, k, \wedge)$.
2. $\mathsf{P_A}$ and $\mathsf{P_B}$ have produced $\langle 1 \rangle = (\alpha_0, \beta_0)$ such that $\alpha_0 + \beta_0 = \varDelta_{\mathsf{A}} \cdot \varDelta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$. For each $i \in [1, L]$, both parties can further generate a dual-key authenticated bit $\langle b_i^* \rangle = (\alpha_i, \beta_i)$ with $\alpha_i + \beta_i = b_i^* \cdot \varDelta_{\mathsf{A}} \cdot \varDelta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$ by running Fix w.r.t. $\varDelta_{\mathsf{A}}$ with input $B_i^* = b_i^* \varDelta_{\mathsf{B}}$. The communication to generate $\langle b_1^* \rangle, \ldots, \langle b_L^* \rangle$ is $L\kappa$ bits and logarithmic to the number n of AND gates due to $L = O(\rho \log(n/\rho))$.
3. $\mathsf{P_B}$ and $\mathsf{P_A}$ initialize $\mathcal{F}_{\mathsf{bCOT}}^{L+1}$ with global keys $\beta_1, \ldots, \beta_L, \varDelta_{\mathsf{B}}$, and then call $\mathcal{F}_{\mathsf{bCOT}}^{L+1}$ to generate $[\boldsymbol{a}]_{\beta_1}, \ldots, [\boldsymbol{a}]_{\beta_L}$ and $[\boldsymbol{a}]_{\varDelta_{\mathsf{B}}}$. For each tuple $([a_i]_{\beta_1}, \ldots, [a_i]_{\beta_L})$, we can convert it to $\langle a_i \boldsymbol{b}^* \rangle$. By multiplying the public matrix $\mathbf{M}$, both parties can obtain $\langle a_i b_j \rangle$ and $\langle a_j b_i \rangle$ for each AND gate $(i, j, k, \wedge)$. From $[\boldsymbol{a}]_{\varDelta_{\mathsf{B}}}$, both parties directly obtain $[a_i], [a_j]$ for each AND gate $(i, j, k, \wedge)$.
4. $\mathsf{P_B}$ and $\mathsf{P_A}$ initialize $\mathcal{F}_{\mathsf{bCOT}}^{2}$ with global keys $\beta_0, \varDelta_{\mathsf{B}}$, and then call $\mathcal{F}_{\mathsf{bCOT}}^{2}$ to generate $[\hat{\boldsymbol{a}}]_{\beta_0}$ and $[\hat{\boldsymbol{a}}]_{\varDelta_{\mathsf{B}}}$. Both parties further run the Fix procedure with input $a_{i,j} = a_i \wedge a_j$ to generate $[a_{i,j}]_{\beta_0}$ and $[a_{i,j}]_{\varDelta_{\mathsf{B}}}$, where $[a_{i,j}]_{\varDelta_{\mathsf{B}}}$ will be used to prove validity of $a_{i,j}$. The parties can convert $[\hat{\boldsymbol{a}}]_{\beta_0}$ and $\{[a_{i,j}]_{\beta_0}\}$ into $\langle \hat{a}_k \rangle$ and $\langle a_{i,j} \rangle$ for each AND gate $(i, j, k, \wedge)$.
5. Both parties can *locally* compute $\langle \tilde{b}_k \rangle := \langle a_{i,j} \rangle \oplus \langle a_i b_j \rangle \oplus \langle a_j b_i \rangle \oplus \langle \hat{a}_k \rangle$. Then, $\mathsf{P_A}$ can send $\mathsf{lsb}(\mathsf{D_A}[\tilde{b}_k])$ to $\mathsf{P_B}$, who computes $\tilde{b}_k := \mathsf{lsb}(\mathsf{D_A}[\tilde{b}_k]) \oplus \mathsf{lsb}(\mathsf{D_B}[\tilde{b}_k])$ due to $\mathsf{lsb}(\varDelta_{\mathsf{A}}\varDelta_{\mathsf{B}}) = 1$. Both parties run Fix on input $\tilde{b}_k$ to generate $[\tilde{b}_k]$.
6. $\mathsf{P_A}$ and $\mathsf{P_B}$ can *locally* compute $[\hat{b}_k] := [\tilde{b}_k] \oplus [b_{i,j}]$. Now, the parties hold $([a_i], [b_i], [a_j], [b_j], [\hat{a}_k], [\hat{b}_k])$ for each AND gate $(i, j, k, \wedge)$.

Consistency Check. We have shown how to generate compressed authenticated AND triples. Below, we show how to verify their correctness. We only need to guarantee the consistency of all Fix inputs, all global keys input to the bCOT functionality and all bits sent by $\mathsf{P_A}$ to $\mathsf{P_B}$. When all messages and inputs are consistent, no malicious party can break the correctness of all triples. Specifically, we present the following checks to guarantee the consistency.

1. Check the correctness of the following authenticated AND triples:
   - $([b_i], [b_j], [b_{i,j}])$ *s.t.* $b_{i,j} = b_i \wedge b_j$ for each AND gate $(i, j, k, \wedge)$.
   - $([a_i], [a_j], [a_{i,j}])$ *s.t.* $a_{i,j} = a_i \wedge a_j$ for each AND gate $(i, j, k, \wedge)$.
   - $([b_i^*], [\varDelta_{\mathsf{B}}], [B_i^*])$ *s.t.* $B_i^* = b_i^* \cdot \varDelta_{\mathsf{B}}$ for each $i \in [1, L]$.
2. The keys $\beta_0, \beta_1, \ldots, \beta_L$ input to functionality $\mathcal{F}_{\mathsf{bCOT}}$ are consistent to the values defined in $\langle 1 \rangle, \langle b_1^* \rangle, \ldots, \langle b_L^* \rangle$.
3. $\mathsf{P_A}$ needs to check that two global keys $\varDelta_{\mathsf{B}}^{(1)}$ and $\varDelta_{\mathsf{B}}^{(2)}$ respectively input to functionalities $\mathcal{F}_{\mathsf{bCOT}}^{L+1}$ and $\mathcal{F}_{\mathsf{bCOT}}^{2}$ are consistent with $\varDelta_{\mathsf{B}}$ defined in $\langle 1 \rangle$.
4. $\mathsf{P_A}$ checks that the bit $\tilde{b}_k$ defined in $[\tilde{b}_k]$ is consistent to that defined in $\langle \tilde{b}_k \rangle$, and $\mathsf{P_B}$ checks that $\tilde{b}_k$ computed by itself is consistent to that defined in $\langle \tilde{b}_k \rangle$.

The first two checks guarantee the correctness of $\langle \tilde{b}_k \rangle$ and $[b_{i,j}]$, the third check verifies the consistency of the global keys in $[a_i], [a_j], [\hat{a}_k]$, and the final check assure the consistency of bits authenticated between $\langle \tilde{b}_k \rangle$ and $[\tilde{b}_k]$. Check 1 can be directly realized by calling functionality $\mathcal{F}_{\mathsf{DVZK}}$.

For Check 2, for each $i \in [0, L]$, we let $\mathsf{P_A}$ and $\mathsf{P_B}$ run the Fix procedure w.r.t. β_i on input $\varDelta'_{\mathsf{A}}$ to generate $[\varDelta'_{\mathsf{A}}]_{\beta_i}$, which can be locally converted into $[\beta_i]_{\varDelta'_{\mathsf{A}}}$, where $\varDelta'_{\mathsf{A}} \in \mathbb{F}_{2^\kappa}$ is sampled uniformly at random by $\mathsf{P_A}$.[2] For $i \in [0, L]$, we present a new protocol to verify the consistency of β_i in the following equations:

$$\alpha_i + \beta_i = b_i^* \cdot \varDelta_{\mathsf{A}} \cdot \varDelta_{\mathsf{B}},$$
$$\mathsf{K}'_{\mathsf{A}}[\beta_i] + \mathsf{M}'_{\mathsf{A}}[\beta_i] = \beta_i \cdot \varDelta'_{\mathsf{A}},$$

where b_0^* is defined as 1. We first multiply two sides of the first equation by $\varDelta_{\mathsf{A}}^{-1}$, and obtain $\alpha_i \cdot \varDelta_{\mathsf{A}}^{-1} + \beta_i \cdot \varDelta_{\mathsf{A}}^{-1} = b_i^* \cdot \varDelta_{\mathsf{B}}$. We rewrite the resulting equation as $\mathsf{K_A}[\beta_i] + \mathsf{M_B}[\beta_i] = \beta_i \cdot \varDelta_{\mathsf{A}}^{-1}$ where $\mathsf{K_A}[\beta_i] = \alpha_i \cdot \varDelta_{\mathsf{A}}^{-1}$ and $\mathsf{M_B}[\beta_i] = b_i^* \cdot \varDelta_{\mathsf{B}}$. Below, we can adapt the known techniques [16,18] to check the consistency of β_i authenticated under different global keys (i.e., $[\beta_i]_{\varDelta_{\mathsf{A}}^{-1}}$ and $[\beta_i]_{\varDelta'_{\mathsf{A}}}$) in a batch (see Sect. 4.3 for details).

For Check 3, we make $\mathsf{P_A}$ and $\mathsf{P_B}$ run the Fix procedure w.r.t. $\varDelta_{\mathsf{B}}^{(1)}$ (resp., $\varDelta_{\mathsf{B}}^{(2)}$) on input $\varDelta'_{\mathsf{A}}$ to obtain $[\varDelta_{\mathsf{B}}^{(1)}]_{\varDelta'_{\mathsf{A}}}$ (resp., $[\varDelta_{\mathsf{B}}^{(2)}]_{\varDelta'_{\mathsf{A}}}$). Authenticated values $[\varDelta_{\mathsf{B}}^{(1)}]_{\varDelta'_{\mathsf{A}}}$ and $[\varDelta_{\mathsf{B}}^{(2)}]_{\varDelta'_{\mathsf{A}}}$ are equivalent to $\langle 1_{\mathsf{B}}^{(1)} \rangle$ and $\langle 1_{\mathsf{B}}^{(2)} \rangle$ where $\varDelta_{\mathsf{B}}^{(1)} \varDelta'_{\mathsf{A}}$ and $\varDelta_{\mathsf{B}}^{(2)} \varDelta'_{\mathsf{A}}$ are used as the global keys in dual-key authentication. Both parties can invoke a relaxed equality-check functionality $\mathcal{F}_{\mathsf{EQ}}$ (shown in the full version [14]) to check $1_{\mathsf{B}}^{(1)} - 1_{\mathsf{B}}^{(2)} = 0$. Using the checking technique by Dittmer et al. [16], we can also check the consistency of the values authenticated between $[\varDelta_{\mathsf{B}}^{(1)}]_{\varDelta'_{\mathsf{A}}}$ and $[\varDelta_{\mathsf{B}}]_{\varDelta_{\mathsf{A}}}$ generated during the sampling phase.

For Check 4, we use a random-linear-combination approach to perform the check in a batch. Specifically, we can let $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_{\mathsf{COT}}$ to generate $[\boldsymbol{r}]_{\mathsf{B}}$ and then obtain $[r]_{\mathsf{B}} \leftarrow \mathsf{B2F}([\boldsymbol{r}]_{\mathsf{B}})$, where $r \in \mathbb{F}_{2^\kappa}$ is uniform. Then, both parties run Fix w.r.t. $\varDelta_{\mathsf{A}}$ on input $r\varDelta_{\mathsf{B}}$ to generate $[r\varDelta_{\mathsf{B}}]_{\varDelta_{\mathsf{A}}}$ (i.e., $\langle r \rangle$). We can let the parties call a standard coin-tossing functionality $\mathcal{F}_{\mathsf{Rand}}$ to sample a random element

[2] An independent global key $\varDelta'_{\mathsf{A}}$ is necessary to perform the consistency check, and otherwise a malicious $\mathsf{P_B}$ will always pass the check if $\varDelta_{\mathsf{A}}$ is reused.

$\chi \in \mathbb{F}_{2^\kappa}$. Then, both parties can locally compute $\langle y \rangle := \sum \chi^k \cdot \langle \tilde{b}_k \rangle + \langle r \rangle$ and $[y]_\mathsf{B} := \sum \chi^k \cdot [\tilde{b}_k]_\mathsf{B} + [r]_\mathsf{B}$. Then, $\mathsf{P_B}$ can open $[y]_\mathsf{B}$ that allows $\mathsf{P_A}$ to get y in an authenticated way. Finally, both parties can use $\mathcal{F}_\mathsf{EQ}$ to verify that the opening of $\langle y \rangle - y \cdot \langle 1 \rangle$ is 0. Since χ is sampled uniformly at random after all authenticated values are determined, the consistency check will detect malicious behaviors except with probability at most $n/2^\kappa$.

3.3 Our Solution for Dual Execution Without Leakage

While the evaluator's random masks are compressed, the state-of-the-art construction of authenticated garbling based on half-gates by Katz et al. [29] is no longer applied. The circuit authentication approach in [29] requires the evaluator to reveal all masked wire values, which is prohibitive for the compression technique. Therefore, based on the technique [36], Dittmer et al. [16] designed a new construction of authenticated garbling without revealing masked wire values. However, this construction incurs extra communication overhead of $3\rho - 1$ bits per AND gate, compared to the half-gates-based construction [29].

In duplex networks, communication cost is often measured by one-way communication. This allows us to adopt the idea of dual execution [33] to perform the authentication of circuit evaluation. In the original dual execution [33], the semi-honest Yao-2PC protocol [44] is executed two times with the same inputs in parallel by swapping the roles of parties for the second execution, and then the correctness of the output is verified by checking that the two executions have the same output bits. However, an inherent problem of the above method is that selective failure attacks are allowed to leak one-bit information of the input by the honest party, even though there exists a protocol to check the consistency of inputs in two executions. For example, suppose that $\mathsf{P_A}$ is honest and $\mathsf{P_B}$ is malicious. When $\mathsf{P_A}$ is a garbler and $\mathsf{P_B}$ is an evaluator, both parties compute an output $f(x, y)$ where x is the $\mathsf{P_A}$'s input and y is the $\mathsf{P_B}$'s input. After swapping the roles, they compute another output $g(x, y)$ with $g \neq f$, as garbler $\mathsf{P_B}$ is malicious. If the output-equality check passes, then $g(x, y) = f(x, y)$, else $g(x, y) \neq f(x, y)$. In both cases, this leaks one-bit information on the input x.

In the authenticated garbling framework, we propose a new technique to circumvent the problem and eliminate the one-bit leakage. Together with our technique to generate compressed authenticated AND triples, we can achieve the cost of one-way communication that is almost the same as the semi-honest half-gates protocol [45]. Specifically, we let $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the protocol, which combines the sub-protocol of generating authenticated AND triples as described above with the construction of distributed garbling [29], for two times with same inputs in the dual-execution way. For each wire w in the circuit, we need to check that the actual values z_w and z'_w in two executions are identical. We perform the checking by verifying $z_w \cdot (\varDelta_\mathsf{A} \oplus \varDelta_\mathsf{B}) = z'_w \cdot (\varDelta_\mathsf{A} \oplus \varDelta_\mathsf{B})$. Since $\varDelta_\mathsf{A} \oplus \varDelta_\mathsf{B}$ is unknown for the adversary, the probability that $z_w \neq z'_w$ but the check passes is negligible. Our approach allows two parties to check the correctness of all wire values in the circuit, and thus prevents selective failure attacks.

In more detail, for each wire w, let Λ_w and (a_w, b_w) be the masked value and wire masks in the first execution and (Λ'_w, a'_w, b'_w) be the values in the second execution. Thus, P_A and P_B need to check that $\Lambda_w \oplus a_w \oplus b_w = \Lambda'_w \oplus a'_w \oplus b'_w$ for each wire w, where the output wires of XOR gates are unnecessary to be checked as they are locally computed. Below, our task is to check that $(\Lambda_w \oplus a_w \oplus b_w) \cdot (\Delta_\mathsf{A} \oplus \Delta_\mathsf{B}) = (\Lambda'_w \oplus a'_w \oplus b'_w) \cdot (\Delta_\mathsf{A} \oplus \Delta_\mathsf{B})$ holds for each wire w. By two protocol executions, both parties hold $([a_w], [b_w], [a'_w], [b'_w])$ for each wire w. When P_A is a garbler and P_B is an evaluator, P_A holds a garbled label $\mathsf{L}_{w,0}$ and P_B holds $(\Lambda_w, \mathsf{L}_{w,\Lambda_w})$. Since $\mathsf{L}_{w,\Lambda_w} = \mathsf{L}_{w,0} \oplus \Lambda_w \Delta_\mathsf{A}$ has the form of IT-MACs, we can view $(\mathsf{L}_{w,0}, \mathsf{L}_{w,\Lambda_w}, \Lambda_w)$ as an authenticated bit $[\Lambda_w]_\mathsf{B}$, where $\mathsf{L}_{w,0}$ is considered as the local key and L_{w,Λ_w} plays the role of MAC tag. Similarly, when P_A is an evaluator and P_B is a garbler, two parties hold an authenticated bit $[\Lambda'_w]_\mathsf{A}$. Following the known observation (e.g., [29]), for any authenticated bit $[y]_\mathsf{B}$, P_A and P_B have an additive sharing of $y \cdot \Delta_\mathsf{A} = \mathsf{K}_\mathsf{A}[y] \oplus \mathsf{M}_\mathsf{B}[y]$. Therefore, for all cross terms, both parties can obtain their additive shares, and then can compute two values that are checked to be identical. In particular, both parties can compute the additive shares of all cross terms: $Z^\mathsf{A}_{w,1} \oplus Z^\mathsf{B}_{w,1} = \Lambda_w \Delta_\mathsf{A}$, $Z^\mathsf{A}_{w,2} \oplus Z^\mathsf{B}_{w,2} = \Lambda'_w \Delta_\mathsf{B}$, $Z^\mathsf{A}_{w,3} \oplus Z^\mathsf{B}_{w,3} = a_w \Delta_\mathsf{B}$, $Z^\mathsf{A}_{w,4} \oplus Z^\mathsf{B}_{w,4} = a'_w \Delta_\mathsf{B}$, $Z^\mathsf{A}_{w,5} \oplus Z^\mathsf{B}_{w,5} = b_w \Delta_\mathsf{A}$, $Z^\mathsf{A}_{w,6} \oplus Z^\mathsf{B}_{w,6} = b'_w \Delta_\mathsf{A}$. Then, for each wire w, P_A and P_B can respectively compute

$$\begin{aligned} V^\mathsf{A}_w &= (\oplus_{i \in [1,6]} Z^\mathsf{A}_{w,i}) \oplus a_w \Delta_\mathsf{A} \oplus \Lambda'_w \Delta_\mathsf{A} \oplus a'_w \Delta_\mathsf{A} \\ V^\mathsf{B}_w &= (\oplus_{i \in [1,6]} Z^\mathsf{B}_{w,i}) \oplus b_w \Delta_\mathsf{B} \oplus \Lambda_w \Delta_\mathsf{B} \oplus b'_w \Delta_\mathsf{B}, \end{aligned}$$

such that $V^\mathsf{A}_w = V^\mathsf{B}_w$. Without loss of generality, we assume that only P_B obtains the output, and thus only P_B needs to check the correctness of all masked values. In this case, we make P_A send the hash value of all V^A_w to P_B, who can check its correctness with V^B_w for each wire w.

Optimizations for Processing Inputs. Dittmer et al. [16] consider that the wire masks (i.e., $\boldsymbol{b}_\mathcal{I}$) on all wires in $\mathcal{I}_\mathsf{B}$ held by evaluator P_B is uniformly random and authenticated AND triples associated with $\boldsymbol{b}_\mathcal{I}$ are generated using the previous approach (e.g., [29]). This will require an independent preprocessing protocol, and also brings more preprocessing communication cost. We solve the problem by specially processing the input of evaluator P_B. In particular, instead of making P_B send masked value $\Lambda_w := y_w \oplus b_w$ for each $w \in \mathcal{I}_\mathsf{B}$ to P_A where y_w is the input bit, we use an OT protocol to transmit L_{w,Λ_w} to P_B. This allows to keep masked wire values $\Lambda_w := y_w \oplus b_w$ for all $w \in \mathcal{I}_\mathsf{B}$ secret. In this case, we can compress the wire masks using the technique as described in Sect. 3.2 and adopt the same preprocessing protocol to handle $\boldsymbol{b}_\mathcal{I}$. Since L is logarithm to the length n of vector $\boldsymbol{b}$ (now $n = |\mathcal{W}| + |\mathcal{I}_\mathsf{B}|$), this optimization essentially incurs no more overhead for the preprocessing phase. Furthermore, our preprocessing protocol to generate authenticated AND triples has already invoked functionality $\mathcal{F}_\mathsf{COT}$. Therefore, we can let two parties call $\mathcal{F}_\mathsf{COT}$ to generate random COT correlations in the preprocessing phase, and then transform them to OT correlations in the standard way. This essentially brings no more communication for the preprocessing phase, due to the sublinear communication of the recent protocols instantiating $\mathcal{F}_\mathsf{COT}$.

Our optimization does not increase the rounds of online phase. As a trade-off, this optimization increases the online communication cost by $|\mathcal{I}_{\mathsf{B}}| \cdot \kappa$ bits.

In the second protocol execution (i.e., $\mathsf{P_A}$ as an evaluator and $\mathsf{P_B}$ as a garbler), we make a further optimization to directly guarantee that the masked values on all circuit-input wires are XOR of actual values and wire masks. In this case, it is unnecessary to check the correctness of masked values on all circuit-input wires between two protocol executions. The key idea is to utilize the authenticated bits and messages on circuit-input wires generated/sent during the first protocol execution along with the authenticated bits produced in the second protocol execution to generate the masked values on the wires in $\mathcal{I}_{\mathsf{A}} \cup \mathcal{I}_{\mathsf{B}}$. Due to the security of IT-MACs, we can guarantee the correctness of these masked values in the second execution. We postpone the details of this optimization to Sect. 5.

4 Preprocessing with Compressed Wire Masks

In this section we introduce the compressed preprocessing functionality $\mathcal{F}_{\mathsf{cpre}}$ (shown in Fig. 3) for two party computation as well as an efficient protocol Π_{cpre} (shown in Fig. 5 and Fig. 6) to realize it. In a modular fashion we first introduce the sub-components which are called in the main preprocessing protocol. The security of the protocol is also argued similarly: we first prove in separate lemmas the respective security properties of sub-components and then utilize these lemmas to prove the main theorem.

4.1 Dual-Key Authentication

In this subsection we define the format of dual-key authentication and list some of its properties that we utilize in the upper level preprocessing protocol.

Definition 1. *We use the notation* $\langle x \rangle := (\mathsf{D_A}[x], \mathsf{D_B}[x], x)$ *to denote the dual-key authenticated value* x*, where* $\mathsf{P_A}, \mathsf{P_B}$ *holds* $\mathsf{D_A}[x], \mathsf{D_B}[x]$ *subject to* $\mathsf{D_A}[x] + \mathsf{D_B}[x] = x\Delta_{\mathsf{A}}\Delta_{\mathsf{B}}$ *and* $\Delta_{\mathsf{A}}, \Delta_{\mathsf{B}}$ *are the IT-MAC keys of* $\mathsf{P_A}, \mathsf{P_B}$ *respectively.*

We remark that for any $x \in \mathbb{F}_{2^\kappa}$ the IT-MAC authentication $[x\Delta_{\mathsf{A}}]_{\Delta_{\mathsf{B}}}$ can be locally transformed to $\langle x \rangle$, which we summarize in the following macro (the case for $[\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$ can be defined analogously). In particular, by computing $[\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$ we implicitly have $\langle 1 \rangle$, i.e., authentication of the constant $1 \in \mathbb{F}_{2^\kappa}$.

- $\langle x \rangle \leftarrow \mathsf{Convert1}_{[\cdot]\to\langle\cdot\rangle}([x\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}})$: Set $\mathsf{D_A}[x] := \mathsf{M_A}[x\Delta_{\mathsf{B}}]$ and $\mathsf{D_B}[x] := \mathsf{K_B}[x\Delta_{\mathsf{B}}]$.

For the ease of presentation, we also define the following macro that generates dual key authentication of cross terms $\langle xy \rangle$ assuming the existence of $\langle y \rangle := (\alpha, \beta)$ and $[x]_{\mathsf{A},\beta} = (\mathsf{K_B}[x]_\beta, \mathsf{M_A}[x]_\beta, x)$. The correctness can be verified straightforwardly.

- $\langle xy \rangle \leftarrow \mathsf{Convert2}_{[\cdot]\to\langle\cdot\rangle}([x]_{\mathsf{A},\beta}, \langle y \rangle)$: Given IT-MAC $[x]_{\mathsf{A},\beta}$ and dual-key authentication $\langle y \rangle$, $\mathsf{P_A}$ and $\mathsf{P_B}$ *locally* compute the following steps:

Functionality $\mathcal{F}_{\mathsf{cpre}}$

This functionality is parameterized by a Boolean circuit $\mathcal{C}$ consisting of a list of gates in the form of (i, j, k, T). Let $n := |\mathcal{W}| + |\mathcal{I}_{\mathsf{B}}|$ (resp., $m := |\mathcal{W}| + |\mathcal{I}_{\mathsf{A}}|$) be the number of all AND gates as well as circuit-input gates corresponding to the input of $\mathsf{P_B}$ (resp., $\mathsf{P_A}$), and $L = \lceil \rho \log \frac{2en}{\rho} + \frac{\log \rho}{2} \rceil$ be a compression parameter. It runs with parties $\mathsf{P_A}$, $\mathsf{P_B}$ and the ideal-world adversary $\mathcal{S}$, and operates as follows:

Initialize. Sample two global keys $\Delta_{\mathsf{A}}, \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$ as follows:

- If $\mathsf{P_A}$ is honest, sample $\Delta_{\mathsf{A}} \leftarrow \mathbb{F}_{2^\kappa}$ such that $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$. Otherwise, receive $\Delta_{\mathsf{A}} \in \mathbb{F}_{2^\kappa}$ with $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$ from $\mathcal{S}$.
- If $\mathsf{P_B}$ is honest, sample $\Delta_{\mathsf{B}} \leftarrow \mathbb{F}_{2^\kappa}$ such that $\mathsf{lsb}(\Delta_{\mathsf{A}}\Delta_{\mathsf{B}}) = 1$ and $\mathsf{msb}(\Delta_{\mathsf{B}}) = 1$. Otherwise, receive $\Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$ with $\mathsf{msb}(\Delta_{\mathsf{B}}) = 1$ from $\mathcal{S}$, and then re-sample $\Delta_{\mathsf{A}} \leftarrow \mathbb{F}_{2^\kappa}$ such that $\mathsf{lsb}(\Delta_{\mathsf{A}}\Delta_{\mathsf{B}}) = 1$ and $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$.
- Store $(\Delta_{\mathsf{A}}, \Delta_{\mathsf{B}})$, and output Δ_{A} and Δ_{B} to $\mathsf{P_A}$ and $\mathsf{P_B}$, respectively.

Macro. $\mathsf{Auth_A}(\boldsymbol{x}, \ell)$ (this is an internal subroutine only)

- If $\mathsf{P_B}$ is honest, sample $\mathsf{K_B}[\boldsymbol{x}] \leftarrow \mathbb{F}_{2^\kappa}^{\ell}$; otherwise, receive $\mathsf{K_B}[\boldsymbol{x}] \in \mathbb{F}_{2^\kappa}^{\ell}$ from $\mathcal{S}$.
- If $\mathsf{P_A}$ is honest, compute $\mathsf{M_A}[\boldsymbol{x}] := \mathsf{K_B}[\boldsymbol{x}] + \boldsymbol{x} \cdot \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}^{\ell}$. Otherwise, receive $\mathsf{M_A}[\boldsymbol{x}] \in \mathbb{F}_{2^\kappa}^{\ell}$ from $\mathcal{S}$, and recompute $\mathsf{K_B}[\boldsymbol{x}] := \mathsf{M_A}[\boldsymbol{x}] + \boldsymbol{x} \cdot \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}^{\ell}$.
- Send $(\boldsymbol{x}, \mathsf{M_A}[\boldsymbol{x}])$ to $\mathsf{P_A}$ and $\mathsf{K_B}[\boldsymbol{x}]$ to $\mathsf{P_B}$.

$\mathsf{Auth_B}(\boldsymbol{x}, \ell)$ can be defined similarly by swapping the roles of $\mathsf{P_A}$ and $\mathsf{P_B}$.

Preprocess the circuit with compressed wire masks. Sample $\mathbf{M} \leftarrow \mathbb{F}_2^{n \times L}$, and then execute as follows:

- For $w \in \mathcal{I}_{\mathsf{A}}$, set $b_w = 0$ and define $[b_w]$; for $w \in \mathcal{I}_{\mathsf{B}}$, set $a_w = 0$ and define $[a_w]$.
- If $\mathsf{P_A}$ is honest, sample $\boldsymbol{a} \leftarrow \mathbb{F}_2^m$; otherwise, receive $\boldsymbol{a} \in \mathbb{F}_2^m$ from $\mathcal{S}$. Then, execute $\mathsf{Auth_A}(\boldsymbol{a}, m)$ to generate $[\boldsymbol{a}]$. For each wire $w \in \mathcal{I}_{\mathsf{A}} \cup \mathcal{W}$, define a_w as the wire mask held by $\mathsf{P_A}$.
- If $\mathsf{P_B}$ is honest, sample $\boldsymbol{b}^* \leftarrow \mathbb{F}_2^L$; otherwise, receive $\boldsymbol{b}^* \in \mathbb{F}_2^L$ from $\mathcal{S}$. Run $\mathsf{Auth_B}(\boldsymbol{b}^*, L)$ to generate $[\boldsymbol{b}^*]$, and then compute $[\boldsymbol{b}] := \mathbf{M} \cdot [\boldsymbol{b}^*]$ with $\boldsymbol{b} \in \mathbb{F}_2^n$. For each wire $w \in \mathcal{I}_{\mathsf{B}} \cup \mathcal{W}$, define b_w as the wire mask held by $\mathsf{P_B}$.
- In a topological order, for each gate (i, j, k, T), do the following:
  - If $T = \oplus$, compute $[a_k] := [a_i] \oplus [a_j]$ and $[b_k] := [b_i] \oplus [b_j]$.
  - If $T = \wedge$, execute as follows:
    1. If $\mathsf{P_A}$ is honest, then sample $\hat{a}_k \leftarrow \{0, 1\}$, else receive $\hat{a}_k \in \{0, 1\}$ from $\mathcal{S}$.
    2. If $\mathsf{P_B}$ is honest, then compute $\hat{b}_k := (a_i \oplus b_i) \wedge (a_j \oplus b_j) \oplus \hat{a}_k$. Otherwise, receive $\hat{b}_k \in \{0, 1\}$ from $\mathcal{S}$, and re-compute $\hat{a}_k := (a_i \oplus b_i) \wedge (a_j \oplus b_j) \oplus \hat{b}_k$.

  Let $\hat{\boldsymbol{a}}$ and $\hat{\boldsymbol{b}}$ be the vectors consisting of bits $\hat{a}_k$ and $\hat{b}_k$ for $k \in \mathcal{W}$. Run $\mathsf{Auth_A}(\hat{\boldsymbol{a}})$ and $\mathsf{Auth_B}(\hat{\boldsymbol{b}})$ to generate $[\hat{\boldsymbol{a}}]$ and $[\hat{\boldsymbol{b}}]$, respectively.
- Output $\mathbf{M}$ and $([\boldsymbol{a}], [\hat{\boldsymbol{a}}], [\boldsymbol{b}^*], [\hat{\boldsymbol{b}}])$ to $\mathsf{P_A}$ and $\mathsf{P_B}$.

Fig. 3. Compressed preprocessing functionality for authenticated triples.

- $\mathsf{P_A}$ outputs $\mathsf{D_A}[xy] := \alpha \cdot x + \mathsf{M_A}[x]_\beta \in \mathbb{F}_{2^\kappa}$.
- $\mathsf{P_B}$ outputs $\mathsf{D_B}[xy] := \mathsf{K_B}[x]_\beta$.

In our protocol we utilize the following properties of dual key authentication. Since they are straightforward we only provide brief explanation and refrain from providing detailed description.

Claim. The dual-key authentication is additively homomorphic. In particular, given $\langle x_1 \rangle := (\mathsf{D_A}[x_1], \mathsf{D_B}[x_1])$ and $\langle x_2 \rangle := (\mathsf{D_A}[x_2], \mathsf{D_B}[x_2])$, $\mathsf{P_A}, \mathsf{P_B}$ can locally compute $\langle x_1 + x_2 \rangle := (\mathsf{D_A}[x_1] + \mathsf{D_A}[x_2], \mathsf{D_B}[x_1] + \mathsf{D_B}[x_2])$.

The additive homomorphism of dual-key authentication implies that given public coefficients $c_0, c_1, \ldots, c_\ell \in \mathbb{F}_{2^\kappa}$, two parties can *locally* compute $\langle y \rangle := c_0 + \sum_{i=1}^{\ell} c_i \cdot \langle x_i \rangle$.

We define the zero-checking macro CheckZero2 which ensures soundness for both parties. We note that this is simply the equality checking operations.

– $\mathsf{CheckZero2}(\langle x_1 \rangle, \ldots \langle x_\ell \rangle)$: On input dual-key authenticated values $\langle x_1 \rangle, \ldots \langle x_\ell \rangle$ both parties check $x_i = 0$ for $i \in [1, \ell]$ as follows:
  1. $\mathsf{P_A}$ computes $h_\mathsf{A} := \mathsf{H}(\mathsf{D_A}[x_1], \ldots, \mathsf{D_A}[x_\ell])$, and $\mathsf{P_B}$ sets $h_\mathsf{B} := \mathsf{H}(\mathsf{D_B}[x_1], \ldots, \mathsf{D_B}[x_\ell])$, where $\mathsf{H} : \{0,1\}^* \to \{0,1\}^\kappa$ is a random oracle.
  2. Both parties call functionality $\mathcal{F}_\mathsf{EQ}$ to check $h_\mathsf{A} = h_\mathsf{B}$. If $\mathcal{F}_\mathsf{EQ}$ outputs false, the parties abort.

Notice that the additive homomorphic and zero-checking properties allow us to check that a dual-key authenticated value $\langle x \rangle$ matches a public value x' assuming the existence of $\langle 1 \rangle = (\mathsf{D_A}[1], \mathsf{D_B}[1])$ by calling $\mathsf{CheckZero2}(\langle x \rangle - x' \langle 1 \rangle)$. Similar to CheckZero we have the following soundness lemma of CheckZero2.

Lemma 2. *If $\Delta_\mathsf{A}, \Delta_\mathsf{B} \in \mathbb{F}_{2^\kappa}$ is sampled uniformly at random and are non-zero, then the probability that there exists some $i \in [1, \ell]$ such that $x_i \neq 0$ and $\mathsf{P_A}$ or $\mathsf{P_B}$ accepts in the* CheckZero2 *procedure is bounded by $\frac{2}{2^\kappa}$.*

4.2 Global-Key Sampling

We require $\Delta_\mathsf{A} \neq 0$, $\Delta_\mathsf{B} \neq 0$, and $\mathsf{lsb}(\Delta_\mathsf{A} \Delta_\mathsf{B}) = 1$ in the preprocessing phase to facilitate dual-key authentication. Considering the requirement of half-gates garbling, we have the constraints $\mathsf{lsb}(\Delta_\mathsf{A}) = 1$, $\mathsf{msb}(\Delta_\mathsf{B}) = 1$, and $\mathsf{lsb}(\Delta_\mathsf{A} \Delta_\mathsf{B}) = 1$ in $\mathcal{F}_\mathsf{cpre}$. We design the protocol Π_samp in Fig. 4 and argue in Lemma 3 that the key constraints are satisfied.

Lemma 3. *The protocol Π_samp satisfies the following properties:*

– *The outputs satisfy that $\mathsf{lsb}(\Delta_\mathsf{A}) = 1$, $\mathsf{msb}(\Delta_\mathsf{B}) = 1$, and $\mathsf{lsb}(\Delta_\mathsf{A} \Delta_\mathsf{B}) = 1$ in the honest case.*
– *If $\mathsf{lsb}(\Delta_\mathsf{A}) \neq 1$ then $\mathsf{P_B}$ aborts except with probability $2^{-\rho}$. Conditioned on $\Delta_\mathsf{A} \neq 0$, if $\mathsf{lsb}(\Delta_\mathsf{A} \Delta_\mathsf{B}) \neq 1$ then $\mathsf{P_B}$ aborts except with probability $2^{-\rho}$.*
– *If $\mathsf{msb}(\Delta_B) \neq 1$ then $\mathsf{P_A}$ aborts except with probability $2^{-\rho}$. Conditioned on $\Delta_\mathsf{B} \neq 0$, if $\mathsf{lsb}(\Delta_\mathsf{A} \Delta_\mathsf{B}) \neq 1$ then $\mathsf{P_B}$ aborts except with probability $2 \cdot 2^{-\kappa} + 2^{-\rho}$.*

Protocol Π_{samp}

$\mathsf{P_A}$ samples $\Delta_{\mathsf{A}} \leftarrow \mathbb{F}_{2^\kappa}$ such that $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$. $\mathsf{P_B}$ samples $\tilde{\Delta}_{\mathsf{B}} \leftarrow \mathbb{F}_{2^\kappa}$ such that $\mathsf{msb}(\tilde{\Delta}_{\mathsf{B}}) = 1$. Then, $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the following steps.

1. $\mathsf{P_A}$ and $\mathsf{P_B}$ call functionality $\mathcal{F}_{\mathsf{COT}}$ on respective input $(\mathsf{init}, sid_0, \Delta_{\mathsf{A}})$ and (init, sid_0), and then call $\mathcal{F}_{\mathsf{COT}}$ on the same input $(\mathsf{extend}, sid_0, \rho)$ to generate random authenticated bits $[\boldsymbol{u}]_{\mathsf{B}}$.
2. Then $\mathsf{P_A}$ convinces $\mathsf{P_B}$ that $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$ by sending a ρ-bit vector $m_{\mathsf{A}}^0 := (\mathsf{lsb}(\mathsf{K_A}[u_1]), \ldots, \mathsf{lsb}(\mathsf{K_A}[u_\rho]))$ to $\mathsf{P_B}$, who checks that $m_{\mathsf{A}}^0 = (\mathsf{lsb}(\mathsf{M_B}[u_1]) \oplus u_1, \ldots, \mathsf{lsb}(\mathsf{M_B}[u_\rho]) \oplus u_\rho)$ holds.
3. $\mathsf{P_B}$ runs $\mathsf{Fix}(sid_0, \tilde{\Delta}_{\mathsf{B}})$ to generate $[\tilde{\Delta}_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$. Then, $\mathsf{P_A}$ sends $m_{\mathsf{A}}^1 = \mathsf{lsb}(\mathsf{K_A}[\tilde{\Delta}_{\mathsf{B}}])$ to $\mathsf{P_B}$, and $\mathsf{P_B}$ sends $m_{\mathsf{B}}^1 = \mathsf{lsb}(\mathsf{M_B}[\tilde{\Delta}_{\mathsf{B}}])$ to $\mathsf{P_A}$ in parallel. If $m_{\mathsf{A}}^1 \oplus m_{\mathsf{B}}^1 = 0$, both parties compute $[\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}} := [\tilde{\Delta}_{\mathsf{B}}]_{\Delta_{\mathsf{A}}} \oplus 1$ where $\Delta_{\mathsf{B}} = \tilde{\Delta}_{\mathsf{B}} \oplus 1$; otherwise, the parties set $[\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}} := [\tilde{\Delta}_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$.
4. $\mathsf{P_A}$ and $\mathsf{P_B}$ calls $\mathcal{F}_{\mathsf{COT}}$ on respective input (init, sid_0') and $(\mathsf{init}, sid_0', \Delta_{\mathsf{B}})$, and then call $\mathcal{F}_{\mathsf{COT}}$ on the same input $(\mathsf{extend}, sid_0', \rho)$ to generate random authenticated bits $[\boldsymbol{v}]_{\mathsf{A}}$.
5. Then $\mathsf{P_B}$ convinces $\mathsf{P_A}$ that $\mathsf{msb}(\Delta_{\mathsf{B}}) = 1$ by sending a ρ-bit vector $m_{\mathsf{B}}^0 := (\mathsf{msb}(\mathsf{K_B}[v_1]), \ldots, \mathsf{msb}(\mathsf{K_B}[v_\rho]))$ to $\mathsf{P_A}$, who checks that $m_{\mathsf{B}}^0 = (\mathsf{msb}(\mathsf{M_A}[v_1]) \oplus v_1, \ldots, \mathsf{msb}(\mathsf{M_A}[v_\rho]) \oplus v_\rho)$ holds.
6. $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the following steps to mutually check that $\mathsf{lsb}(\Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}}) = 1$.
   (a) Both parties call $\mathcal{F}_{\mathsf{COT}}$ on the same input $(\mathsf{extend}, sid_0, \rho)$ to generate random authenticated bits $[\boldsymbol{x}]_{\mathsf{B}}$, as well as run $\mathsf{Fix}(sid_0, \Delta_{\mathsf{B}} \cdot \boldsymbol{x})$ to generate $[\Delta_{\mathsf{B}} \cdot \boldsymbol{x}]_{\mathsf{B}}$. $\mathsf{P_B}$ proves to $\mathsf{P_A}$ that a set of authenticated triples $\{([x_i]_{\mathsf{B}}, [\Delta_{\mathsf{B}}]_{\mathsf{B}}, [x_i\Delta_{\mathsf{B}}]_{\mathsf{B}})\}_{i\in[1,\rho]}$ is valid by calling $\mathcal{F}_{\mathsf{DVZK}}$, and $\mathsf{P_A}$ aborts if it receives false from $\mathcal{F}_{\mathsf{DVZK}}$.
   (b) Both parties set $\langle \boldsymbol{x} \rangle := \mathsf{Convert1}_{[\cdot]\to\langle\cdot\rangle}([\Delta_{\mathsf{B}} \cdot \boldsymbol{x}]_{\mathsf{B}})$. Then, $\mathsf{P_A}$ sends $m_{\mathsf{A}}^2 := (\mathsf{lsb}(\mathsf{D_A}[x_1]), \ldots, \mathsf{lsb}(\mathsf{D_A}[x_\rho]))$ to $\mathsf{P_B}$, who checks that $m_{\mathsf{A}}^2 = (\mathsf{lsb}(\mathsf{D_B}[x_1]) \oplus x_1, \ldots, \mathsf{lsb}(\mathsf{D_B}[x_\rho]) \oplus x_\rho)$.
   (c) The parties run $\mathsf{Fix}(sid_0', \Delta_{\mathsf{A}})$ to generate $[\Delta_{\mathsf{A}}]_{\mathsf{A}}$.
   (d) Both parties call $\mathcal{F}_{\mathsf{COT}}$ on the same input $(\mathsf{extend}, sid_0', \rho)$ to generate random authenticated bits $[\boldsymbol{y}]_{\mathsf{A}}$, as well as run $\mathsf{Fix}(sid_0', \Delta_{\mathsf{A}} \cdot \boldsymbol{y})$ to generate $[\Delta_{\mathsf{A}} \cdot \boldsymbol{y}]_{\mathsf{A}}$. $\mathsf{P_B}$ proves to $\mathsf{P_A}$ that a set of authenticated triples $\{([y_i]_{\mathsf{A}}, [\Delta_{\mathsf{A}}]_{\mathsf{A}}, [y_i\Delta_{\mathsf{A}}]_{\mathsf{A}})\}_{i\in[1,\rho]}$ is valid by calling $\mathcal{F}_{\mathsf{DVZK}}$, and $\mathsf{P_B}$ aborts if it receives false from $\mathcal{F}_{\mathsf{DVZK}}$.
   (e) Both parties set $\langle \boldsymbol{y} \rangle := \mathsf{Convert1}_{[\cdot]\to\langle\cdot\rangle}([\Delta_{\mathsf{A}} \cdot \boldsymbol{y}]_{\mathsf{A}})$. Then, $\mathsf{P_B}$ sends $m_{\mathsf{B}}^2 := (\mathsf{lsb}(\mathsf{D_B}[y_1]), \ldots, \mathsf{lsb}(\mathsf{D_B}[y_\rho]))$ to $\mathsf{P_A}$, who checks that $m_{\mathsf{B}}^2 = (\mathsf{lsb}(\mathsf{D_A}[y_1]) \oplus y_1, \ldots, \mathsf{lsb}(\mathsf{D_A}[y_\rho]) \oplus y_\rho)$.
   (f) Both parties locally compute two dual-key authenticated bits $\langle 1_{\mathsf{B}} \rangle := \mathsf{Convert1}_{[\cdot]\to\langle\cdot\rangle}([\Delta_{\mathsf{B}}]_{\mathsf{B}})$ and $\langle 1_{\mathsf{A}} \rangle := \mathsf{Convert1}_{[\cdot]\to\langle\cdot\rangle}([\Delta_{\mathsf{A}}]_{\mathsf{A}})$.
   (g) The parties run $\mathsf{CheckZero2}(\langle 1_{\mathsf{B}} \rangle - \langle 1_{\mathsf{A}} \rangle)$, and abort if the check fails.
7. $\mathsf{P_A}$ outputs $(\Delta_{\mathsf{A}}, \alpha_0)$ and $\mathsf{P_B}$ outputs $(\Delta_{\mathsf{B}}, \beta_0)$, such that $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$, $\mathsf{msb}(\Delta_{\mathsf{B}}) = 1$, $\mathsf{lsb}(\Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}}) = 1$ and $\alpha_0 + \beta_0 = \Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$.

Fig. 4. Sub-protocol for sampling global keys.

Proof. For the honest case since $\mathsf{P_A}$ and $\mathsf{P_B}$ follow the protocol instruction when sampling keys, the constraints on Δ_A and Δ_B are satisfied automatically. Moreover, notice that $\mathsf{lsb}(\Delta_\mathsf{A}\tilde{\Delta}_\mathsf{B}) = \mathsf{lsb}(\mathsf{K_A}[\tilde{\Delta}_\mathsf{B}]) \oplus \mathsf{lsb}(\mathsf{M_B}[\tilde{\Delta}_\mathsf{B}])$ and $\mathsf{lsb}(\Delta_\mathsf{A}) = 1$. If the parties discover in step 6b that $\mathsf{lsb}(\Delta_\mathsf{A}\tilde{\Delta}_\mathsf{B}) = 0$, $\mathsf{P_B}$ sets $\Delta_\mathsf{B} := \tilde{\Delta}'_\mathsf{B} \oplus 1$ and $\mathsf{lsb}(\Delta_\mathsf{A}\Delta_\mathsf{B}) = \mathsf{lsb}(\Delta_\mathsf{A}\tilde{\Delta}_\mathsf{B} + \Delta_\mathsf{A}) = 1$.

For the case of a corrupted $\mathsf{P_A}$, notice that $\mathsf{lsb}(\mathsf{K_A}[r]) \oplus \mathsf{lsb}(\mathsf{M_B}[r]) = r \cdot \mathsf{lsb}(\Delta_\mathsf{A})$ and $\mathsf{lsb}(\mathsf{D_A}[r]) \oplus \mathsf{lsb}(\mathsf{D_B}[r]) = r \cdot \mathsf{lsb}(\Delta_\mathsf{A}\Delta_\mathsf{B})$ for $r \in \mathbb{F}_2$. If $\mathsf{lsb}(\Delta_\mathsf{A}) = 0$ then $\mathsf{P_A}$ passing the test is equivalent to $m^0_\mathsf{A} \oplus (\mathsf{lsb}(\mathsf{K_A}[u_1]), \ldots, \mathsf{lsb}(\mathsf{K_A}[u_\rho])) = \boldsymbol{u}$ which happens with $2^{-\rho}$ probability since $\boldsymbol{u}$ is sampled independently from the left-hand side of the equation. Conditioned on $\Delta_\mathsf{A} \neq 0$, the second test passes when $\mathsf{lsb}(\Delta_\mathsf{A}\Delta_\mathsf{B}) = 0$ except with $2^{-\rho}$ probability from similar argument.

For the case of a corrupted $\mathsf{P_B}$, the checks in step 5 and step 6e are equivalent to the corrupted $\mathsf{P_A}$ case. Thus the soundness of the first check is $2^{-\rho}$. Also Lemma 2 guarantees that inconsistent Δ_B will be detected except with $2 \cdot 2^{-\kappa}$ probability. By union bound the soundness of the second check is $2 \cdot 2^{-\kappa} + 2^{-\rho}$.

4.3 Consistency Check Between Values and MAC Tags

In our protocol to generate dual-key authentication, we need a party (e.g., $\mathsf{P_B}$) to use the MAC tags (denoted as $\{\beta_i\}$) of some existing IT-MAC authenticated values as the global keys of another $\mathcal{F}_\mathsf{bCOT}$ instance (denoted as $\{\beta'_i\}$). We enforce this constraint by checking equality between values authenticated by different keys. Our first observation is that the MAC tags are already implicitly authenticated by Δ_A^{-1}.

Authentication Under Inverse Key. We define the Invert macro to *locally* convert $[x]_\mathsf{B} = (\mathsf{K_A}[x], \mathsf{M_B}[x], x)$ to $[y]_{\mathsf{B},\Delta_\mathsf{A}^{-1}} := (\mathsf{K_A}[y]_{\Delta_\mathsf{A}^{-1}}, \mathsf{M_B}[y]_{\Delta_\mathsf{A}^{-1}}, y)$. We note that this technique appeared previously in the certified VOLE protocols [18].

– $[y]_{\mathsf{B},\Delta_\mathsf{A}^{-1}} \leftarrow \mathsf{Invert}([x]_\mathsf{B})$: On input $[x]_\mathsf{B}$ for $x \in \mathbb{F}_{2^\kappa}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the following:
  - $\mathsf{P_B}$ outputs $y := \mathsf{M_B}[x]$ and $\mathsf{M_B}[y]_{\Delta_\mathsf{A}^{-1}} := x$.
  - $\mathsf{P_A}$ outputs $\mathsf{K_A}[y]_{\Delta_\mathsf{A}^{-1}} := \mathsf{K_A}[x] \cdot \Delta_\mathsf{A}^{-1} \in \mathbb{F}_{2^\kappa}$.

We demonstrate the correctness of the Invert macro as follows.

Lemma 4. *Let $[x]_\mathsf{B} = (\alpha, \beta, x)$ where $x \in \mathbb{F}_{2^\kappa}$ then the MAC tag of $\mathsf{P_B}$, β, is implicitly authenticated by Δ_A^{-1}, i.e., the inverse of $\mathsf{P_A}$'s global key over $\mathbb{F}_{2^\kappa}$.*

This claim can be verified by multiplying both side of the equation by Δ_A^{-1}.

$$\underbrace{\beta}_{\mathsf{M_B}[x]} = \underbrace{\alpha}_{\mathsf{K_A}[x]} + x \cdot \Delta_\mathsf{A} \implies \underbrace{x}_{\mathsf{M_B}[\beta]_{\Delta_A^{-1}}} = \underbrace{\alpha \cdot \Delta_\mathsf{A}^{-1}}_{\mathsf{K_A}[\beta]_{\Delta_A^{-1}}} + \beta \cdot \Delta_\mathsf{A}^{-1} .$$

Random Inverse Key Authentication. Notice that in the Invert macro, if we require the input $[x]$ to be uniformly random, i.e., $x \leftarrow \mathbb{F}_{2^\kappa}$, then the output value $y := \mathsf{M}_\mathsf{A}[x] = x\Delta_\mathsf{A} - \mathsf{K}_\mathsf{B}[x]$ is also uniformly random in the view of P_A. Using this method we can generate random $\mathbb{F}_{2^\kappa}$ elements authenticated by Δ_A^{-1}.

Equality Check Across Different Keys. We recall a known technique to verify equality between two values authenticated by respective independent keys [16], which we summarize in the $\mathsf{EQCheck}$ macro. We recall its soundness in Lemma 5 and prove it in the full version [14]. In the following, we assume that $\mathcal{F}_\mathsf{COT}$ has been initialized with (sid, Δ_A) and $(sid', \Delta'_\mathsf{A})$.

– $\mathsf{EQCheck}(\{[y_i]_{\Delta_\mathsf{A}}\}_{i\in[1,\ell]}, \{[y'_i]_{\Delta'_\mathsf{A}}\}_{i\in[1,\ell]})$: On input two sets of authenticated values under different keys $\Delta_\mathsf{A}, \Delta'_\mathsf{A}$, P_A and P_B check that $y_i = y'_i$ for all $i \in [1,\ell]$ as follows:
  1. Let $[y_i]_{\Delta_\mathsf{A}} = (k_i, m_i, y_i)$ and $[y'_i]_{\Delta'_\mathsf{A}} = (k'_i, m'_i, y'_i)$. Two parties P_A and P_B run $\mathsf{Fix}(sid, \{m'_i\}_{i\in[1,\ell]})$ to obtain a set of authenticated values $\{[m'_i]_{\Delta_\mathsf{A}}\}_{i\in[1,\ell]}$, and also run $\mathsf{Fix}(sid', \{m_i\}_{i\in[1,\ell]})$ to get another set of authenticated values $\{[m_i]_{\Delta'_\mathsf{A}}\}_{i\in[1,\ell]}$.
  2. For each $i \in [1,\ell]$, P_A computes $V_i := k_i \cdot \Delta'_\mathsf{A} + k'_i \cdot \Delta_\mathsf{A} + \mathsf{K}_\mathsf{A}[m_i]_{\Delta'_\mathsf{A}} + \mathsf{K}_\mathsf{A}[m'_i]_{\Delta_\mathsf{A}} \in \mathbb{F}_{2^\kappa}$, and P_B computes $W_i := \mathsf{M}_\mathsf{B}[m_i]_{\Delta'_\mathsf{A}} + \mathsf{M}_\mathsf{B}[m'_i]_{\Delta_\mathsf{A}} \in \mathbb{F}_{2^\kappa}$.
  3. P_B sends $h := \mathsf{H}(W_1, \ldots, W_\ell)$ to P_A, who verifies that $h = \mathsf{H}(V_1, \ldots, V_\ell)$. If the check fails, P_A aborts.

Lemma 5. *If Δ_A and Δ'_A are independently sampled from $\mathbb{F}_{2^\kappa}$, then the probability that there exists some $i \in [1,\ell]$ such that $y_i \neq y'_i$ and P_A accepts in the $\mathsf{EQCheck}$ procedure is bounded by $\frac{3}{2^\kappa}$.*

The Consistency Check. The observation in Lemma 4 suggests that the MAC tags $\{\beta_i\}$ are already implicitly authenticated by Δ_A^{-1}. Moreover, by calling $\mathsf{Fix}(\Delta'_\mathsf{A})$, P_A and P_B can acquire $\{[\Delta'_\mathsf{A}]_{\beta'_i}\}$ and locally convert them to $\{[\beta'_i]_{\Delta'_\mathsf{A}}\}$. Since Δ_A and Δ'_A are independent, we can apply $\mathsf{EQCheck}$ to complete our goal.

We list the differences that inverse key authentication induces to $\mathsf{EQCheck}$. Recall that $\mathcal{F}_\mathsf{COT}$ has been initialized with (sid, Δ_A) and $(sid', \Delta'_\mathsf{A})$.

– $\mathsf{EQCheck}(\{[\beta_i]_{\Delta_\mathsf{A}^{-1}}\}_{i\in[1,\ell]}, \{[\beta'_i]_{\Delta'_\mathsf{A}}\}_{i\in[1,\ell]})$: On input two sets of authenticated values under different keys $\Delta_\mathsf{A}^{-1}, \Delta'_\mathsf{A}$, P_A and P_B check that $\beta_i = \beta'_i$ for all $i \in [1,\ell]$ as follows:
  1. P_A and P_B call $\mathcal{F}_\mathsf{COT}$ on the same input $(\mathsf{extend}, sid, \ell\kappa)$ to get authenticated bits $[\boldsymbol{r}_1]_{\Delta_\mathsf{A}}, \ldots, [\boldsymbol{r}_\ell]_{\Delta_\mathsf{A}}$ with $\boldsymbol{r}_i \in \mathbb{F}_2^\kappa$. Then, for $i \in [1,\ell]$, both parties define $[r_i]_{\Delta_\mathsf{A}} := \mathsf{B2F}([\boldsymbol{r}_i]_{\Delta_\mathsf{A}})$ with $r_i \in \mathbb{F}_{2^\kappa}$, and set $[s_i]_{\Delta_\mathsf{A}^{-1}} := \mathsf{Invert}([r_i]_{\Delta_\mathsf{A}})$.
  2. P_A and P_B run $\mathsf{EQCheck}(\{[\beta_i]_{\Delta_\mathsf{A}^{-1}}\}_{i\in[1,\ell]}, \{[\beta'_i]_{\Delta'_\mathsf{A}}\}_{i\in[1,\ell]})$ as described above, except that they use random authenticated values $[s_i]_{\Delta_\mathsf{A}^{-1}}$ for $i \in [1,\ell]$ to generate chosen authenticated values under Δ_A^{-1} in the Fix procedure.

It is straightforward to verify the soundness is not affected by changing to the inverse key. Thus we omit the proof of the following lemma.

Lemma 6. *If Δ_{A} and Δ'_{A} are independently sampled from $\mathbb{F}_{2^\kappa}$, then the probability that there exists some $i \in [1, \ell]$ such that $\beta_i \neq \beta'_i$ and P_{A} accepts in the* $\mathsf{EQCheck}$ *procedure is bounded by $\frac{3}{2^\kappa}$.*

4.4 Circuit Dependent Compressed Preprocessing

We now describe the protocol to realize the functionality $\mathcal{F}_{\mathsf{cpre}}$. Following the conventions of previous works, we defer all consistency checks to the end of the protocol. Notice that step 1 to step 5 corresponds to the circuit-independent phase (where we only require the scale rather than the topology information of the circuit) while the rest is the circuit-dependent phase (where the entire circuit is known). The protocol is shown in Fig. 5 and Fig. 6. We then analyze its security in Theorem 1. The proof is presented in the full version [14].

Theorem 1. *Protocol Π_{cpre} shown in Figs. 5 and 6 securely realizes functionality $\mathcal{F}_{\mathsf{cpre}}$ (Fig. 3) against malicious adversaries in the $(\mathcal{F}_{\mathsf{COT}}, \mathcal{F}_{\mathsf{bCOT}}, \mathcal{F}_{\mathsf{DVZK}}, \mathcal{F}_{\mathsf{EQ}}, \mathcal{F}_{\mathsf{Rand}})$-hybrid model.*

Consistency Checks. We explain the rationale of the consistency checks in Π_{cpre}.

- The $\mathcal{F}_{\mathsf{DVZK}}$ in step 11 checks that the Fix inputs of P_{A} in step 6 and those of P_{B} in step 6 and step 3 are well-formed.
- The $\mathsf{CheckZero2}$ and $\mathsf{EQCheck}$ in step 12 ensure to P_{A} that the multiple instances of Δ_{B} in Π_{samp} (Fig. 4) and Π_{cpre} (step 4 and step 5 in Fig. 5) are identical. Also, P_{B} can make sure that Δ'_{A} in step 4 and step 5 of Π_{cpre} (Fig. 5) are identical.
- P_{B} checks that the message in step 9 of Π_{cpre} from P_{A} are correct. To do this, P_{B} checks its locally computed value against the dual-key authenticated value, which is unalterable. Moreover, we reduce the communication using random linear combination. This is done in step 14 and step 15 of Π_{cpre} (Fig. 6).
- P_{A} checks that the Fix inputs of P_{B} in step 10 of Π_{cpre} (Fig. 6) are correct. This is done by checking the IT-MAC authenticated values against the dual-key authenticated ones in step 16 of Π_{cpre} (Fig. 6).

Optimization Based on Fiat-Shamir. In the protocol Π_{cpre}, both parties choose random public challenges by calling functionality $\mathcal{F}_{\mathsf{Rand}}$. Based on the Fiat-Shamir heuristic [19], both parties can generate the challenges by hashing the protocol transcript up until this point, which is secure in the random oracle model. This optimization can save one communication round, and has also been used in previous work such as [10,43].

Protocol Π_{cpre}

Inputs: A Boolean circuit $\mathcal{C}$ that consists of a list of gates of the form (i, j, k, T). Let $n = |\mathcal{W}| + |\mathcal{I}_{\mathsf{B}}|$, $m = |\mathcal{W}| + |\mathcal{I}_{\mathsf{A}}|$, $L = \lceil \rho \log \frac{2en}{\rho} + \frac{\log \rho}{2} \rceil$ and $t = |\mathcal{W}|$.

Initialize: $\mathsf{P_A}$ and $\mathsf{P_B}$ execute sub-protocol Π_{samp} (Figure 4) to obtain $(\Delta_{\mathsf{A}}, \alpha_0)$ and $(\Delta_{\mathsf{B}}, \beta_0)$ respectively, such that $\mathsf{lsb}(\Delta_{\mathsf{A}}) = 1$, $\mathsf{msb}(\Delta_{\mathsf{B}}) = 1$, $\mathsf{lsb}(\Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}}) = 1$ and $\alpha_0 + \beta_0 = \Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}} \in \mathbb{F}_{2^\kappa}$. Thus, both parties hold $\langle 1 \rangle$ (i.e., $[\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$). After the sub-protocol execution, $\mathcal{F}_{\mathsf{COT}}$ was initialized by session identifier sid_0 and Δ_{A}.

Generate authenticated AND triples: $\mathsf{P_A}$ and $\mathsf{P_B}$ execute as follows:

1. $\mathsf{P_B}$ samples a matrix $\mathbf{M} \leftarrow \mathbb{F}_2^{n \times L}$ and sends it to $\mathsf{P_A}$.
2. Both parties call $\mathcal{F}_{\mathsf{COT}}$ on input $(\mathsf{extend}, sid_0, L)$ to generate random authenticated bits $[\boldsymbol{b}^*]$ where $\boldsymbol{b}^* \in \mathbb{F}_2^L$ and compute $[\boldsymbol{b}] := \mathbf{M} \cdot [\boldsymbol{b}^*]$ with $\boldsymbol{b} \in \mathbb{F}_2^n$.
3. Both parties run $\mathsf{Fix}(sid_0, \{b_i^* \Delta_{\mathsf{B}}\}_{i \in [1,L]})$ to generate authenticated values $[b_i^* \Delta_{\mathsf{B}}]_{\mathsf{B}}$. The parties locally run $\langle b_i^* \rangle \leftarrow \mathsf{Convert1}_{[\cdot] \to \langle \cdot \rangle}([b_i^* \Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}})$. Let $\alpha_i, \beta_i \in \mathbb{F}_{2^\kappa}$ such that $\alpha_i + \beta_i = b_i^* \cdot \Delta_{\mathsf{A}} \cdot \Delta_{\mathsf{B}}$ for each $i \in [1, L]$.
4. $\mathsf{P_B}$ and $\mathsf{P_A}$ call $\mathcal{F}_{\mathsf{bCOT}}^{L+1}$ on respective inputs $(\mathsf{init}, sid_1, \beta_1, ..., \beta_L, \Delta_{\mathsf{B}})$ and (init, sid_1). Then, both parties send $(\mathsf{extend}, sid_1, m)$ to $\mathcal{F}_{\mathsf{bCOT}}^{L+1}$, which returns $([\boldsymbol{a}]_{\beta_1}, \ldots, [\boldsymbol{a}]_{\beta_L}, [\boldsymbol{a}]_{\Delta_{\mathsf{A}}})$ where $\boldsymbol{a} \in \mathbb{F}_2^m$. Then, $\mathsf{P_A}$ samples $\Delta'_{\mathsf{A}} \leftarrow \mathbb{F}_{2^\kappa}$, and then two parties run $\mathsf{Fix}(sid_1, \Delta'_{\mathsf{A}})$ to obtain $([\Delta'_{\mathsf{A}}]_{\beta_1}, \ldots, [\Delta'_{\mathsf{A}}]_{\beta_L}, [\Delta'_{\mathsf{A}}]_{\Delta_{\mathsf{B}}})$. $\mathsf{P_A}$ and $\mathsf{P_B}$ set $\langle 1_{\mathsf{B}}^{(1)} \rangle := \mathsf{Convert1}_{[\cdot] \to \langle \cdot \rangle}([\Delta_{\mathsf{B}}]_{\Delta'_{\mathsf{A}}})$ where $[\Delta_{\mathsf{B}}]_{\Delta'_{\mathsf{A}}}$ is equivalent to $[\Delta'_{\mathsf{A}}]_{\Delta_{\mathsf{B}}}$, and define $[\beta_i]_{\Delta'_{\mathsf{A}}} = [\Delta'_{\mathsf{A}}]_{\beta_i}$ for $i \in [1, L]$.
5. $\mathsf{P_B}$ and $\mathsf{P_A}$ call $\mathcal{F}_{\mathsf{bCOT}}^{2}$ on respective input $(\mathsf{init}, sid_2, \beta_0, \Delta_{\mathsf{B}})$ and (init, sid_2). Then, both parties send $(\mathsf{extend}, sid_2, t)$ to $\mathcal{F}_{\mathsf{bCOT}}^{2}$, which returns $([\hat{\boldsymbol{a}}]_{\beta_0}, [\hat{\boldsymbol{a}}]_{\Delta_{\mathsf{B}}})$ to the parties. $\mathsf{P_A}$ and $\mathsf{P_B}$ run $\mathsf{Fix}(sid_2, \Delta'_{\mathsf{A}})$ to get $[\Delta'_{\mathsf{A}}]_{\beta_0}$ and $[\Delta'_{\mathsf{A}}]_{\Delta_{\mathsf{B}}}$, and then locally convert to $[\beta_0]_{\Delta'_{\mathsf{A}}}$ and $[\Delta_{\mathsf{B}}]_{\Delta'_{\mathsf{A}}}$. Then, both parties set $\langle 1_{\mathsf{B}}^{(2)} \rangle :=$ $\mathsf{Convert1}_{[\cdot] \to \langle \cdot \rangle}([\Delta_{\mathsf{B}}]_{\Delta'_A})$.
6. For $w \in \mathcal{I}_{\mathsf{A}}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ set $[b_w] = [0]$; for $w \in \mathcal{I}_{\mathsf{B}}$, both parties set $[a_w] = [0]$. For each wire $w \in \mathcal{I}_{\mathsf{A}} \cup \mathcal{W}$, two parties define $[a_w]$ in $[\boldsymbol{a}]$ as the authenticated bit on wire w; for each wire $w \in \mathcal{I}_{\mathsf{B}} \cup \mathcal{W}$, define $[b_w]$ in $[\boldsymbol{b}]$ as the authenticated bit on wire w. In a topological order, for each gate (i, j, k, T), $\mathsf{P_A}$ and $\mathsf{P_B}$ do the following:
   - If $T = \oplus$, compute $[a_k] := [a_i] \oplus [a_j]$ and $[b_k] := [b_i] \oplus [b_j]$.
   - If $T = \wedge$, $\mathsf{P_A}$ computes $a_{i,j} := a_i \wedge a_j$, and $\mathsf{P_B}$ computes $b_{i,j} := b_i \wedge b_j$.
7. Both parties run $\mathsf{Fix}(sid_0, \{b_{i,j}\}_{(i,j,*,\wedge) \in \mathcal{C}_{\mathsf{and}}})$ to generate a set of authenticated bits $\{[b_{i,j}]\}$, and also execute $\mathsf{Fix}(sid_2, \{a_{i,j}\}_{(i,j,*,\wedge) \in \mathcal{C}_{\mathsf{and}}})$ to generate a set of authenticated bits $\{[a_{i,j}]\}$.
8. For $i \in [1, n], j \in [1, L]$, $\mathsf{P_A}$ and $\mathsf{P_B}$ set $\langle a_i b_j^* \rangle := \mathsf{Convert2}_{[\cdot] \to \langle \cdot \rangle}([a_i]_{\beta_j}, \langle b_j^* \rangle)$. Then, both parties collect these dual-key authenticated bits to obtain $\langle a_i \boldsymbol{b}^* \rangle$, and compute $\langle a_i b_j \rangle$ and $\langle a_j b_i \rangle$ for each AND gate $(i, j, k, \wedge)$ from $\mathbf{M} \cdot \langle a_i \boldsymbol{b}^* \rangle$ for $i \in [1, n]$. Further, both parties set $\langle \hat{a}_k \rangle := \mathsf{Convert2}_{[\cdot] \to \langle \cdot \rangle}([\hat{a}_k]_{\beta_0}, \langle 1 \rangle)$ and $\langle a_{i,j} \rangle \leftarrow \mathsf{Convert2}_{[\cdot] \to \langle \cdot \rangle}([a_{i,j}]_{\beta_0}, \langle 1 \rangle)$.

Fig. 5. The compressed preprocessing protocol for a Boolean circuit $\mathcal{C}$.

Communication Complexity. As recent PCG-like COT protocols have communication complexity sublinear to the number of resulting correlations, we can ignore the communication cost of generating random COT correlations when

Protocol Π_{cpre}, continued

9. For each AND gate $(i, j, k, \wedge)$, $\mathsf{P_A}$ and $\mathsf{P_B}$ locally compute $\langle \tilde{b}_k \rangle := \langle a_{i,j} \rangle \oplus \langle a_i b_j \rangle \oplus \langle a_j b_i \rangle \oplus \langle \hat{a}_k \rangle$. Then, for each $k \in \mathcal{W}$, $\mathsf{P_A}$ sends $\mathsf{lsb}(\mathsf{D_A}[\tilde{b}_k])$ to $\mathsf{P_B}$, who computes $\tilde{b}_k := \mathsf{lsb}(\mathsf{D_A}[\tilde{b}_k]) \oplus \mathsf{lsb}(\mathsf{D_B}[\tilde{b}_k])$. For each AND gate $(i, j, k, \wedge)$, $\mathsf{P_B}$ computes $\hat{b}_k := \tilde{b}_k \oplus b_{i,j}$.
10. Both parties run $\mathsf{Fix}(sid_0, \{\hat{b}_k\}_{k \in \mathcal{W}})$ to obtain $[\hat{b}_k]$ for each $k \in \mathcal{W}$.

Consistency check: $\mathsf{P_A}$ and $\mathsf{P_B}$ perform the following consistency-check steps:

11. Let $[B_i^*] = [b_i^* \Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$ produced in the previous phase. Both parties call $\mathcal{F}_{\mathsf{DVZK}}$ to prove the following statements hold:
    - For each AND gate $(i, j, k, \wedge)$, for $([b_i], [b_j], [b_{i,j}])$, $b_{i,j} = b_i \wedge b_j$.
    - For each AND gate $(i, j, k, \wedge)$, for $([a_i], [a_j], [a_{i,j}])$, $a_{i,j} = a_i \wedge a_j$.
    - For each $i \in [1, L]$, for $([b_i^*], [\Delta_{\mathsf{B}}], [B_i^*])$, $B_i^* = b_i^* \cdot \Delta_{\mathsf{B}}$.
12. $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_{\mathsf{COT}}$ on respective input $(\mathsf{init}, sid_3, \Delta'_{\mathsf{A}})$ and (init, sid_3). Then they run $[\Delta_{\mathsf{B}}]_{\Delta'_{\mathsf{A}}} := \mathsf{Fix}(sid_3, \Delta_{\mathsf{B}})$ and $\langle 1_{\mathsf{B}}^{(3)} \rangle := \mathsf{Convert1}_{[\cdot] \to \langle \cdot \rangle}([\Delta_{\mathsf{B}}]_{\Delta'_{\mathsf{A}}})$. $\mathsf{P_A}$ and $\mathsf{P_B}$ run $\mathsf{CheckZero2}(\langle 1_{\mathsf{B}}^{(1)} \rangle - \langle 1_{\mathsf{B}}^{(2)} \rangle, \langle 1_{\mathsf{B}}^{(2)} \rangle - \langle 1_{\mathsf{B}}^{(3)} \rangle)$ and $\mathsf{EQCheck}([\Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}, [\Delta_{\mathsf{B}}]_{\Delta'_{\mathsf{A}}})$ to check that $\Delta'_{\mathsf{A}}, \Delta_{\mathsf{B}}$ are consistent when it is used in different functionalities. Both parties run $[\beta_i]_{\Delta_{\mathsf{A}}^{-1}} \leftarrow \mathsf{Invert}([b_i^* \Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}})$ for each $i \in [0, L]$, and then execute $\mathsf{EQCheck}(\{[\beta_i]_{\Delta_{\mathsf{A}}^{-1}}\}_{i \in [0,L]}, \{[\beta_i]_{\Delta'_{\mathsf{A}}}\}_{i \in [0,L]})$.
13. $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_{\mathsf{COT}}$ on input $(\mathsf{extend}, sid_0, \kappa)$ to generate a vector of random authenticated bits $[\boldsymbol{r}]_{\mathsf{B}}$ with $\boldsymbol{r} \in \mathbb{F}_2^{\kappa}$, and run $[r]_{\mathsf{B}} \leftarrow \mathsf{B2F}([\boldsymbol{r}]_{\mathsf{B}})$ where $r = \sum_{i \in [0, \kappa)} r_i \cdot X^i \in \mathbb{F}_{2^\kappa}$. Then both parties run $\mathsf{Fix}(sid_0, r \cdot \Delta_{\mathsf{B}})$ to obtain $[r \cdot \Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}}$. The parties execute $\langle r \rangle \leftarrow \mathsf{Convert1}_{[\cdot] \to \langle \cdot \rangle}([r \cdot \Delta_{\mathsf{B}}]_{\Delta_{\mathsf{A}}})$.
14. $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_{\mathsf{Rand}}$ to sample a random element $\chi \in \mathbb{F}_{2^\kappa}$.
15. $\mathsf{P_A}$ convinces $\mathsf{P_B}$ that $\tilde{b}_k$ is correct (and thus $\hat{b}_k$ is correct) for $k \in \mathcal{W}$ as follows.
    (a) Both parties compute $\langle y \rangle := \sum_{k \in \mathcal{W}} \chi^k \cdot \langle \tilde{b}_k \rangle + \langle r \rangle$. Then $\mathsf{P_B}$ sends y to $\mathsf{P_A}$.
    (b) The parties execute $\mathsf{CheckZero2}(\langle y \rangle - y \cdot \langle 1 \rangle)$.
16. $\mathsf{P_B}$ convinces $\mathsf{P_A}$ that $[\hat{b}_k]$ is correct for $k \in \mathcal{W}$ as follows:
    (a) For each AND gate $(i, j, k, \wedge)$, $\mathsf{P_A}$ and $\mathsf{P_B}$ compute $[\tilde{b}_k]_{\mathsf{B}} := [\hat{b}_k]_{\mathsf{B}} \oplus [b_{i,j}]_{\mathsf{B}}$.
    (b) Both parties compute $[y]_{\mathsf{B}} := \sum_{k \in \mathcal{W}} \chi^k \cdot [\tilde{b}_k]_{\mathsf{B}} + [r]_{\mathsf{B}}$.
    (c) $\mathsf{P_A}$ and $\mathsf{P_B}$ run $\mathsf{CheckZero}([y]_{\mathsf{B}} - y)$.

Output: $\mathsf{P_A}$ and $\mathsf{P_B}$ output a matrix $\mathbf{M}$ along with $([\boldsymbol{a}], [\hat{\boldsymbol{a}}], [\boldsymbol{b}^*], [\hat{\boldsymbol{b}}])$.

Fig. 6. The compressed preprocessing protocol for a Boolean circuit $\mathcal{C}$, continued.

counting the communication amortized to every triple. Our checking protocols only introduce a negligibly small communication overhead. Therefore, the Fix procedure brings the main communication cost where Fix is used to transform random COT to chosen COT. Also, since parameter L is logarithmic to the number n of triples, we only need to consider the Fix procedures related to n.

This includes IT-MAC generation of $a_{i,j}$ (from $\mathsf{P_A}$ to $\mathsf{P_B}$ in step 6 of Fig. 5), $b_{i,j}$ (from $\mathsf{P_B}$ to $\mathsf{P_A}$ in the same step), $\hat{b}_k$ (from $\mathsf{P_B}$ to $\mathsf{P_A}$ in step 10 of Fig. 6). In addition, for each triple, $\mathsf{P_A}$ needs to send $\mathsf{lsb}(\mathsf{D}[\tilde{b}_k])$ to $\mathsf{P_B}$ in step 9 of Fig. 6. Overall, the one-way communication cost is 2 bits per triple.

5 Authenticated Garbling from COT

Now we describe the online phase of our two-party computation protocol. We first introduce a generalized distributed garbling syntax which can be instantiated by different schemes and then introduce the complete Boolean circuit evaluation protocol Π_{2PC}.

5.1 Distributed Garbling

We define the format of distributed garbling using two macros Garble and Eval, assuming that the preprocessing information is ready. Notice that these two macros can be instantiated by different garbling schemes. In our main protocol that optimizes towards one-way communication we instantiate it using the distributed half-gates garbling [29] whereas we use the optimized WRK garbling of Dittmer et al. [16] for the version that optimizes towards two-way communication. We recall the respective schemes in the full version [14].

- $\mathsf{Garble}(\mathcal{C})$: P_A and P_B perform *local* operations as follows:
  - P_A computes and outputs $(\mathcal{GC}_\mathsf{A}, \{\mathsf{L}_{w,0}, \mathsf{L}_{w,1}\}_{w\in\mathcal{I}_\mathsf{A}\cup\mathcal{I}_\mathsf{B}\cup\mathcal{W}\cup\mathcal{O}})$.
  - P_B computes and outputs $\mathcal{GC}_\mathsf{B}$.
- $\mathsf{Eval}(\mathcal{GC}_\mathsf{A}, \mathcal{GC}_\mathsf{B}, \{(\Lambda_w, \mathsf{L}_{w,\Lambda_w})\}_{w\in\mathcal{I}_\mathsf{A}\cup\mathcal{I}_\mathsf{B}})$: P_B evaluates the garbled circuit and obtain $\{\Lambda_w, \mathsf{L}_{w,\Lambda_w}\}_{w\in\mathcal{W}\cup\mathcal{O}}$.

The addition of evaluator's random masks is to decouple the abort probability with the real input values (recall that the Eval function only requires masked values). The following definition captures this security property.

Definition 2. *For a distributed garbling scheme with preprocessing defined by* Garble *and* Eval*, consider the event* Bad *where the evaluator aborts or outputs masked wire value* Λ_w *that is incorrect (wrt. the input values of* Eval *and the masks of preprocessing). We call a distributed garbling scheme to be* ϵ-selective failure resilience*, if conditioned on the garbled circuit* $\mathcal{GC}_\mathsf{A}, \mathcal{GC}_\mathsf{B}$*, the evaluator's candidate input wire labels* $\{(\mathsf{L}_{w,0}, \mathsf{L}_{w,1})\}_{w\in\mathcal{I}_\mathsf{B}}$ *and the garbler's input wire masked values and labels* $\{(\Lambda_w, \mathsf{L}_w)\}_{w\in\mathcal{I}_\mathsf{A}}$*, for any two pairs of* P_B*'s inputs* $\boldsymbol{y}, \boldsymbol{y}'$*, we have*

$$|\Pr[\mathsf{Bad}|\boldsymbol{y}] - \Pr[\mathsf{Bad}|\boldsymbol{y}']| \leq \epsilon \ ,$$

where $\Pr[\mathsf{Bad}|\boldsymbol{y}]$ *denotes the probability that the event* Bad *happens when the evaluator's input value is* $\boldsymbol{y}$ *and with aforementioned conditions.*

With uncompressed preprocessing the DILO-WRK and KRRW distributed garbling (recalled in the full version [14].) has 0-selective failure resilience [29,36] since the inputs Λ_w to Eval are completely masked and independent of the real input. In Lemma 9 we show that for the DILO-WRK and KRRW schemes, replacing the evaluator's mask to ρ-wise independent randomness induces $2^{-\rho}$-selective failure resilience.

The next lemma states that after evaluating the garbled circuit the garbler and evaluator implicitly holds the authentication of the masked public wire values (color/permutation bits). To the best of our knowledge we are the first to apply this observation in the consistency check of authenticated garbling.

Lemma 7. *After running* Eval*, the evaluator holds the 'color bits'* Λ_w *for every wire* $w \in \mathcal{W}$*. The garbler* $\mathsf{P_A}$ *and evaluator* $\mathsf{P_B}$ *also hold* $\mathsf{K_A}[\Lambda_w], \mathsf{M_B}[\Lambda_w]$ *subject to* $\mathsf{M_B}[\Lambda_w] = \mathsf{K_A}[\Lambda_w] + \Lambda_w \Delta_\mathsf{A}$.

Proof. We can define the following values using only wire labels:

$$\Lambda_w := (\mathsf{L}_{w,0} \oplus \mathsf{L}_{w,\Lambda_w}) \cdot \Delta_\mathsf{A}^{-1}, \quad \mathsf{M_B}[\Lambda_w] := \mathsf{L}_{w,\Lambda_w}, \quad \mathsf{K_A}[\Lambda_w] := \mathsf{L}_{w,0} \ .$$

It is easy to verify $\mathsf{M_B}[\Lambda_w] = \mathsf{K_A}[\Lambda_w] + \Lambda_w \cdot \Delta_\mathsf{A}$, which implies that $[\Lambda_w]_\mathsf{B} := (\mathsf{L}_{w,0}, \mathsf{L}_{w,\Lambda_w}, \Lambda_w)$ is a valid IT-MAC.

5.2 A Dual Execution Protocol Without Leakage

We describe a malicious secure 2PC protocol with almost the same one-way communication as half-gates garbling. We achieve this by adapting the dual execution technique to the distributed garbling setting. Intuitively, our observation in Lemma 7 allows us to check the consistency of every wire of the circuit. Together with some IT-MAC techniques to ensure input consistency, our protocol circumvents the one-bit leakage of previous dual execution protocols [27,28].

In the following descriptions, we denote the actual value induced by the input on each wire w of the circuit $\mathcal{C}$ by z_w. The masked value on that wire is denoted as $\Lambda_w := z_w \oplus a_w \oplus b_w$ which is revealed to the evaluator during evaluation. The protocol is described in Fig. 7 and Fig. 8.

Intuitions of Consistency Checking. The security of the semi-honest garbled circuit guarantees that when the garbled circuit is correctly computed, then except with negligible probability the evaluator can only acquire one of the two labels (corresponding to the execution path) for each wire in the circuit. Thus, we can check the color bits of the honest party against the labels that the corrupted party acquires (in the separate execution) to verify consistency.

Using the notations from Lemma 7, let $\bar{\Lambda}_w := (\mathsf{L}_{w,\Lambda_w} \oplus \mathsf{L}_{w,0}) \cdot \Delta_\mathsf{A}^{-1}, \bar{\Lambda}'_w := (\mathsf{L}'_{w,\Lambda'_w} \oplus \mathsf{L}'_{w,0}) \cdot \Delta_\mathsf{B}^{-1}$ for $w \in \mathcal{W}$. Our goal is to check the following equations where the left-hand (resp. right-hand) side is the evaluation result of $\mathsf{P_A}$ (resp. $\mathsf{P_B}$).

$$\bar{\Lambda}'_w \oplus a'_w \oplus b'_w = \Lambda_w \oplus a_w \oplus b_w \text{ for the corrupted } \mathsf{P_A} \text{ case,} \quad (1)$$
$$\Lambda'_w \oplus a'_w \oplus b'_w = \bar{\Lambda}_w \oplus a_w \oplus b_w \text{ for the corrupted } \mathsf{P_B} \text{ case.} \quad (2)$$

Multiplying the first equation by Δ_B, the second by Δ_A and do summation[3] gives the $\tilde{V}_w^\mathsf{A}, \tilde{V}_w^\mathsf{B}$ values in the consistency checking.

$$\begin{matrix} (a_w + a'_w + \Lambda'_w)\Delta_\mathsf{A} + \mathsf{M_A}[a_w + a'_w] \\ + \mathsf{M_A}[\bar{\Lambda}'_w] + \mathsf{K_A}[b_w + b'_w + \bar{\Lambda}_w] \end{matrix} = \begin{matrix} (b_w + b'_w + \Lambda_w)\Delta_\mathsf{B} + \mathsf{M_B}[b_w + b'_w] \\ + \mathsf{M_B}[\bar{\Lambda}_w] + \mathsf{K_B}[a_w + a'_w + \bar{\Lambda}'_w] \end{matrix}$$

[3] We define a_w, a'_w, b_w, b'_w by the MAC tag and keys to implicitly authenticate them.

Protocol Π_{2PC}

Inputs: In the preprocessing phase, $\mathsf{P_A}$ and $\mathsf{P_B}$ agree on a Boolean circuit $\mathcal{C}$ with circuit-input wires $\mathcal{I}_\mathsf{A} \cup \mathcal{I}_\mathsf{B}$, output wires of all AND gates $\mathcal{W}$ and circuit-output wires $\mathcal{O}$. In the online phase, $\mathsf{P_A}$ holds an input $x \in \{0,1\}^{|\mathcal{I}_\mathsf{A}|}$ and $\mathsf{P_B}$ holds an input $y \in \{0,1\}^{|\mathcal{I}_\mathsf{B}|}$; $\mathsf{P_B}$ will receive the output $z = \mathcal{C}(x,y)$. Let $\mathsf{H} : \{0,1\}^{2\kappa} \to \{0,1\}^\kappa$ and $\mathsf{H}' : \{0,1\}^* \to \{0,1\}^\kappa$ be two random oracles.

Preprocessing: $\mathsf{P_A}$ plays the role of a garbler and $\mathsf{P_B}$ acts as an evaluator, and two parties execute as follows:

1. Both parties call $\mathcal{F}_\mathsf{cpre}$ to obtain a matrix $\mathbf{M}$ and vectors of authenticated bits $([\boldsymbol{a}], [\hat{\boldsymbol{a}}], [\boldsymbol{b}^*], [\hat{\boldsymbol{b}}])$. The parties locally compute $[\boldsymbol{b}] := \mathbf{M} \cdot [\boldsymbol{b}^*]$.
2. Following a predetermined topological order, $\mathsf{P_A}$ and $\mathsf{P_B}$ use $([\boldsymbol{a}], [\hat{\boldsymbol{a}}], [\boldsymbol{b}], [\hat{\boldsymbol{b}}])$ to obtain authenticated masks $[a_w], [b_w]$ for each wire w and other authenticated bits that will be used in the construction of authenticated garbling.
3. Using the authenticated bits from the previous step and the KRRW garbling scheme, $\mathsf{P_A}$ and $\mathsf{P_B}$ run Garble to generate a distributed garbled circuit $(\mathcal{GC}_\mathsf{A}, \mathcal{GC}_\mathsf{B})$, and $\mathsf{P_A}$ sends $\mathcal{GC}_\mathsf{A}$ to $\mathsf{P_B}$. For each wire w, two garbled labels $\mathsf{L}_{w,0}, \mathsf{L}_{w,1} \in \{0,1\}^\kappa$ are generated and satisfy $\mathsf{L}_{w,1} = \mathsf{L}_{w,0} \oplus \Delta_\mathsf{A}$. $\mathsf{P_A}$ knows the label $\mathsf{L}_{w,0}$ for each wire w as well as Δ_A.

Online: In the following steps, $\mathsf{P_A}$ securely transmits one label on each circuit-input wire to $\mathsf{P_B}$, and $\mathsf{P_B}$ evaluates the circuit.

4. For each $w \in \mathcal{I}_\mathsf{A}$, $\mathsf{P_A}$ computes a masked value $\Lambda_w := x_w \oplus a_w \in \{0,1\}$, and then sends $(\Lambda_w, \mathsf{L}_{w,\Lambda_w})$ to $\mathsf{P_B}$.
5. $\mathsf{P_A}$ and $\mathsf{P_B}$ call $\mathcal{F}_\mathsf{COT}$ on respective input $(\mathsf{init}, sid, \Delta_\mathsf{A})$ and (init, sid), and then send $(\mathsf{extend}, sid, |\mathcal{I}_\mathsf{B}|)$ to $\mathcal{F}_\mathsf{COT}$, which returns random authenticated bits $[\boldsymbol{r}]_\mathsf{B}$ to the parties.
6. For each $w \in \mathcal{I}_\mathsf{B}$, $\mathsf{P_B}$ computes $\Lambda_w := y_w \oplus b_w$ and then sends $d_w := \Lambda_w \oplus r_w$ to $\mathsf{P_A}$. Both parties set $[\Lambda_w]_\mathsf{B} := [r_w]_\mathsf{B} \oplus d_w$. For each $w \in \mathcal{I}_\mathsf{B}$, $\mathsf{P_A}$ sends $m_{w,0} := \mathsf{H}(\mathsf{K_A}[\Lambda_w], w\|1) \oplus \mathsf{L}_{w,0}$ and $m_{w,1} := \mathsf{H}(\mathsf{K_A}[\Lambda_w] \oplus \Delta_\mathsf{A}, w\|1) \oplus \mathsf{L}_{w,1}$ to $\mathsf{P_B}$, who computes $\mathsf{L}_{w,\Lambda_w} := m_{w,\Lambda_w} \oplus \mathsf{H}(\mathsf{M_B}[\Lambda_w], w\|1)$.
7. $\mathsf{P_B}$ runs $\mathsf{Eval}(\mathcal{GC}_\mathsf{A}, \mathcal{GC}_\mathsf{B}, \{(\Lambda_w, \mathsf{L}_{w,\Lambda_w})\}_{w \in \mathcal{I}_\mathsf{A} \cup \mathcal{I}_\mathsf{B}})$ to obtain $(\Lambda_w, \mathsf{L}_{w,\Lambda_w})$ for each wire $w \in \mathcal{W} \cup \mathcal{O}$. For each $w \in \mathcal{W}$, both parties define $[\Lambda_w]_\mathsf{B} = (\mathsf{L}_{w,0}, \mathsf{L}_{w,\Lambda_w}, \Lambda_w)$.

Fig. 7. Actively secure 2PC protocol in the $\mathcal{F}_\mathsf{cpre}$-hybrid model.

Communication Complexity. In our dual execution protocol, $\mathsf{P_A}$ and $\mathsf{P_B}$ sends $(2\kappa+1)t + (\kappa+1)|\mathcal{I}_\mathsf{A}| + 2\kappa|\mathcal{I}_\mathsf{B}| + \kappa + |\mathcal{O}|$ and $(2\kappa+1)t + (\kappa+2)|\mathcal{I}_\mathsf{B}| + 2\kappa|\mathcal{I}_\mathsf{A}|$ bits respectively. Therefore the amortized one-way communication is $2\kappa+1$ bits per AND gate. Since we need to call $\mathcal{F}_\mathsf{cpre}$ twice in Π_2PC, we conclude that the amortized one-way (resp. two-way) communication in the ($\mathcal{F}_\mathsf{COT}$, $\mathcal{F}_\mathsf{bCOT}$, $\mathcal{F}_\mathsf{DVZK}$, $\mathcal{F}_\mathsf{EQ}$, $\mathcal{F}_\mathsf{Rand}$)-hybrid model is $2\kappa+5$ (resp. $4\kappa+10$) bits.

For the second version that combines Π_cpre and the optimized WRK online protocol, the amortized one-way (resp. two-way) communication is $2\kappa+3\rho+2$ (resp. $2\kappa+3\rho+4$) bits in the same hybrid model.

Protocol Π_{2PC}, continued

Dual execution and consistency check:

8. Re-using the initialization procedure of functionality $\mathcal{F}_{\mathsf{cpre}}$ (i.e., the same global keys Δ_{A} and Δ_{B} are adopted), $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the preprocessing phase as described above again by swapping the roles (i.e., $\mathsf{P_A}$ is an evaluator and $\mathsf{P_B}$ is a garbler). Thus, for each $w \in \mathcal{W}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ hold $[a'_w]$ and $[b'_w]$. For each wire w, $\mathsf{P_B}$ has also the label $\mathsf{L}'_{w,0}$.
9. Swapping the roles (i.e., $\mathsf{P_A}$ is the evaluator and $\mathsf{P_B}$ is the garbler), $\mathsf{P_A}$ and $\mathsf{P_B}$ execute the online phase as described above again, except for the following differences of processing inputs:
   (a) For each $w \in \mathcal{I}_{\mathsf{B}}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ run $\mathsf{Open}([b_w] \oplus [b'_w] \oplus [r_w]_{\mathsf{B}} \oplus d_w)$ that enables $\mathsf{P_A}$ to obtain the masked value $\Lambda'_w = y_w \oplus b'_w$, and $\mathsf{P_B}$ sends $\mathsf{L}'_{w,\Lambda'_w}$ to $\mathsf{P_A}$.
   (b) For each $w \in \mathcal{I}_{\mathsf{A}}$, both parties set $[\Lambda'_w]_{\mathsf{A}} := [a_w] \oplus [a'_w] \oplus \Lambda_w$, and then garbler $\mathsf{P_B}$ sends $m'_{w,0} := \mathsf{H}(\mathsf{K_B}[\Lambda'_w], w\|2) \oplus \mathsf{L}'_{w,0}$ and $m'_{w,1} := \mathsf{H}(\mathsf{K_B}[\Lambda'_w] \oplus \Delta_{\mathsf{B}}, w\|2) \oplus \mathsf{L}'_{w,1}$ to $\mathsf{P_A}$, who computes $\mathsf{L}'_{w,\Lambda'_w} := m'_{w,\Lambda'_w} \oplus \mathsf{H}(\mathsf{M_A}[\Lambda'_w], w\|2)$.

   After the 2th execution of online phase, $\mathsf{P_A}$ and $\mathsf{P_B}$ obtain $[\Lambda'_w]_{\mathsf{A}}$ for all $w \in \mathcal{W}$.
10. $\mathsf{P_A}$ and $\mathsf{P_B}$ check that $(\Lambda_w \oplus a_w \oplus b_w) \cdot (\Delta_{\mathsf{A}} \oplus \Delta_{\mathsf{B}}) = (\Lambda'_w \oplus a'_w \oplus b'_w) \cdot (\Delta_{\mathsf{A}} \oplus \Delta_{\mathsf{B}})$ holds by performing the following steps.
    (a) For each $w \in \mathcal{W}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ respectively compute
    $$V_w^{\mathsf{A}} = (a_w \oplus a'_w \oplus \Lambda'_w)\Delta_{\mathsf{A}} \oplus \mathsf{M_A}[a_w] \oplus \mathsf{M_A}[a'_w] \oplus \mathsf{M_A}[\Lambda'_w] \oplus \quad \mathsf{K_A}[b_w]$$
    $$\oplus \mathsf{K_A}[b'_w] \oplus \mathsf{K_A}[\Lambda_w],^{\mathsf{B}} = (b_w \oplus b'_w \oplus \Lambda_w)\Delta_{\mathsf{B}}$$
    $$\oplus \mathsf{M_B}[b_w] \oplus \mathsf{M_B}[b'_w] \oplus \mathsf{M_B}[\Lambda_w] \oplus \quad \mathsf{K_B}[a_w] \oplus \mathsf{K_B}[a'_w] \oplus \mathsf{K_B}[\Lambda'_w].$$
    (b) $\mathsf{P_A}$ computes $h := \mathsf{H}'(V_1^{\mathsf{A}}, \ldots, V_t^{\mathsf{A}})$, and then sends it to $\mathsf{P_B}$ who checks that $h = \mathsf{H}'(V_1^{\mathsf{B}}, \ldots, V_t^{\mathsf{B}})$. If the check fails, $\mathsf{P_B}$ aborts.

Output processing: For each $w \in \mathcal{O}$, $\mathsf{P_A}$ and $\mathsf{P_B}$ run $\mathsf{Open}([a_w])$ such that $\mathsf{P_B}$ receives a_w, and then $\mathsf{P_B}$ computes $z_w := \Lambda_w \oplus (a_w \oplus b_w)$.

Fig. 8. Actively secure 2PC protocol in the $\mathcal{F}_{\mathsf{cpre}}$-hybrid model, continued.

5.3 Security Analysis

We first give two useful lemmas about the equality checking (following the proofs of [17,29,36]) refer to the full version [14] for their proofs. We state the security of our 2PC protocol in Theorem 2 and prove it in the full version [14].

Lemma 8. *After the equality check, except with probability $\frac{2+\mathsf{poly}(\kappa)}{2^\kappa}$, $\mathsf{P_B}$ either aborts or evaluates the garbled circuit exactly according to $\mathcal{C}(\boldsymbol{x}, \boldsymbol{y})$, where we canonically define the circuit input $\boldsymbol{x}, \boldsymbol{y}$ using the messages in step 4, step 6, and the randomness from the preprocessing phase.*

Lemma 9. *For the DILO-WRK and KRRW distributed garbling schemes (see details in the full version [14].) by sampling the wire masks $\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{b}, \boldsymbol{b}'$ using the compressed preprocessing functionality $\mathcal{F}_{\mathsf{cpre}}$ (recall that $\boldsymbol{b} := \mathbf{M} \cdot \boldsymbol{b}^*, \boldsymbol{a}' := \mathbf{M} \cdot (\boldsymbol{a}^*)'$ are compressed randomness), the resulting schemes have $2^{-\rho}$-selective failure resilience.*

Theorem 2. *Protocol Π_{2PC} shown in Fig. 7 and Fig. 8 securely realizes functionality $\mathcal{F}_{\mathsf{2PC}}$ in the presence of malicious adversary in the $\mathcal{F}_{\mathsf{cpre}}$-hybrid model and the random oracle model.*

Acknowledgements. Kang Yang is supported by the National Key Research and Development Program of China (Grant No. 2022YFB2702000), and by the National Natural Science Foundation of China (Grant Nos. 62102037, 61932019, 62022018). Yu Yu is supported by the National Natural Science Foundation of China (Grant Nos. 62125204 and 92270201), the National Key Research and Development Program of China (Grant No. 2018YFA0704701), and the Major Program of Guangdong Basic and Applied Research (Grant No. 2019B030302008). Yu Yu also acknowledges the support from the XPLORER PRIZE. Xiao Wang is supported by DARPA under Contract No. HR001120C0087, NSF award #2016240, #2236819, and research awards from Meta and Google. The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government. We thanks anonymous reviewers for their helpful comments.

References

1. Abascal, J., Sereshgi, M.H.F., Hazay, C., Ishai, Y., Venkitasubramaniam, M.: Is the classical GMW paradigm practical? the case of non-interactive actively secure 2PC. In: ACM Conference on Computer and Communications Security (CCS) 2020, pp. 1591–1605. ACM Press (2020). https://doi.org/10.1145/3372297.3423366
2. Baum, C., Braun, L., Munch-Hansen, A., Razet, B., Scholl, P.: Appenzeller to brie: efficient zero-knowledge proofs for mixed-mode arithmetic and Z2k. In: ACM Conference on Computer and Communications Security (CCS) 2021, pp. 192–211. ACM Press (2021). https://doi.org/10.1145/3460120.3484812
3. Baum, C., Braun, L., Munch-Hansen, A., Scholl, P.: Moz$\mathbb{Z}_{2^k}$arella: efficient vector-OLE and zero-knowledge proofs over $\mathbb{Z}_{2^k}$. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part IV. LNCS, vol. 13510, pp. 329–358. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15985-5_12
4. Baum, C., Malozemoff, A.J., Rosen, M.B., Scholl, P.: Mac'n'Cheese: zero-knowledge proofs for Boolean and arithmetic circuits with nested disjunctions. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part IV. LNCS, vol. 12828, pp. 92–122. Springer, Cham (2021)
5. Beaver, D., Micali, S., Rogaway, P.: The round complexity of secure protocols (extended abstract). In: 22nd Annual ACM Symposium on Theory of Computing (STOC), pp. 503–513. ACM Press (1990). https://doi.org/10.1145/100216.100287
6. Bellare, M., Hoang, V.T., Keelveedhi, S., Rogaway, P.: Efficient garbling from a fixed-key blockcipher. In: IEEE Symposium on Security and Privacy (S&P) 2013, pp. 478–492 (2013). https://doi.org/10.1109/SP.2013.39
7. Bendlin, R., Damgård, I., Orlandi, C., Zakarias, S.: Semi-homomorphic encryption and multiparty computation. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 169–188. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_11
8. Blum, A., Furst, M., Kearns, M., Lipton, R.J.: Cryptographic primitives based on hard learning problems. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 278–291. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_24

9. Boyle, E., et al.: Correlated pseudorandomness from expand-accumulate codes. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part II. LNCS, vol. 13508, pp. 603–633. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15979-4_21
10. Boyle, E., et al.: Efficient two-round OT extension and silent non-interactive secure computation. In: ACM Conference on Computer and Communications Security (CCS) 2019, pp. 291–308. ACM Press (2019). https://doi.org/10.1145/3319535.3354255
11. Boyle, E., Couteau, G., Gilboa, N., Ishai, Y., Kohl, L., Scholl, P.: Efficient pseudorandom correlation generators: silent OT extension and more. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part III. LNCS, vol. 11694, pp. 489–518. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26954-8_16
12. Canetti, R.: Security and composition of multiparty cryptographic protocols. J. Cryptology **13**(1), 143–202 (2000). https://doi.org/10.1007/s001459910006
13. Couteau, G., Rindal, P., Raghuraman, S.: Silver: silent VOLE and oblivious transfer from hardness of decoding structured LDPC codes. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part III. LNCS, vol. 12827, pp. 502–534. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84252-9_17
14. Cui, H., Wang, X., Yang, K., Yu, Y.: Actively Secure Half-Gates with Minimum Overhead under Duplex Networks. Cryptology ePrint Archive, Paper 2023/278 (2023). https://eprint.iacr.org/2023/278
15. Damgård, I., Nielsen, J.B., Nielsen, M., Ranellucci, S.: The TinyTable protocol for 2-party secure computation, or: gate-scrambling revisited. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part I. LNCS, vol. 10401, pp. 167–187. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_6
16. Dittmer, S., Ishai, Y., Lu, S., Ostrovsky, R.: Authenticated garbling from simple correlations. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part IV. LNCS, vol. 13510, pp. 57–87. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15985-5_3
17. Dittmer, S., Ishai, Y., Lu, S., Ostrovsky, R.: Improving line-point zero knowledge: two multiplications for the price of one. In: ACM Conference on Computer and Communications Security (CCS) 2022, pp. 829–841. ACM Press (2022). https://doi.org/10.1145/3548606.3559385
18. Dittmer, S., Ishai, Y., Ostrovsky, R.: Line-point zero knowledge and its applications. In: 2nd Conference on Information-Theoretic Cryptography (2021)
19. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
20. Goldreich, O.: Foundations of Cryptography: Basic Applications, vol. 2. Cambridge University Press, Cambridge, UK (2004)
21. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: 19th Annual ACM Symposium on Theory of Computing (STOC), pp. 218–229. ACM Press (1987). https://doi.org/10.1145/28395.28420
22. Guo, C., Katz, J., Wang, X., Weng, C., Yu, Yu.: Better Concrete security for half-gates garbling (in the multi-instance setting). In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part II. LNCS, vol. 12171, pp. 793–822. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-56880-1_28
23. Guo, C., Katz, J., Wang, X., Yu, Y.: Efficient and secure multiparty computation from fixed-key block ciphers. In: IEEE Symposium on Security and Privacy (S&P) 2020, pp. 825–841 (2020). https://doi.org/10.1109/SP40000.2020.00016

24. Hazay, C., Ishai, Y., Venkitasubramaniam, M.: Actively secure garbled circuits with constant communication overhead in the plain model. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10678, pp. 3–39. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70503-3_1
25. Hazay, C., Scholl, P., Soria-Vazquez, E.: Low cost constant round MPC combining BMR and oblivious transfer. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 598–628. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_21
26. Hazay, C., Scholl, P., Soria-Vazquez, E.: Low cost constant round MPC combining BMR and oblivious transfer. J. Cryptology **33**(4), 1732–1786 (2020). https://doi.org/10.1007/s00145-020-09355-y
27. Hazay, C., Shelat, A., Venkitasubramaniam, M.: Going beyond dual execution: MPC for functions with efficient verification. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 328–356. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45388-6_12
28. Huang, Y., Katz, J., Evans, D.: Quid-Pro-Quo-tocols: strengthening semi-honest protocols with dual execution. In: IEEE Symposium on Security and Privacy (S&P) 2012, pp. 272–284 (2012). https://doi.org/10.1109/SP.2012.43
29. Katz, J., Ranellucci, S., Rosulek, M., Wang, X.: Optimizing authenticated garbling for faster secure two-party computation. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part III. LNCS, vol. 10993, pp. 365–391. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96878-0_13
30. Kolesnikov, V., Schneider, T.: Improved garbled circuit: free XOR gates and applications. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008. LNCS, vol. 5126, pp. 486–498. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-70583-3_40
31. Lindell, Y., Pinkas, B., Smart, N.P., Yanai, A.: Efficient constant round multi-party computation combining BMR and SPDZ. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 319–338. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_16
32. Lindell, Y., Smart, N.P., Soria-Vazquez, E.: More efficient constant-round multi-party computation from BMR and SHE. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9985, pp. 554–581. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53641-4_21
33. Mohassel, P., Franklin, M.: Efficiency tradeoffs for malicious two-party computation. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 458–473. Springer, Heidelberg (2006). https://doi.org/10.1007/11745853_30
34. Nielsen, J.B., Nordholt, P.S., Orlandi, C., Burra, S.S.: A new approach to practical active-secure two-party computation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 681–700. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_40
35. Rosulek, M., Roy, L.: Three halves make a whole? beating the half-gates lower bound for garbled circuits. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part I. LNCS, vol. 12825, pp. 94–124. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-84242-0_5
36. Wang, X., Ranellucci, S., Katz, J.: Authenticated garbling and efficient maliciously secure two-party computation. In: ACM Conference on Computer and Communications Security (CCS) 2017, pp. 21–37. ACM Press (2017). https://doi.org/10.1145/3133956.3134053

37. Wang, X., Ranellucci, S., Katz, J.: Global-scale secure multiparty computation. In: ACM Conference on Computer and Communications Security (CCS) 2017, pp. 39–56. ACM Press (2017). https://doi.org/10.1145/3133956.3133979
38. Weng, C., Yang, K., Katz, J., Wang, X.: Wolverine: fast, scalable, and communication-efficient zero-knowledge proofs for Boolean and arithmetic circuits. In: IEEE Symposium on Security and Privacy (S&P) 2021, pp. 1074–1091 (2021). https://doi.org/10.1109/SP40001.2021.00056
39. Weng, C., Yang, K., Xie, X., Katz, J., Wang, X.: Mystique: efficient conversions for zero-knowledge proofs with applications to machine learning. In: USENIX Security Symposium 2021, pp. 501–518. USENIX Association (2021)
40. Weng, C., Yang, K., Yang, Z., Xie, X., Wang, X.: AntMan: interactive zero-knowledge proofs with sublinear communication. In: ACM Conference on Computer and Communications Security (CCS) 2022, pp. 2901–2914. ACM Press (2022). https://doi.org/10.1145/3548606.3560667
41. Yang, K., Sarkar, P., Weng, C., Wang, X.: QuickSilver: efficient and affordable zero-knowledge proofs for circuits and polynomials over any field. In: ACM Conference on Computer and Communications Security (CCS) 2021, pp. 2986–3001. ACM Press (2021). https://doi.org/10.1145/3460120.3484556
42. Yang, K., Wang, X., Zhang, J.: More efficient MPC from improved triple generation and authenticated garbling. In: ACM Conference on Computer and Communications Security (CCS) 2020, pp. 1627–1646. ACM Press (2020). https://doi.org/10.1145/3372297.3417285
43. Yang, K., Weng, C., Lan, X., Zhang, J., Wang, X.: Ferret: fast extension for correlated OT with small communication. In: ACM Conference on Computer and Communications Security (CCS) 2020, pp. 1607–1626. ACM Press (2020). https://doi.org/10.1145/3372297.3417276
44. Yao, A.C.C.: How to generate and exchange secrets (extended abstract). In: 27th Annual Symposium on Foundations of Computer Science (FOCS), pp. 162–167. IEEE (1986). https://doi.org/10.1109/SFCS.1986.25
45. Zahur, S., Rosulek, M., Evans, D.: Two halves make a whole. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 220–250. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_8