

IPDL Case Studies

Kristina Sojakova

Mihai Codescu

Joshua Gancher

June 13, 2023

Abstract

We present here the full proofs of our IPDL case studies: Authenticated-To-Secure Channel in Section 3; Diffie-Hellman Key Exchange (DHKE) in Section 4; DHKE + One-Time Pad in 5; Oblivious Transfer: 1-Out-Of-2 Pre-Processing in Section 6; Multi-Party Coin Toss in Section 7; and Two-Party GMW Protocol in Section 8.

Acknowledgement

This project was funded through the NGI Assure Fund, a fund established by NLnet with financial support from the European Commission's Next Generation Internet programme, under the aegis of DG Communications Networks, Content and Technology under grant agreement No. 957073.

1 Symmetric-Key Encryption: CPA Security

Semantic security, also known as *security against chosen-plaintext attacks (CPA)*, for a symmetric-key encryption schema states that encoding q fixed messages with a secret key is computationally indistinguishable from encoding any other q messages. Or equivalently, encoding q fixed messages with a secret key is computationally indistinguishable from encoding the same message q times. We now show this equivalence in IPDL.

Formally, we assume types $\text{key}, \text{msg}, \text{ctxt}$ of keys, messages, and ciphertexts, respectively; a chosen message $\text{zeros} : 1 \rightarrow \text{msg}$; a probabilistic key generation algorithm $\text{gen}_{\text{key}} : 1 \rightarrow \text{key}$; and a probabilistic encryption algorithm $\text{enc} : \text{msg} \times \text{key} \rightarrow \text{ctxt}$ that takes a message and a key, and returns a ciphertext. We will write $\text{enc}(m, k)$ in place of $\text{enc}(m, k)$.

We can express the standard (*left-right*) version of the CPA cryptographic assumption as the following protocol-level axiom: in the channel context $\{\text{Msg}_L(i) : \text{msg}\}_i, \{\text{Msg}_R(i) : \text{msg}\}_i, \text{Key} : \text{key}, \{\text{Enc}(i) : \text{ctxt}\}_i$ where $i := 1, \dots, q$, the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(\textcolor{red}{m}_L, k)$ for $0 \leq i < q$

with inputs $\text{Msg}_L(-), \text{Msg}_R(-)$, outputs $\text{Enc}(-)$, and an internal channel Key rewrites approximately to the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(\textcolor{red}{m}_R, k)$ for $0 \leq i < q$

The *chosen-message* version of CPA security is another protocol-level axiom: in the channel context $\{\text{Msg}(i) : \text{msg}\}_i, \text{Key} : \text{key}, \{\text{Enc}(i) : \text{ctxt}\}_i$ where $i := 1, \dots, q$, the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(\textcolor{red}{m}, k)$ for $0 \leq i < q$

with inputs $\text{Msg}(-)$, outputs $\text{Enc}(-)$, and an internal channel Key rewrites approximately to the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(\textcolor{red}{\text{zeros}}, k)$ for $0 \leq i < q$

To prove that these are equivalent, assume first the *left-right* version of CPA security. The protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

can be factored as the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(m_L, k) \text{ for } 0 \leq i < q$

(the left-hand side of our CPA assumption) and the protocol

- $\text{Msg}_L(i) := \text{read Msg}(i) \text{ for } 0 \leq i < q$
- $\text{Msg}_R(i) := \text{ret zeros for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}_L(-)$, $\text{Msg}_R(-)$.

Applying the CPA assumption yields the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(m_R, k) \text{ for } 0 \leq i < q$

and the (unchanged) protocol

- $\text{Msg}_L(i) := \text{read Msg}(i) \text{ for } 0 \leq i < q$
- $\text{Msg}_R(i) := \text{ret zeros for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}_L(-)$, $\text{Msg}_R(-)$.

Reversing the factorization process yields the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$

as desired.

For the other direction, assume the *chosen-message* version of CPA security. The protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(m_L, k) \text{ for } 0 \leq i < q$

can be factored as the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

(the left-hand side of our CPA assumption) and the protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_L \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Applying the CPA assumption yields the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$

and the (unchanged) protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_L \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Substituting the channels $\text{Msg}(-)$ away yields the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$

The above can be factored as the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$

(the right-hand side of our CPA assumption) and the protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_R \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Applying the CPA assumption again (this time from right to left) yields the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

and the (unchanged) protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_R \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Reversing the factorization process yields the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(m_R, k) \text{ for } 0 \leq i < q$

as desired.

2 Symmetric-Key Encryption: CPA\$-To-CPA Security

Many CPA-secure encryption schemas also satisfy the stronger property of having *pseudo-random ciphertexts in the presence of chosen-plaintext attacks (CPA\$)*. This latter notion states that encoding q fixed messages with a secret key is computationally indistinguishable from generating q random ciphertexts. We now show that CPA\$ security implies CPA security in IPDL.

Formally, we assume types $\text{key}, \text{msg}, \text{ctxt}$ of keys, messages, and ciphertexts, respectively; a chosen message $\text{zeros} : 1 \rightarrow \text{msg}$; a uniform distribution $\text{unif}_{\text{ctxt}} : 1 \twoheadrightarrow \text{ctxt}$ on ciphertexts; a probabilistic key generation algorithm $\text{gen}_{\text{key}} : 1 \twoheadrightarrow \text{key}$; and a probabilistic encryption algorithm $\text{enc} : \text{msg} \times \text{key} \twoheadrightarrow \text{ctxt}$ that takes a message and a key, and returns a ciphertext. We will write $\text{enc}(m, k)$ in place of $\text{enc}(m, k)$.

We can express the CPA\$ cryptographic assumption as the following protocol-level axiom: in the channel context $\{\text{Msg}(i) : \text{msg}\}_i, \text{Key} : \text{key}, \{\text{Enc}(i) : \text{ctxt}\}_i$ where $i := 1, \dots, q$, the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

with inputs $\text{Msg}(-)$, outputs $\text{Enc}(-)$, and an internal channel Key rewrites approximately to the protocol

- $\text{Enc}(i) := m \leftarrow \text{Msg}; \text{samp unif}_{\text{ctxt}} \text{ for } 0 \leq i < q$

We now show that the above axiom implies CPA security. The protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$

- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(m_L, k) \text{ for } 0 \leq i < q$

can be factored as the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

(the left-hand side of the CPA\$ assumption) and the protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_L \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Applying the CPA\$ assumption yields the composition of the protocol

- $\text{Enc}(i) := m \leftarrow \text{Msg}; \text{samp unif}_{\text{ctxt}} \text{ for } 0 \leq i < q$

and the (unchanged) protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_L \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Substituting the channels $\text{Msg}(-)$ away yields the protocol

- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{samp unif}_{\text{ctxt}} \text{ for } 0 \leq i < q$

The above can be factored as the composition of the protocol

- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); \text{samp unif}_{\text{ctxt}} \text{ for } 0 \leq i < q$

(the right-hand side of the CPA\$ assumption) and the protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_R \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Applying the CPA\$ assumption again (this time from right to left) yields the composition of the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{Msg}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

and the (unchanged) protocol

- $\text{Msg}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); \text{ret } m_R \text{ for } 0 \leq i < q$

followed by the hiding of the channels $\text{Msg}(-)$.

Reversing the factorization process yields the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m_L \leftarrow \text{Msg}_L(i); m_R \leftarrow \text{Msg}_R(i); k \leftarrow \text{Key}; \text{samp enc}(m_R, k) \text{ for } 0 \leq i < q$

as desired.

3 Symmetric-Key Encryption: Authenticated-To-Secure Channel

Alice wants to communicate q messages to Bob using an authenticated channel. The authenticated channel is not secure: it leaks each message to Eve, and waits to receive an ok message back from her before delivering the in-flight message. Thus, Eve cannot modify any of the messages but can read and delay them for any amount of time. To transmit information securely, Alice sends encryptions of her messages, which Bob decrypts using a shared key not known to Eve.

Formally, we assume types $\text{key}, \text{msg}, \text{ctxt}$ of keys, messages, and ciphertexts, respectively; a chosen message zeros $: 1 \rightarrow \text{msg}$; a probabilistic key generation algorithm $\text{gen}_{\text{key}} : 1 \rightarrow \text{key}$; a probabilistic encryption algorithm $\text{enc} : \text{msg} \times \text{key} \rightarrow \text{ctxt}$ that takes a message and a key, and returns a ciphertext; and a decryption algorithm $\text{dec} : \text{ctxt} \times \text{key} \rightarrow \text{msg}$ that takes a ciphertext and a key, and returns a message. We will write $\text{enc}(m, k)$ and $\text{dec}(c, k)$ in place of $\text{enc}(m, k)$ and $\text{dec}(c, k)$.

3.1 The Assumptions

The *correctness* assumption on the encryption schema states that encoding and decoding a single message with the same key yields the original message. We express this as a protocol-level axiom: in the channel context $\text{In} : \text{msg}, \text{Key} : \text{key}, \text{Enc} : \text{ctxt}, \text{Dec} : \text{msg}$ the protocol

- $\text{Enc} := m \leftarrow \text{In}; k \leftarrow \text{Key}; \text{samp enc}(m, k)$
- $\text{Dec} := c \leftarrow \text{Enc}; k \leftarrow \text{Key}; \text{ret dec}(c, k)$

with inputs In , Key and outputs Enc , Dec rewrites strictly to the protocol

- $\text{Enc} := m \leftarrow \text{In}; k \leftarrow \text{Key}; \text{samp enc}(m, k)$
- $\text{Dec} := \text{read In}$

Applying this assumption q times, we get that the protocol

- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k)$ for $0 \leq i < q$
- $\text{Dec}(i) := c \leftarrow \text{Enc}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k)$ for $0 \leq i < q$

rewrites strictly to the protocol

- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k)$ for $0 \leq i < q$
- $\text{Dec}(i) := \text{read In}(i)$ for $0 \leq i < q$

The CPA cryptographic assumption states that if the key is secret, encoding q fixed messages is computationally indistinguishable from encoding the chosen message q times: in the channel context $\{\text{In}(i) : \text{msg}\}_i, \text{Key} : \text{key}, \{\text{Enc}(i) : \text{ctxt}\}_i$ where $i := 1, \dots, q$, the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k)$ for $0 \leq i < q$

with inputs $\text{In}(-)$, outputs $\text{Enc}(-)$, and an internal channel Key rewrites approximately to the protocol

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k)$ for $0 \leq i < q$

3.2 The Ideal Functionality

The ideal functionality reads the input message, leaks a confirmation to Eve to signal that the message has been received, and, upon the approval from Eve, outputs the message:

- $\text{LeakMsgRcvd}(i)_{\text{adv}}^{\text{id}} := m \leftarrow \text{In}(i); \text{ret } \checkmark$ for $0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkMsg}(i)_{\text{id}}^{\text{adv}}; \text{read In}(i)$ for $0 \leq i < q$

3.3 The Real Protocol

The real-world protocol consists of Alice, Bob, the key-generating functionality, and the authenticated channel. The functionality starts by calling the key generation algorithm:

- $\text{Key} := \text{samp gen}_{\text{key}}$

Alice encrypts each input with the provided key, samples a ciphertext from the resulting distribution, and sends it to the authenticated channel:

- $\text{Send}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k)$

The authenticated channel leaks each ciphertext received from Alice to Eve, and, upon receiving the okay from Eve, forwards the ciphertext to Bob:

- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Send}(i)$
- $\text{Recv}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read Send}(i)$

Bob decrypts each ciphertext with the shared key and outputs the result:

- $\text{Out}(i) := c \leftarrow \text{Recv}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k)$

Composing all of this together and hiding the internal communication yields the real-world protocol.

3.4 The Simulator

The simulator turns the adversarial inputs and outputs of the real world protocol into the adversarial inputs and outputs of the ideal functionality, thereby converting any adversary for the real-world protocol into an adversary for the ideal functionality. This means that the channels $\text{LeakMsgRcvd}(-)_{\text{adv}}^{\text{id}}$, $\text{OkCtxt}(-)_{\text{net}}^{\text{adv}}$ are inputs to the simulator and the channels $\text{LeakCtxt}(-)_{\text{adv}}^{\text{net}}$, $\text{OkMsg}(-)_{\text{id}}^{\text{adv}}$ are the outputs. Hence, upon receiving the empty message from the ideal functionality to indicate that a message has been received, the simulator must conjure up a ciphertext to leak to Eve. This is accomplished by generating a key and encrypting the chosen message:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := _ \leftarrow \text{LeakMsgRcvd}(i)_{\text{id}}^{\text{id}}; k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$

Upon receiving the approval from Eve for the generated ciphertext, the simulator gives the approval to the functionality to output the message:

- $\text{OkMsg}(i)_{\text{id}}^{\text{adv}} := \text{read OkCtxt}(i)_{\text{net}}^{\text{adv}} \text{ for } 0 \leq i < q$

Putting this all together yields the following code for the simulator:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := _ \leftarrow \text{LeakMsgRcvd}(i)_{\text{id}}^{\text{id}}; k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$
- $\text{OkMsg}(i)_{\text{id}}^{\text{adv}} := \text{read OkCtxt}(i)_{\text{net}}^{\text{adv}} \text{ for } 0 \leq i < q$

3.5 Real \approx Ideal + Simulator

Composing the simulator with the ideal functionality and hiding the internal communication yields the following:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := _ \leftarrow \text{LeakMsgRcvd}(i)_{\text{id}}^{\text{id}}; k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$
- $\text{OkMsg}(i)_{\text{id}}^{\text{adv}} := \text{read OkCtxt}(i)_{\text{net}}^{\text{adv}} \text{ for } 0 \leq i < q$
- $\text{LeakMsgRcvd}(i)_{\text{adv}}^{\text{id}} := m \leftarrow \text{In}(i); \text{ret } \checkmark \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkMsg}(i)_{\text{id}}^{\text{adv}}; \text{read In}(i) \text{ for } 0 \leq i < q$

The internal channels $\text{LeakMsgRcvd}(-)_{\text{adv}}^{\text{id}}$ and $\text{OkMsg}(-)_{\text{id}}^{\text{adv}}$ that originally served as a line of communication for Eve can now be substituted away:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read In}(i) \text{ for } 0 \leq i < q$

Next we move on to simplifying the real protocol. Explicitly, we have the code below:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Send}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Send}(i) \text{ for } 0 \leq i < q$
- $\text{Recv}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read Send}(i) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := c \leftarrow \text{Recv}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k) \text{ for } 0 \leq i < q$

We first substitute away the internal channels $\text{Recv}(-)$:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Send}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Send}(i) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; c \leftarrow \text{Send}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k) \text{ for } 0 \leq i < q$

Next we conceptually separate the encryption and decryption actions from the message-passing in the real-world by introducing new internal channels $\text{Enc}(-)$ and $\text{Dec}(-)$:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{Send}(i) := \text{read Enc}(i) \text{ for } 0 \leq i < q$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Send}(i) \text{ for } 0 \leq i < q$
- $\text{Dec}(i) := c \leftarrow \text{Send}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read Dec}(i) \text{ for } 0 \leq i < q$

We can now substitute away the internal channels $\text{Send}(-)$ as well:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Enc}(i) \text{ for } 0 \leq i < q$
- $\text{Dec}(i) := c \leftarrow \text{Enc}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read Dec}(i) \text{ for } 0 \leq i < q$

As we observed earlier, the subprotocol

- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{Dec}(i) := c \leftarrow \text{Enc}(i); k \leftarrow \text{Key}; \text{ret dec}(c, k) \text{ for } 0 \leq i < q$

strictly rewrites to the following protocol snippet:

- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{Dec}(i) := \text{read In}(i) \text{ for } 0 \leq i < q$

Our original protocol thus becomes:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Enc}(i) \text{ for } 0 \leq i < q$
- $\text{Dec}(i) := \text{read In}(i) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read Dec}(i) \text{ for } 0 \leq i < q$

Since the channel Key is only used in the channels $\text{Enc}(-)$, we can extract the following subprotocol, where Key is hidden:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(m, k) \text{ for } 0 \leq i < q$

The CPA assumption allows us to approximately rewrite the above protocol snippet to

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$

Plugging this back into the original protocol yields the following:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{Enc}(i) := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := \text{read Enc}(i) \text{ for } 0 \leq i < q$
- $\text{Dec}(i) := \text{read In}(i) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read Dec}(i) \text{ for } 0 \leq i < q$

Finally, we can fold away the internal channels $\text{Enc}(-)$ and $\text{Dec}(-)$:

- $\text{Key} := \text{samp gen}_{\text{key}}$
- $\text{LeakCtxt}(i)_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}(i); k \leftarrow \text{Key}; \text{samp enc}(\text{zeros}, k) \text{ for } 0 \leq i < q$
- $\text{Out}(i) := _ \leftarrow \text{OkCtxt}(i)_{\text{net}}^{\text{adv}}; \text{read In}(i) \text{ for } 0 \leq i < q$

This is precisely the simplified composition of the ideal functionality and the simulator from the beginning of this section.

4 Diffie-Hellman Key Exchange (DHKE)

In symmetric-key encryption, the sender (Alice) and the receiver (Bob) need to agree on a shared secret key. One such key-agreement protocol is the Diffie-Hellman Key Exchange (DHKE), which we now prove secure in IPDL.

Formally, we assume a type key of secret keys (elements of $\{0, \dots, p-1\}$, where p is a prime); a type msg of messages, also serving as public keys (elements of a cyclic group $G = \{g^0, \dots, g^{p-1}\}$); a uniform distribution $\text{unif}_{\text{key}} : 1 \rightarrow \text{key}$ on keys; a uniform distribution $\text{unif}_{\text{msg}} : 1 \rightarrow \text{msg}$ on messages; the generator $\text{g} : 1 \rightarrow \text{msg}$ of G ; and the exponentiation function $\text{exp} : \text{msg} \times \text{key} \rightarrow \text{msg}$ that raises an element of G to the power of $k \in \{0, \dots, p-1\}$. We will write m^k in place of $\text{exp}(m, k)$.

4.1 The Assumptions

At the level of expressions, we only need to know that exponents commute:

- $k : \text{key}, l : \text{key} \vdash (g^l)^k = (g^k)^l : \text{msg}$, and

At the level of distributions, we need to know that sampling a random secret key k from unif_{key} and returning g^k is the same as sampling from unif_{msg} directly (a consequence of unif_{key} being uniform),

- $\cdot \vdash (k \leftarrow \text{unif}_{\text{key}}; \text{ret } g^k) = \text{unif}_{\text{msg}} : \text{msg}$

Finally, at the level of protocols we need the *decisional Diffie-Hellman (DDH)* cryptographic assumption: as long as the secret keys k, l are generated uniformly, even if the adversary knows the values g^k and g^l , they will be unable to distinguish $(g^k)^l$ from a uniformly generated element of G . The corresponding protocol-level axiom states that in the channel context $\text{DDH}_3 : \text{msg} \times (\text{msg} \times \text{msg})$, the single-reaction no-input protocol

- $\text{DDH}_3 := k_A \leftarrow \text{unif}_{\text{key}}; k_B \leftarrow \text{unif}_{\text{key}}; \text{ret } (g^{k_A}, (g^{k_B}, (g^{k_A})^{k_B}))$

rewrites approximately to the protocol

- $\text{DDH}_3 := k_A \leftarrow \text{unif}_{\text{key}}; k_B \leftarrow \text{unif}_{\text{key}}; k_R \leftarrow \text{unif}_{\text{key}}; \text{ret } (g^{k_A}, (g^{k_B}, g^{k_R}))$

4.2 The Ideal Functionality

The ideal functionality for the key exchange generates the shared key randomly, and, upon the approval from the adversary, sends it to the respective party:

- $\text{SharedKey} := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; \text{read } \text{SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{read } \text{SharedKey}$

Here the channel SharedKey is internal.

4.3 The Real Protocol

The real-world protocol consists of Alice, Bob, and two authenticated channels. Alice randomly generates a secret key k_A and sends the value g^{k_A} as her public key to Bob using one of the authenticated channels:

- $\text{SecretKey}(\text{Alice}) := \text{samp } \text{unif}_{\text{key}}$
- $\text{Send}(\text{Alice}, \text{Bob}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$

Symmetrically, Bob generates a secret key k_B and sends the value g^{k_B} to Alice using the second authenticated channel:

- $\text{SecretKey}(\text{Bob}) := \text{samp } \text{unif}_{\text{key}}$
- $\text{Send}(\text{Bob}, \text{Alice}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$

Each authenticated channel leaks the corresponding public key to the adversary and waits for their approval before forwarding the key to the other party:

- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read } \text{Send}(\text{Alice}, \text{Bob})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read } \text{Send}(\text{Bob}, \text{Alice})$
- $\text{Recv}(\text{Alice}, \text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read } \text{Send}(\text{Alice}, \text{Bob})$
- $\text{Recv}(\text{Bob}, \text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read } \text{Send}(\text{Bob}, \text{Alice})$

Upon receiving Bob's public key g^{k_B} , Alice computes the shared key as the value $(g^{k_B})^{k_A}$:

- $\text{Key}(\text{Alice}) := p_B \leftarrow \text{Recv}(\text{Bob}, \text{Alice}); k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } p_B^{k_A}$

Analogously, upon receiving Alice's public key g^{k_A} , Bob computes the shared key as the value $(g^{k_A})^{k_B}$:

- $\text{Key}(\text{Bob}) := p_A \leftarrow \text{Recv}(\text{Alice}, \text{Bob}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } p_A^{k_B}$

Thus, we have the following code for Alice:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{Send}(\text{Alice}, \text{Bob}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{Key}(\text{Alice}) := p_B \leftarrow \text{Recv}(\text{Bob}, \text{Alice}); k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } p_B^{k_A}$

The code for Bob has the symmetric form:

- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{Send}(\text{Bob}, \text{Alice}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{Key}(\text{Bob}) := p_A \leftarrow \text{Recv}(\text{Alice}, \text{Bob}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } p_A^{k_B}$

At last we have the two authenticated channels: from Alice to Bob,

- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read Send}(\text{Alice}, \text{Bob})$
- $\text{Recv}(\text{Alice}, \text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read Send}(\text{Alice}, \text{Bob})$

and from Bob to Alice:

- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read Send}(\text{Bob}, \text{Alice})$
- $\text{Recv}(\text{Bob}, \text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read Send}(\text{Bob}, \text{Alice})$

Composing all of this together and hiding the internal communication yields the Diffie-Hellman Key Exchange protocol.

4.4 The Simulator

The channels $\text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}$ and $\text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}$ are inputs to the simulator, whereas the channels $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}$, $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}$ and $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$, $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$ are the outputs.

The simulator constructs the public keys for Alice and Bob exactly as in the real protocol: it randomly generates the respective secret keys k_A and k_B , and computes the corresponding public keys as g^{k_A} and g^{k_B} . In the real-world Diffie-Hellman Key Exchange, Alice can only construct the shared key once the adversary approves the forwarding of Bob's public key to her. Hence, the ideal functionality is only allowed to forward the shared key to Alice once the approval for Bob's public key clears, and vice versa.

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}} := \text{read OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}$
- $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}} := \text{read OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}$

In the above, the channels $\text{SecretKey}(\text{Alice})$, $\text{SecretKey}(\text{Bob})$ and $\text{PublicKey}(\text{Alice})$, $\text{PublicKey}(\text{Bob})$ are internal.

4.5 Real \approx Ideal + Simulator

Plugging the simulator into the ideal functionality and substituting away the internal channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$, $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$ that originally served as a line of communication for the adversary yields the following:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := \text{samp unif}_{\text{msg}}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$

Next we move on to simplifying the real protocol. Explicitly, we have the code below:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{Send}(\text{Alice}, \text{Bob}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{Send}(\text{Bob}, \text{Alice}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read } \text{Send}(\text{Alice}, \text{Bob})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read } \text{Send}(\text{Bob}, \text{Alice})$
- $\text{Recv}(\text{Alice}, \text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read } \text{Send}(\text{Alice}, \text{Bob})$
- $\text{Recv}(\text{Bob}, \text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read } \text{Send}(\text{Bob}, \text{Alice})$
- $\text{Key}(\text{Alice}) := p_B \leftarrow \text{Recv}(\text{Bob}, \text{Alice}); k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } p_B^{k_A}$
- $\text{Key}(\text{Bob}) := p_A \leftarrow \text{Recv}(\text{Alice}, \text{Bob}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } p_A^{k_B}$

The internal channels $\text{Send}(\text{Alice}, \text{Bob})$, $\text{Send}(\text{Bob}, \text{Alice})$ and $\text{Recv}(\text{Alice}, \text{Bob})$, $\text{Recv}(\text{Bob}, \text{Alice})$ can be substituted away:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; k_B \leftarrow \text{SecretKey}(\text{Bob}); k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } (g^{k_B})^{k_A}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$

Exponents commute by assumption, so we can rewrite the channel $\text{Key}(\text{Alice})$ equivalently as

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$

- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; k_B \leftarrow \text{SecretKey}(\text{Bob}); k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } (g^{k_A})^{k_B}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$

After rearranging, the channels $\text{Key}(\text{Alice})$ and $\text{Key}(\text{Bob})$ construct the exact same shared key:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$

We can extract the key construction into a new internal channel SharedKey :

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

Similarly, we can extract the public key construction for Alice and Bob into new internal channels $\text{PublicKey}(\text{Alice})$ and $\text{PublicKey}(\text{Bob})$:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

Adding a gratuitous dependency on the channel $\text{SecretKey}(\text{Bob})$ into the channel $\text{PublicKey}(\text{Alice})$, and, analogously, on the channel $\text{SecretKey}(\text{Alice})$ into the channel $\text{PublicKey}(\text{Bob})$ yields

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A})^{k_B}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

We can now extract the DDH triple into a new internal channel DDH_3 :

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{DDH}_3 := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } (g^{k_A}, (g^{k_B}, (g^{k_A})^{k_B}))$
- $\text{SharedKey} := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k$
- $\text{PublicKey}(\text{Alice}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_A$
- $\text{PublicKey}(\text{Bob}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_B$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

The internal channels $\text{SecretKey}(\text{Alice})$ and $\text{SecretKey}(\text{Bob})$ are now only used in the channel DDH_3 , so we can fold them in:

- $\text{DDH}_3 := k_A \leftarrow \text{unif}_{\text{key}}; k_B \leftarrow \text{unif}_{\text{key}}; \text{ret } (g^{k_A}, (g^{k_B}, (g^{k_A})^{k_B}))$
- $\text{SharedKey} := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k$
- $\text{PublicKey}(\text{Alice}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_A$
- $\text{PublicKey}(\text{Bob}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_B$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

Using the DDH assumption, we can approximately rewrite the above protocol to

- $\text{DDH}_3 := k_A \leftarrow \text{unif}_{\text{key}}; k_B \leftarrow \text{unif}_{\text{key}}; k_R \leftarrow \text{unif}_{\text{key}}; \text{ret } (g^{k_A}, (g^{k_B}, g^{k_R}))$
- $\text{SharedKey} := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k$

- $\text{PublicKey}(\text{Alice}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_A$
- $\text{PublicKey}(\text{Bob}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_B$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$

Unfolding the three samplings from the channel DDH_3 into new internal channels $\text{SecretKey}(\text{Alice})$, $\text{SecretKey}(\text{Bob})$, Key yields

- $\text{Key} := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{DDH}_3 := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); k_R \leftarrow \text{Key}; \text{ret } (g^{k_A}, (g^{k_B}, g^{k_R}))$
- $\text{SharedKey} := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k$
- $\text{PublicKey}(\text{Alice}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_A$
- $\text{PublicKey}(\text{Bob}) := (k_A, (k_B, k)) \leftarrow \text{DDH}_3; \text{ret } k_B$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$

The internal channel DDH_3 can now be substituted away:

- $\text{Key} := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); k_R \leftarrow \text{Key}; \text{ret } g^{k_R}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); k_R \leftarrow \text{Key}; \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); k_B \leftarrow \text{SecretKey}(\text{Bob}); k_R \leftarrow \text{Key}; \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read } \text{PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read } \text{SharedKey}$

Dropping the gratuitous dependencies – on channels $\text{SecretKey}(\text{Alice})$, $\text{SecretKey}(\text{Bob})$ in the channel SharedKey , on channels $\text{SecretKey}(\text{Bob})$, Key in the channel $\text{PublicKey}(\text{Alice})$, and on channels $\text{SecretKey}(\text{Alice})$, Key in the channel $\text{PublicKey}(\text{Bob})$ – yields the following:

- $\text{Key} := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := k_R \leftarrow \text{Key}; \text{ret } g^{k_R}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

Since the channel Key is now only used in the channel SharedKey , we can fold it in:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := k_R \leftarrow \text{unif}_{\text{key}}; \text{ret } g^{k_R}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

By assumption, sampling a random secret key k_R from unif_{key} and returning g^{k_R} is the same as sampling from unif_{msg} directly, so we can simplify the channel SharedKey as follows:

- $\text{SecretKey}(\text{Alice}) := \text{samp unif}_{\text{key}}$
- $\text{SecretKey}(\text{Bob}) := \text{samp unif}_{\text{key}}$
- $\text{SharedKey} := \text{samp unif}_{\text{msg}}$
- $\text{PublicKey}(\text{Alice}) := k_A \leftarrow \text{SecretKey}(\text{Alice}); \text{ret } g^{k_A}$
- $\text{PublicKey}(\text{Bob}) := k_B \leftarrow \text{SecretKey}(\text{Bob}); \text{ret } g^{k_B}$
- $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Alice})$
- $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}} := \text{read PublicKey}(\text{Bob})$
- $\text{Key}(\text{Alice}) := _ \leftarrow \text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$
- $\text{Key}(\text{Bob}) := _ \leftarrow \text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}; \text{read SharedKey}$

This is precisely the simplified composition of the ideal functionality and the simulator from the beginning of this section.

5 Diffie-Hellman Key Exchange (DHKE) + One-Time Pad (OTP)

We now use the Diffie-Hellman Key Exchange protocol from Section 4 to turn an authenticated channel into a one-time pad that delivers a single secret message from Alice to Bob.

Formally, we assume a type `key` of secret keys (elements of $\{0, \dots, p-1\}$, where p is a prime); a type `msg` of messages, also serving as public keys (elements of a cyclic group $G = \{g^0, \dots, g^{p-1}\}$); a uniform distribution $\text{unif}_{\text{key}} : 1 \rightarrow \text{key}$ on keys; a uniform distribution $\text{unif}_{\text{msg}} : 1 \rightarrow \text{msg}$ on messages; the generator $g : 1 \rightarrow \text{msg}$ of G ; the group multiplication function $\text{mul} : \text{msg} \times \text{msg} \rightarrow \text{msg}$, where we write $m * k$ in place of $\text{mul}(m, k)$; the group inverse function $\text{inv} : \text{msg} \rightarrow \text{msg}$, where we write k^{-1} in place of $\text{inv } k$; and the exponentiation function $\text{exp} : \text{msg} \times \text{key} \rightarrow \text{msg}$ that raises an element of G to the power of $k \in \{0, \dots, p-1\}$. We will write m^k in place of $\text{exp}(m, k)$.

We will structure our proof modularly: in the first step, we establish that the Diffie-Hellman Key Exchange can be replaced with an idealization. In the second step, we prove that the resulting One-Time Pad protocol itself reduces to an idealization.

5.1 The Assumptions

In addition to the assumptions from Section 4, we will need the fact that inverses cancel on the right:

- $m : \text{msg}, k : \text{msg} \vdash (m * k) * k^{-1} = m : \text{msg}$

Additionally, we need to know that the distribution unif_{msg} on messages is invariant under the operation of multiplication with a fixed message (a consequence of unif_{msg} being uniform):

- $m : \text{msg} \vdash (k \leftarrow \text{unif}_{\text{msg}}; \text{ret } m * k) = \text{unif}_{\text{msg}} : \text{msg}$

5.2 The Ideal Functionality

The ideal functionality reads the input message, leaks a confirmation to the adversary to signal that the message has been received, and, upon the approval from the adversary, outputs the message:

- $\text{LeakMsgRcvd}_{\text{adv}}^{\text{id}} := m \leftarrow \text{In}; \text{ret } \checkmark$
- $\text{Out} := _ \leftarrow \text{OkMsg}_{\text{id}}^{\text{adv}}; \text{read In}$

5.3 The Real Protocol

The real-world protocol consists of Alice, Bob, and three authenticated channels: two for carrying out the Diffie-Hellman Key Exchange, as described in Section 4, and one for communicating the secret message from Alice to Bob. The complete code for Alice is the composition of Alice's key exchange part with the single-reaction protocol

- $\text{Send} := m \leftarrow \text{In}; k_A \leftarrow \text{Key}(\text{Alice}); \text{ret } m * k_A$

In the above, Alice encrypts the input message by multiplying it with the shared key produced by the key exchange, and sends the resulting ciphertext to Bob via the third authenticated channel. The complete code for Bob is the composition of Bob's key exchange part with the single-reaction protocol

- $\text{Out} := c \leftarrow \text{Recv}; k_B \leftarrow \text{Key}(\text{Bob}); \text{ret } c * k_B^{-1}$

In the above, Bob decrypts the ciphertext received from Alice by multiplying it with the inverse of the shared key, and outputs the result. For communicating the ciphertext from Alice to Bob through the adversary, we have the third authenticated channel:

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := \text{read Send}$
- $\text{Recv} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; \text{read Send}$

The real protocol is a composition of the two parties and the three authenticated channels, followed by the hiding of the internal communication.

5.4 The Simulator

The inputs to the simulator are channels $\text{OkPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}$, $\text{OkPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}$, $\text{OkCtxt}_{\text{net}}^{\text{adv}}$, $\text{LeakMsgRcvd}_{\text{adv}}^{\text{id}}$, whereas the outputs are channels $\text{LeakPublicKey}(\text{Alice})_{\text{net}}^{\text{adv}}$, $\text{LeakPublicKey}(\text{Bob})_{\text{net}}^{\text{adv}}$, $\text{LeakCtxt}_{\text{adv}}^{\text{net}}$, $\text{OkMsg}_{\text{id}}^{\text{adv}}$. We define the simulator as the composition of the key exchange simulator and the protocol

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := _ \leftarrow \text{LeakMsgRcvd}_{\text{adv}}^{\text{id}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; \text{samp unif}_{\text{msg}}$
- $\text{OkMsg}_{\text{id}}^{\text{adv}} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{ret } \checkmark$

followed by the hiding of the channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$ and $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$.

5.5 Real \approx Ideal + Simulator: One-Time Pad

Plugging the simulator into the ideal functionality and substituting away the internal channels $\text{LeakMsgRcvd}_{\text{adv}}^{\text{id}}$ and $\text{OkMsg}_{\text{id}}^{\text{adv}}$ that originally served as a line of communication for the adversary yields the composition of the key exchange simulator with the protocol

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; \text{samp unif}_{\text{msg}}$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{read In}$

followed by the hiding of the channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$ and $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$.

Next we move on to simplifying the real protocol. The real protocol can be refactored as the composition of the key exchange part and the protocol

- $\text{Send} := m \leftarrow \text{In}; k_A \leftarrow \text{Key}(\text{Alice}); \text{ret } m * k_A$
- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := \text{read Send}$
- $\text{Recv} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; \text{read Send}$
- $\text{Out} := c \leftarrow \text{Recv}; k_B \leftarrow \text{Key}(\text{Bob}); \text{ret } c * k_B^{-1}$

where the channels Send and Recv are internal, followed by the hiding of the channels $\text{Key}(\text{Alice})$ and $\text{Key}(\text{Bob})$.

The channels Send and Recv can be substituted away, turning our protocol into the composition of the key exchange part and the protocol

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; k_A \leftarrow \text{Key}(\text{Alice}); \text{ret } m * k_A$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; m \leftarrow \text{In}; k_A \leftarrow \text{Key}(\text{Alice}); k_B \leftarrow \text{Key}(\text{Bob}); \text{ret } (m * k_A) * k_B^{-1}$

followed by the hiding of the channels $\text{Key}(\text{Alice})$ and $\text{Key}(\text{Bob})$.

We can approximately rewrite the key exchange part as the composition of the key exchange idealization and the key exchange simulator, followed by the hiding of the channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$ and $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$. Thus, we can express the real protocol as the composition of the key exchange idealization, the key exchange simulator, and the protocol

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; k_A \leftarrow \text{Key}(\text{Alice}); \text{ret } m * k_A$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; m \leftarrow \text{In}; k_A \leftarrow \text{Key}(\text{Alice}); k_B \leftarrow \text{Key}(\text{Bob}); \text{ret } (m * k_A) * k_B^{-1}$

all followed by the hiding of the channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$, $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$, and $\text{Key}(\text{Alice})$, $\text{Key}(\text{Bob})$.

Composing the above protocol snippet with the key exchange idealization, and substituting away the internal channels $\text{Key}(\text{Alice})$ and $\text{Key}(\text{Bob})$ that originally served as a line of communication between the key exchange part and the one-time pad yields the protocol

- $\text{SharedKey} := \text{samp unif}_{\text{msg}}$
- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; k \leftarrow \text{SharedKey}; \text{ret } m * k$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; k \leftarrow \text{SharedKey}; \text{ret } (m * k) * k^{-1}$

where the channel `SharedKey` is internal. Canceling out k with its inverse in the channel `Out` yields

- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; k \leftarrow \text{SharedKey}; \text{ret } m$

Dropping the gratuitous dependency on the channel `SharedKey` yields

- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{ret } m$

which simplifies to

- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{read In}$

Summarizing, the cleaned-up version of the real protocol is the composition of the the key exchange simulator and the protocol

- $\text{SharedKey} := \text{samp unif}_{\text{msg}}$
- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; k \leftarrow \text{SharedKey}; \text{ret } m * k$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{read In}$

where the channel `SharedKey` is internal, followed by the hiding of the channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$ and $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$. Since the channel `SharedKey` is now only used in the channel $\text{LeakCtxt}_{\text{adv}}^{\text{net}}$, we can fold it in:

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; k \leftarrow \text{unif}_{\text{msg}}; \text{ret } m * k$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{read In}$

By assumption, the distribution unif_{msg} on messages is invariant under the operation of multiplication with a fixed message, so we can simplify the channel $\text{LeakCtxt}_{\text{adv}}^{\text{net}}$ as follows:

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; \text{samp unif}_{\text{msg}}$

Thus, the final version of the real protocol is the composition of the key exchange simulator and the protocol

- $\text{LeakCtxt}_{\text{adv}}^{\text{net}} := m \leftarrow \text{In}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; \text{samp unif}_{\text{msg}}$
- $\text{Out} := _ \leftarrow \text{OkCtxt}_{\text{net}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}; _ \leftarrow \text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}; \text{read In}$

followed by the hiding of the channels $\text{OkKey}(\text{Alice})_{\text{id}}^{\text{adv}}$ and $\text{OkKey}(\text{Bob})_{\text{id}}^{\text{adv}}$. But this is precisely the simplified composition of the ideal functionality and the simulator from the beginning of this section.

6 Oblivious Transfer: 1-Out-Of-2 Pre-Processing

In this case study, Alice and Bob carry out a 1-Out-Of-2 Oblivious Transfer (OT) separated into an *offline* phase, where Alice and Bob exchange a key using a single idealized 1-Out-Of-2 OT instance, and an *online* phase that relies on the shared key and requires no cryptographic assumptions at all, thereby being very fast. We prove the protocol semi-honest secure in the case when the receiver is corrupt. Formally, we assume a type `msg` of messages; a coin-flip distribution $\text{flip} : 1 \rightarrow \text{Bool}$; a uniform distribution $\text{unif}_{\text{msg}} : 1 \rightarrow \text{msg}$ on messages; and a bitwise xor function $\oplus_{\text{msg}} : \text{msg} \times \text{msg} \rightarrow \text{msg}$ on messages. We will write $\oplus(x, y)$ as $x \oplus y$.

6.1 The Assumptions

At the expression level, we assume that the operation of bitwise xor with a fixed message is self-inverse:

- $x : \text{msg}, y : \text{msg} \vdash (x \oplus y) \oplus y = x : \text{msg}.$

At the distribution level, we assume that the distribution unif_{msg} on messages is invariant under the operation of xor-ing with a fixed message (a consequence of unif_{msg} being uniform):

- $x : \text{msg} \vdash (y \leftarrow \text{unif}_{\text{msg}}; \text{ret } x \oplus y) = \text{unif}_{\text{msg}} : \text{msg}.$

6.2 The Ideal Functionality

In its basic form, the ideal functionality reads two messages m_0, m_1 from the sender, and one Boolean c from the receiver, and outputs the following message:

$$\begin{cases} m_0 & \text{if } c = \text{false} \\ m_1 & \text{if } c = \text{true} \end{cases}$$

In code:

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{if } c \text{ then ret } m_1 \text{ else ret } m_0$

Since the sender is honest, only the timing information for their messages is leaked:

- $\text{MsgRcvd}(0)_{\text{adv}}^{\text{id}} := m_0 \leftarrow \text{Msg}(0); \text{ret } \checkmark$
- $\text{MsgRcvd}(1)_{\text{adv}}^{\text{id}} := m_1 \leftarrow \text{Msg}(1); \text{ret } \checkmark$

Since the receiver is semi-honest, the choice as well as selected message are leaked to the adversary:

- $\text{Choice}_{\text{adv}}^{\text{id}} := \text{read Choice}$
- $\text{Out}_{\text{adv}}^{\text{id}} := \text{read Out}$

6.3 The Real Protocol

For the offline phase, we assume an ideal OT functionality. Alice randomly generates a new pair of messages, to be treated as keys, and sends them to the OT functionality:

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$
- $\text{OTMsg}(0) := \text{read Key}(0)$
- $\text{OTMsg}(1) := \text{read Key}(1)$

Bob flips a coin to decide which key he will ask for and informs the adversary:

- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$

He subsequently sends his choice to the OT functionality:

- $\text{OTChoice} := \text{read Flip}$

The OT functionality selects the corresponding key and sends it to Bob, accompanied by the requisite leakages:

- $\text{OTOut} := m_0 \leftarrow \text{OTMsg}(0); m_1 \leftarrow \text{OTMsg}(1); c \leftarrow \text{OTChoice}; \text{if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := m_0 \leftarrow \text{OTMsg}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := m_1 \leftarrow \text{OTMsg}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read OTChoice}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read OTOut}$

Bob stores the result of the OT exchange as the key shared between him and Alice:

- $\text{SharedKey} := \text{read OTOut}$

This ends the offline phase. The online phase starts by Bob's informing the adversary about his choice of message:

- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$

Bob subsequently encrypts this choice by xor-ing it with the shared key established in the pre-processing phase, and sends the encryption to Alice while leaking its value:

- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$

Upon receiving Bob's encrypted choice, Alice encrypts her messages by bitwise xor-ing them with the keys - either their own respective keys in case Bob's encrypted choice is false, or the mutually-swapped keys if Bob's encrypted choice is true:

- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc};$
if e then ret $m_0 \oplus k_1$ else ret $m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc};$
if e then ret $m_1 \oplus k_0$ else ret $m_1 \oplus k_1$

After receiving Alice's encrypted messages, Bob leaks them to the adversary:

- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$

He then selects the encryption of the message he wants, decrypts it by xor-ing it with the shared key, and outputs the result while leaking its value:

- $\text{Out} := e_0 \leftarrow \text{MsgEnc}(0); e_1 \leftarrow \text{MsgEnc}(1); k \leftarrow \text{SharedKey}; c \leftarrow \text{Choice}; \text{if } c \text{ then ret } e_1 \oplus k \text{ else ret } e_0 \oplus k$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}$

Thus, we have the following code for Alice:

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$
- $\text{OTMsg}(0) := \text{read Key}(0)$
- $\text{OTMsg}(1) := \text{read Key}(1)$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc};$
if e then ret $m_0 \oplus k_1$ else ret $m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc};$
if e then ret $m_1 \oplus k_0$ else ret $m_1 \oplus k_1$

The code for Bob has the following form:

- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTChoice} := \text{read Flip}$
- $\text{SharedKey} := \text{read OTOut}$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$

- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(1)$
- $\text{Out} := e_0 \leftarrow \text{MsgEnc}(0); e_1 \leftarrow \text{MsgEnc}(1); k \leftarrow \text{SharedKey}; c \leftarrow \text{Choice}; \text{if } c \text{ then ret } e_1 \oplus k \text{ else ret } e_0 \oplus k$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read } \text{Out}$

Finally, we recall the code for the OT functionality:

- $\text{OTOut} := m_0 \leftarrow \text{OTMsg}(0); m_1 \leftarrow \text{OTMsg}(1); c \leftarrow \text{OTChoice}; \text{if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := m_0 \leftarrow \text{OTMsg}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := m_1 \leftarrow \text{OTMsg}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read } \text{OTChoice}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read } \text{OTOut}$

Composing all of this together and hiding the internal communication yields the real-world protocol.

6.4 Real = Ideal + Simulator

Our goal is to simplify the real protocol until it becomes clear how to separate it out into the ideal functionality part and the simulator part. We recall the code:

- $\text{Key}(0) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Flip} := \text{samp } \text{flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read } \text{Flip}$
- $\text{OTMsg}(0) := \text{read } \text{Key}(0)$
- $\text{OTMsg}(1) := \text{read } \text{Key}(1)$
- $\text{OTChoice} := \text{read } \text{Flip}$
- $\text{OTOut} := m_0 \leftarrow \text{OTMsg}(0); m_1 \leftarrow \text{OTMsg}(1); c \leftarrow \text{OTChoice}; \text{if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := m_0 \leftarrow \text{OTMsg}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := m_1 \leftarrow \text{OTMsg}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read } \text{OTChoice}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read } \text{OTOut}$
- $\text{SharedKey} := \text{read } \text{OTOut}$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read } \text{Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then (if } c \text{ then false else true) else (if } c \text{ then true else false)}$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read } \text{ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc}; \text{if } e \text{ then ret } m_0 \oplus k_1 \text{ else ret } m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc}; \text{if } e \text{ then ret } m_1 \oplus k_0 \text{ else ret } m_1 \oplus k_1$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(0)$

- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(1)$
- $\text{Out} := e_0 \leftarrow \text{MsgEnc}(0); e_1 \leftarrow \text{MsgEnc}(1); k \leftarrow \text{SharedKey}; c \leftarrow \text{Choice}; \text{if } c \text{ then ret } e_1 \oplus k \text{ else ret } e_0 \oplus k$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read } \text{Out}$

We start by eliminating the internal OT channels by substituting them into the OT leakage channels and the channel SharedKey :

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$
- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read } \text{Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read } \text{Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read } \text{SharedKey}$
- $\text{SharedKey} := k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; \text{if } f \text{ then ret } k_1 \text{ else ret } k_0$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read } \text{Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then (if } c \text{ then false else true) else (if } c \text{ then true else false)}$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read } \text{ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc};$
if e then ret $m_0 \oplus k_1$ else ret $m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); e \leftarrow \text{ChoiceEnc};$
if e then ret $m_1 \oplus k_0$ else ret $m_1 \oplus k_1$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(1)$
- $\text{Out} := e_0 \leftarrow \text{MsgEnc}(0); e_1 \leftarrow \text{MsgEnc}(1); k \leftarrow \text{SharedKey}; c \leftarrow \text{Choice}; \text{if } c \text{ then ret } e_1 \oplus k \text{ else ret } e_0 \oplus k$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read } \text{Out}$

Substituting the channel ChoiceEnc into $\text{MsgEnc}(0)$ and $\text{MsgEnc}(1)$ yields

- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then ret $m_0 \oplus k_0$ else ret $m_0 \oplus k_1$) else (if c then ret $m_0 \oplus k_1$ else ret $m_0 \oplus k_0$)
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then ret $m_1 \oplus k_1$ else ret $m_1 \oplus k_0$) else (if c then ret $m_1 \oplus k_0$ else ret $m_1 \oplus k_1$)

Substituting the channel SharedKey into Out yields

- $\text{Out} := e_0 \leftarrow \text{MsgEnc}(0); e_1 \leftarrow \text{MsgEnc}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then ret $e_1 \oplus k_1$ else ret $e_0 \oplus k_1$) else (if c then ret $e_1 \oplus k_0$ else ret $e_0 \oplus k_0$)

Further substituting the channels $\text{MsgEnc}(0)$ and $\text{MsgEnc}(1)$ into Out yields

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then $\text{ret } (m_1 \oplus k_1) \oplus k_1$ else $\text{ret } (m_0 \oplus k_1) \oplus k_1$)
else (if c then $\text{ret } (m_1 \oplus k_0) \oplus k_0$ else $\text{ret } (m_0 \oplus k_0) \oplus k_0$)

We can now cancel out the two applications of \oplus since they are mutually inverse by assumption:

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then $\text{ret } m_1$ else $\text{ret } m_0$) else (if c then $\text{ret } m_1$ else $\text{ret } m_0$)

We can now drop the gratuitous dependencies on channels $\text{Key}(0)$, $\text{Key}(1)$:

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then $\text{ret } m_1$ else $\text{ret } m_0$) else (if c then $\text{ret } m_1$ else $\text{ret } m_0$)

Since both branches are the same, we can also not flip:

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$ if c then $\text{ret } m_1$ else $\text{ret } m_0$

After dropping the gratuitous dependency on the channel Flip , we get

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice};$ if c then $\text{ret } m_1$ else $\text{ret } m_0$

Summarizing, the cleaned-up version of the real protocol is below:

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$
- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read SharedKey}$
- $\text{SharedKey} := k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip};$ if f then $\text{ret } k_1$ else $\text{ret } k_0$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$ if f then (if c then false else true) else (if c then true else false)
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then $\text{ret } m_0 \oplus k_0$ else $\text{ret } m_0 \oplus k_1$) else (if c then $\text{ret } m_0 \oplus k_1$ else $\text{ret } m_0 \oplus k_0$)
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$
if f then (if c then $\text{ret } m_1 \oplus k_1$ else $\text{ret } m_1 \oplus k_0$) else (if c then $\text{ret } m_1 \oplus k_0$ else $\text{ret } m_1 \oplus k_1$)
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice};$ if c then $\text{ret } m_1$ else $\text{ret } m_0$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}$

Since both keys are generated from the same distribution, the coin flip that distinguishes between them can be eliminated (“*decoupling*”). To show this, we introduce an internal channel `KeyPair` that constructs the pair of two keys, where the first one is shared and the second one is private:

- `Key(0) := samp unifmsg`
- `Key(1) := samp unifmsg`
- `Flip := samp flip`
- `Flipadvrec := read Flip`
- `OTMsgRcvd(0)advot := k0 ← Key(0); ret ✓`
- `OTMsgRcvd(1)advot := k1 ← Key(1); ret ✓`
- `OTChoiceadvot := read Flip`
- `OTOutadvot := read SharedKey`
- `KeyPair := k0 ← Key(0); k1 ← Key(1); f ← Flip; if f then ret (k1, k0) else ret (k0, k1)`
- `SharedKey := (ks, kp) ← KeyPair; ret ks`
- `Choiceadvrec := read Choice`
- `ChoiceEnc := f ← Flip; c ← Choice; if f then (if c then false else true) else (if c then true else false)`
- `ChoiceEncadvrec := read ChoiceEnc`
- `MsgEnc(0) := m0 ← Msg(0); m1 ← Msg(1); (ks, kp) ← KeyPair; c ← Choice; if c then ret m0 ⊕ kp else ret m0 ⊕ ks`
- `MsgEnc(1) := m0 ← Msg(0); m1 ← Msg(1); (ks, kp) ← KeyPair; c ← Choice; if c then ret m1 ⊕ ks else ret m1 ⊕ kp`
- `MsgEnc(0)advrec := read MsgEnc(0)`
- `MsgEnc(1)advrec := read MsgEnc(1)`
- `Out := m0 ← Msg(0); m1 ← Msg(1); c ← Choice; if c then ret m1 else ret m0`
- `Outadvrec := read Out`

The internal channels `Key(0)` and `Key(1)` are now only used in the channel `KeyPair`. We can therefore fold them in:

- `Flip := samp flip`
- `Flipadvrec := read Flip`
- `OTMsgRcvd(0)advot := k0 ← Key(0); ret ✓`
- `OTMsgRcvd(1)advot := k1 ← Key(1); ret ✓`
- `OTChoiceadvot := read Flip`
- `OTOutadvot := read SharedKey`
- `KeyPair := k0 ← unifmsg; k1 ← unifmsg; f ← Flip; if f then ret (k1, k0) else ret (k0, k1)`
- `SharedKey := (ks, kp) ← KeyPair; ret ks`

- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); (k_s, k_p) \leftarrow \text{KeyPair}; c \leftarrow \text{Choice};$
if c then ret $m_0 \oplus k_p$ else ret $m_0 \oplus k_s$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); (k_s, k_p) \leftarrow \text{KeyPair}; c \leftarrow \text{Choice};$
if c then ret $m_1 \oplus k_s$ else ret $m_1 \oplus k_p$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}$

Rearranging the order of bindings inside KeyPair yields

- $\text{KeyPair} := f \leftarrow \text{Flip}; k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{if } f \text{ then ret } (k_1, k_0) \text{ else ret } (k_0, k_1)$

Since sampling and branching are interchangeable, the three reaction snippets

- $k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{if } f \text{ then ret } (k_1, k_0) \text{ else ret } (k_0, k_1)$
- $\text{if } f \text{ then } (k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ret } (k_1, k_0)) \text{ else } (k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ret } (k_0, k_1))$
- $\text{if } f \text{ then } (k_1 \leftarrow \text{unif}_{\text{msg}}; k_0 \leftarrow \text{unif}_{\text{msg}}; \text{ret } (k_1, k_0)) \text{ else } (k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ret } (k_0, k_1))$

are equivalent. But the last snippet amounts to doing the same thing either way, so we might just as well not flip:

- $\text{KeyPair} := f \leftarrow \text{Flip}; k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ret } (k_0, k_1)$

Getting rid of the gratuitous dependency on the channel Flip gives us

- $\text{KeyPair} := k_0 \leftarrow \text{unif}_{\text{msg}}; k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ret } (k_0, k_1)$

Unfolding the samplings back thus yields the following protocol:

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$
- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read SharedKey}$
- $\text{KeyPair} := k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); \text{ret } (k_0, k_1)$
- $\text{SharedKey} := (k_s, k_p) \leftarrow \text{KeyPair}; \text{ret } k_s$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$

- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); (k_s, k_p) \leftarrow \text{KeyPair}; c \leftarrow \text{Choice};$
if c then ret $m_0 \oplus k_p$ else ret $m_0 \oplus k_s$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); (k_s, k_p) \leftarrow \text{KeyPair}; c \leftarrow \text{Choice};$
if c then ret $m_1 \oplus k_s$ else ret $m_1 \oplus k_p$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice};$ if c then ret m_1 else ret m_0
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}$

The internal channel KeyPair can now be substituted away:

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$
- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read SharedKey}$
- $\text{SharedKey} := \text{read Key}(0)$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice};$ if f then (if c then false else true) else (if c then true else false)
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice};$
if c then ret $m_0 \oplus k_1$ else ret $m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice};$
if c then ret $m_1 \oplus k_0$ else ret $m_1 \oplus k_1$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice};$ if c then ret m_1 else ret m_0
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}$

The second key is now only referenced in the channels $\text{MsgEnc}(0)$ and $\text{MsgEnc}(1)$, where we use it to encrypt either the first or the second message, respectively. This encryption process can be extracted out into a new internal channel PrivateMsg :

- $\text{Key}(0) := \text{samp unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp unif}_{\text{msg}}$

- Flip := samp flip
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read SharedKey}$
- SharedKey := read Key(0)
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- ChoiceEnc := $f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- PrivateMsg := $m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice};$
if c then ret $m_0 \oplus k_1$ else ret $m_1 \oplus k_1$
- MsgEnc(0) := $m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); m_p \leftarrow \text{PrivateMsg}; c \leftarrow \text{Choice};$
if c then ret m_p else ret $m_0 \oplus k_0$
- MsgEnc(1) := $m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); m_p \leftarrow \text{PrivateMsg}; c \leftarrow \text{Choice};$
if c then ret $m_1 \oplus k_0$ else ret m_p
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$
- Out := $m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}$

We can now fold the internal channel Key(1) into the channel PrivateMsg:

- Key(0) := samp unif_{msg}
- Flip := samp flip
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read SharedKey}$
- SharedKey := read Key(0)
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}$
- ChoiceEnc := $f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- PrivateMsg := $m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_1 \leftarrow \text{unif}_{\text{msg}}; c \leftarrow \text{Choice};$
if c then ret $m_0 \oplus k_1$ else ret $m_1 \oplus k_1$

- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); m_p \leftarrow \text{PrivateMsg}; c \leftarrow \text{Choice};$
if c then ret m_p else ret $m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); m_p \leftarrow \text{PrivateMsg}; c \leftarrow \text{Choice};$
if c then ret $m_1 \oplus k_0$ else ret m_p
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice};$ if c then ret m_1 else ret m_0
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read } \text{Out}$

Rearranging the order of bindings inside PrivateMsg yields

- $\text{PrivateMsg} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; k_1 \leftarrow \text{unif}_{\text{msg}};$
if c then ret $m_0 \oplus k_1$ else ret $m_1 \oplus k_1$

Since sampling and branching are interchangeable, and by assumption unif_{msg} is invariant under xor-ing with a fixed message, the three reaction snippets

- $k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ if } c \text{ then ret } m_0 \oplus k_1 \text{ else ret } m_1 \oplus k_1$
- $\text{ if } c \text{ then } (k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ ret } m_0 \oplus k_1) \text{ else } (k_1 \leftarrow \text{unif}_{\text{msg}}; \text{ ret } m_1 \oplus k_1)$
- $\text{ if } c \text{ then samp } \text{unif}_{\text{msg}} \text{ else samp } \text{unif}_{\text{msg}}$

are equivalent. So we may just as well not branch:

- $\text{PrivateMsg} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{ samp } \text{unif}_{\text{msg}}$

Unfolding the sampling back gives us:

- $\text{Key}(0) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read } \text{Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read } \text{Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read } \text{SharedKey}$
- $\text{SharedKey} := \text{read } \text{Key}(0)$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read } \text{Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{ if } f \text{ then } (\text{ if } c \text{ then false else true}) \text{ else } (\text{ if } c \text{ then true else false})$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read } \text{ChoiceEnc}$
- $\text{PrivateMsg} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{ read } \text{Key}(1)$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); m_p \leftarrow \text{PrivateMsg}; c \leftarrow \text{Choice};$
if c then ret m_p else ret $m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); m_p \leftarrow \text{PrivateMsg}; c \leftarrow \text{Choice};$
if c then ret $m_1 \oplus k_0$ else ret m_p

- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{ if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read } \text{Out}$

The internal channel PrivateMsg can now be substituted away, yielding the final version of the real protocol:

- $\text{Key}(0) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Flip} := \text{samp } \text{flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read } \text{Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read } \text{Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read } \text{SharedKey}$
- $\text{SharedKey} := \text{read } \text{Key}(0)$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read } \text{Choice}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{ if } f \text{ then (if } c \text{ then false else true) else (if } c \text{ then true else false)}$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read } \text{ChoiceEnc}$
- $\text{MsgEnc}(0) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice};$
 $\text{ if } c \text{ then ret } k_1 \text{ else ret } m_0 \oplus k_0$
- $\text{MsgEnc}(1) := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice};$
 $\text{ if } c \text{ then ret } m_1 \oplus k_0 \text{ else ret } k_1$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read } \text{MsgEnc}(1)$
- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{ if } c \text{ then ret } m_1 \text{ else ret } m_0$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read } \text{Out}$

6.5 The Simulator

The channel

- $\text{Out} := m_0 \leftarrow \text{Msg}(0); m_1 \leftarrow \text{Msg}(1); c \leftarrow \text{Choice}; \text{ if } c \text{ then ret } m_1 \text{ else ret } m_0$

can now be separated out as coming from the functionality, and the remainder of the protocol is turned into the simulator below. Plugging in the simulator into the ideal functionality and substituting away the internal channels $\text{Choice}_{\text{adv}}^{\text{id}}$ and $\text{Out}_{\text{adv}}^{\text{id}}$ that originally served as a line of communication for the adversary yields the final version of the real protocol, as desired.

- $\text{Key}(0) := \text{samp } \text{unif}_{\text{msg}}$
- $\text{Key}(1) := \text{samp } \text{unif}_{\text{msg}}$

- $\text{Flip} := \text{samp flip}$
- $\text{Flip}_{\text{adv}}^{\text{rec}} := \text{read Flip}$
- $\text{OTMsgRcvd}(0)_{\text{adv}}^{\text{ot}} := k_0 \leftarrow \text{Key}(0); \text{ret } \checkmark$
- $\text{OTMsgRcvd}(1)_{\text{adv}}^{\text{ot}} := k_1 \leftarrow \text{Key}(1); \text{ret } \checkmark$
- $\text{OTChoice}_{\text{adv}}^{\text{ot}} := \text{read Flip}$
- $\text{OTOut}_{\text{adv}}^{\text{ot}} := \text{read SharedKey}$
- $\text{SharedKey} := \text{read Key}(0)$
- $\text{Choice}_{\text{adv}}^{\text{rec}} := \text{read Choice}_{\text{adv}}^{\text{id}}$
- $\text{ChoiceEnc} := f \leftarrow \text{Flip}; c \leftarrow \text{Choice}; \text{if } f \text{ then } (\text{if } c \text{ then false else true}) \text{ else } (\text{if } c \text{ then true else false})$
- $\text{ChoiceEnc}_{\text{adv}}^{\text{rec}} := \text{read ChoiceEnc}$
- $\text{MsgEnc}(0) := m \leftarrow \text{Out}_{\text{adv}}^{\text{id}}; k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice}_{\text{adv}}^{\text{id}};$
 $\text{if } c \text{ then ret } k_1 \text{ else ret } m \oplus k_0$
- $\text{MsgEnc}(1) := m \leftarrow \text{Out}_{\text{adv}}^{\text{id}}; k_0 \leftarrow \text{Key}(0); k_1 \leftarrow \text{Key}(1); c \leftarrow \text{Choice}_{\text{adv}}^{\text{id}};$
 $\text{if } c \text{ then ret } m \oplus k_0 \text{ else ret } k_1$
- $\text{MsgEnc}(0)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(0)$
- $\text{MsgEnc}(1)_{\text{adv}}^{\text{rec}} := \text{read MsgEnc}(1)$
- $\text{Out}_{\text{adv}}^{\text{rec}} := \text{read Out}_{\text{adv}}^{\text{id}}$

7 Multi-Party Coin Toss

In this section we implement a protocol where $n + 2$ parties labeled $0, \dots, n + 1$ reach a Boolean consensus. We prove the protocol secure against a malicious attacker in the case when the last party is honest and any other party is arbitrarily honest or corrupt. Formally, we assume a coin-flip distribution $\text{flip} : 1 \rightarrow \text{Bool}$ and a Boolean sum function $\oplus : \text{Bool} \times \text{Bool} \rightarrow \text{Bool}$, where we write $x \oplus y$ in place of $\oplus(x, y)$.

7.1 The Assumptions

At the expression level, we assume that the operation of Boolean sum with a fixed bit is self-inverse:

- $x : \text{Bool}, y : \text{Bool} \vdash (x \oplus y) \oplus y = x : \text{Bool}.$

At the distribution level, we assume that the distribution flip on bits is invariant under the operation of Boolean sum with a fixed bit (as is indeed the case when flip is uniform):

- $x : \text{Bool} \vdash (y \leftarrow \text{flip}; \text{ret } x \oplus y) = \text{flip} : \text{Bool}$

7.2 The Ideal Protocol

The ideal functionality generates a random Boolean, leaks it to the adversary, and, upon the approval from the adversary, outputs it on behalf of every honest party:

- $\text{Flip} := \text{samp flip}$
- $\text{LeakFlip}_{\text{adv}}^{\text{id}} := \text{read Flip}$
- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{Ok}_{\text{id}}^{\text{adv}}; \text{read Flip} & \text{if } 0 \leq i \leq n + 1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

The output of every corrupted party diverges, since in the malicious setting the external outputs of corrupted parties provide no useful information.

7.3 The Real Protocol

We assume that each party has an associated *commitment functionality* that broadcasts information, and that all broadcast communication is visible to the adversary. At the start of the protocol, each honest party i commits to a randomly generated Boolean and sends it to its commitment functionality:

- $\text{Commit}(i) := \text{samp flip}$

In the malicious setting, we assume that the adversary supplies inputs to each corrupted party in lieu of the party's own internal computation. Thus, each corrupted party i commits to the Boolean of the adversary's choice:

- $\text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}}$

To uniformly cover all cases, we assume channels $\text{AdvCommit}_{\text{party}(i)}^{\text{adv}}$ as inputs to the real protocol, for all $0 \leq i \leq n+1$ even if i is honest; in this case the corresponding input simply goes unused.

Upon receiving the commit from the party, each commitment functionality broadcasts the fact that a commit happened – but not its value – to everybody, including the adversary:

- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i)$

Each honest party i inductively keeps track of all parties that have already committed:

- $\begin{cases} \text{AllCommitted}(i, 0) := \text{ret } \checkmark \\ \text{AllCommitted}(i, j+1) := _ \leftarrow \text{AllCommitted}(i, j); c_j \leftarrow \text{Committed}(j); \text{ret } \checkmark \end{cases} \text{ for } 0 \leq j \leq n+1$

After all parties have committed, each honest party lets the commitment functionality open its commit for everybody else to see:

- $\text{Open}(i) := _ \leftarrow \text{AllCommitted}(i, n+2); \text{ret } \checkmark$

A corrupted party i opens its commit when the adversary says so:

- $\text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}}$

We again assume channels $\text{AdvOpen}_{\text{party}(i)}^{\text{adv}}$ as inputs to the real protocol for all $0 \leq i \leq n+1$.

Upon receiving the party's decision to open the commit, each commitment functionality broadcasts the value of the commit to everybody, including the adversary:

- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i)$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i)$

Each honest party i inductively sums up the commits of all parties once they have been opened:

- $\begin{cases} \text{SumOpened}(i, 0) := \text{ret false} \\ \text{SumOpened}(i, j+1) := x_j \leftarrow \text{SumOpened}(i, j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \end{cases} \text{ for } 0 \leq j \leq n+1$

Finally, each honest party i outputs the consensus - the Boolean sum of all commits:

- $\text{Out}(i) := \text{read SumOpened}(i, n+2)$

The output of each corrupted party i diverges:

- $\text{Out}(i) := \text{read Out}(i)$

Thus, we have the following code for each honest party i :

- $\text{Commit}(i) := \text{samp flip}$

- $\begin{cases} \text{AllCommitted}(i, 0) := \text{ret } \checkmark \\ \text{AllCommitted}(i, j + 1) := _ \leftarrow \text{AllCommitted}(i, j); c_j \leftarrow \text{Committed}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n + 1 \end{cases}$
- $\text{Open}(i) := _ \leftarrow \text{AllCommitted}(i, n + 2); \text{ret } \checkmark$
- $\begin{cases} \text{SumOpened}(i, 0) := \text{ret false} \\ \text{SumOpened}(i, j + 1) := x_j \leftarrow \text{SumOpened}(i, j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n + 1 \end{cases}$
- $\text{Out}(i) := \text{read SumOpened}(i, n + 2)$

The code for a corrupted party i has the following form:

- $\text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}}$
- $\text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}}$
- $\text{Out}(i) := \text{read Out}(i)$

Finally, the code for the commitment functionality for party i is below:

- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i)$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Committed}(i)$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i)$

Composing all of the above together and hiding the internal communication yields the real protocol.

7.4 The Simulator

In the real protocol, the consensus is the Boolean sum of all parties' commits. The simulator, however, gets the value of the consensus from the ideal functionality. To preserve the invariant that the consensus is the sum of all commits, we adjust the last party's commit: it is no longer a random Boolean, but rather the sum of all other commits plus the consensus. Hence, in the simulator, the last commit only happens after all the other commits, unlike in the real world where the last commit has no dependencies. This is okay – the last party is by assumption honest, so there is no leakage that would need to happen right away – but requires some care. Specifically, the announcement that the last party committed must be independent of the timing of the other commits, so we cannot let it actually depend on the last commit as it does in the real world. Instead, we manually postulate no dependencies. The simulator gives the ok message to the functionality once all the commits (except the last, which we explicitly construct) and all the requests to open have been made.

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{LastCommit} := x_{n+1} \leftarrow \text{SumCommit}(n + 1); f \leftarrow \text{LeakFlip}_{\text{adv}}^{\text{id}}; \text{ret } x_{n+1} \oplus f$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j + 1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n \end{cases}$
- $\text{SumCommit}(n + 2) := x_{n+1} \leftarrow \text{SumCommit}(n + 1); c_{n+1} \leftarrow \text{LastCommit}; \text{ret } x_{n+1} \oplus c_{n+1}$
- $\text{Committed}(i) := c_j \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n$
- $\text{Committed}(n + 1) := \text{ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n + 1$

- $\begin{cases} \text{Open}(i) := x_{n+1} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{Ok}_{\text{id}}^{\text{adv}} := _ \leftarrow \text{AllOpen}(n+2); x_{n+1} \leftarrow \text{SumCommit}(n+1); \text{ret } \checkmark$

7.5 Real = Ideal + Simulator

In the real protocol, the composition of all commitment functionalities has the following form:

- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$

Currently, each honest party i keeps its own track of who committed. This is of course unnecessary, as each party has the same information, so we can add new internal channels $\text{AllCommitted}(-)$ that inductively keep a global track of commitment:

- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{AllCommitted}(0) := \text{ret } \checkmark \\ \text{AllCommitted}(j+1) := _ \leftarrow \text{AllCommitted}(j); c_j \leftarrow \text{Committed}(j); \text{ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$

In the presence of the above, we can inductively rewrite the code of each honest party i to the following:

- $\text{Commit}(i) := \text{samp flip}$
- $\text{AllCommitted}(i, j) := \text{read AllCommitted}(j) \text{ for } 0 \leq j \leq n+2$
- $\text{Open}(i) := _ \leftarrow \text{AllCommitted}(i, n+2); \text{ret } \checkmark$
- $\begin{cases} \text{SumOpened}(i, 0) := \text{ret false} \\ \text{SumOpened}(i, j+1) := x_j \leftarrow \text{SumOpened}(i, j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Out}(i) := \text{read SumOpened}(i, n+2)$

After substituting the channel $\text{AllCommitted}(i, n+2)$ into $\text{Open}(i)$, the internal channels $\text{AllCommitted}(i, -)$ become unused and we can eliminate them entirely:

- $\text{Commit}(i) := \text{samp flip}$
- $\text{Open}(i) := _ \leftarrow \text{AllCommitted}(n+2); \text{ret } \checkmark$

- $\begin{cases} \text{SumOpened}(i, 0) := \text{ret false} \\ \text{SumOpened}(i, j + 1) := x_j \leftarrow \text{SumOpened}(i, j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n + 1 \end{cases}$
- $\text{Out}(i) := \text{read SumOpened}(i, n + 2)$

By the same token, we can add new internal channels $\text{SumOpened}(-)$ to the composition of functionalities that inductively keep a global track of the sum of all commits once they have been opened:

- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \quad \text{for } 0 \leq i \leq n + 1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \quad \text{for } 0 \leq i \leq n + 1$
- $\begin{cases} \text{AllCommitted}(0) := \text{ret } \checkmark \\ \text{AllCommitted}(j + 1) := _ \leftarrow \text{AllCommitted}(j); c_j \leftarrow \text{Committed}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n + 1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \quad \text{for } 0 \leq i \leq n + 1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \quad \text{for } 0 \leq i \leq n + 1$
- $\begin{cases} \text{SumOpened}(0) := \text{ret false} \\ \text{SumOpened}(j + 1) := x_j \leftarrow \text{SumOpened}(j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n + 1 \end{cases}$

In the presence of the above, we can inductively rewrite the code of each honest party i to the following:

- $\text{Commit}(i) := \text{samp flip}$
- $\text{Open}(i) := _ \leftarrow \text{AllCommitted}(n + 2); \text{ret } \checkmark$
- $\text{SumOpened}(i, j) := \text{read SumOpened}(j) \quad \text{for } 0 \leq j \leq n + 2$
- $\text{Out}(i) := \text{read SumOpened}(i, n + 2)$

After substituting the channel $\text{SumOpened}(i, n + 2)$ into $\text{Out}(i)$, the internal channels $\text{SumOpened}(i, -)$ become unused and we can eliminate them entirely:

- $\text{Commit}(i) := \text{samp flip}$
- $\text{Open}(i) := _ \leftarrow \text{AllCommitted}(n + 2); \text{ret } \checkmark$
- $\text{Out}(i) := \text{read SumOpened}(n + 2)$

The combined code for the real protocol after the aforementioned changes is thus as follows:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n + 1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \quad \text{for } 0 \leq i \leq n + 1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \quad \text{for } 0 \leq i \leq n + 1$
- $\begin{cases} \text{AllCommitted}(0) := \text{ret } \checkmark \\ \text{AllCommitted}(j + 1) := _ \leftarrow \text{AllCommitted}(j); c_j \leftarrow \text{Committed}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n + 1 \end{cases}$
- $\begin{cases} \text{Open}(i) := _ \leftarrow \text{AllCommitted}(n + 2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n + 1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \quad \text{for } 0 \leq i \leq n + 1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \quad \text{for } 0 \leq i \leq n + 1$

- $\begin{cases} \text{SumOpened}(0) := \text{ret false} \\ \text{SumOpened}(j+1) := x_j \leftarrow \text{SumOpened}(j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\begin{cases} \text{Out}(i) := \text{read SumOpened}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

Instead of summing up the commits once they have been opened, we can sum them up at the beginning, as done in the simulator, using new internal channels $\text{SumCommit}(-)$:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{AllCommitted}(0) := \text{ret } \checkmark \\ \text{AllCommitted}(j+1) := _ \leftarrow \text{AllCommitted}(j); c_j \leftarrow \text{Committed}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\begin{cases} \text{Open}(i) := _ \leftarrow \text{AllCommitted}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{SumOpened}(0) := \text{ret false} \\ \text{SumOpened}(j+1) := x_j \leftarrow \text{SumOpened}(j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\begin{cases} \text{Out}(i) := \text{read SumOpened}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

In the presence of these new channels, the channels $\text{AllCommitted}(-)$ can be simplified:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{AllCommitted}(j) := c_j \leftarrow \text{SumCommit}(j); \text{ret } \checkmark \text{ for } 0 \leq j \leq n+2$
- $\begin{cases} \text{Open}(i) := _ \leftarrow \text{AllCommitted}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$

- $\begin{cases} \text{SumOpened}(0) := \text{ret false} \\ \text{SumOpened}(j+1) := x_j \leftarrow \text{SumOpened}(j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\begin{cases} \text{Out}(i) := \text{read SumOpened}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

After substituting the channel $\text{AllCommitted}(n+2)$ into the channels $\text{Open}(i)$ for $0 \leq i \leq n+1$ honest, the internal channels $\text{AllCommitted}(-)$ become unused and we can eliminate them entirely:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{SumOpened}(0) := \text{ret false} \\ \text{SumOpened}(j+1) := x_j \leftarrow \text{SumOpened}(j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\begin{cases} \text{Out}(i) := \text{read SumOpened}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

Proceeding further, we can keep track of the decisions to open the commits just as the simulator does, using new internal channels $\text{AllOpen}(-)$:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$

- $\begin{cases} \text{SumOpened}(0) := \text{ret false} \\ \text{SumOpened}(j+1) := x_j \leftarrow \text{SumOpened}(j); o_j \leftarrow \text{Opened}(j); \text{ret } x_j \oplus o_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\begin{cases} \text{Out}(i) := \text{read SumOpened}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

In the presence of these new channels, the channels $\text{SumOpened}(-)$ can be simplified:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{SumOpened}(j) := _ \leftarrow \text{AllOpen}(j); \text{read SumCommit}(j) \text{ for } 0 \leq j \leq n+2$
- $\begin{cases} \text{Out}(i) := \text{read SumOpened}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

After substituting the channel $\text{SumOpened}(n+2)$ into the channels $\text{Out}(i)$ for $0 \leq i \leq n$ honest, the internal channels $\text{SumOpened}(-)$ become unused and we can eliminate them entirely:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark \quad \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$

- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

This is the cleaned-up version of the real protocol. Plugging the simulator into the ideal protocol and substituting away the channels $\text{LeakFlip}_{\text{adv}}^{\text{id}}$ and $\text{Ok}_{\text{id}}^{\text{adv}}$ that have now become internal yields the following:

- $\text{Flip} := \text{samp flip}$
- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{LastCommit} := x_{n+1} \leftarrow \text{SumCommit}(n+1); f \leftarrow \text{Flip}; \text{ret } x_{n+1} \oplus f$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); \text{ret } x_j \oplus c_j & \text{for } 0 \leq j \leq n \end{cases}$
- $\text{SumCommit}(n+2) := x_{n+1} \leftarrow \text{SumCommit}(n+1); c_{n+1} \leftarrow \text{LastCommit}; \text{ret } x_{n+1} \oplus c_{n+1}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n$
- $\text{Committed}(n+1) := \text{ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); x_{n+1} \leftarrow \text{SumCommit}(n+1); \text{read Flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

Substituting the channel LastCommit into the channel $\text{SumCommit}(n+2)$ yields:

- $\text{SumCommit}(n+2) := x_{n+1} \leftarrow \text{SumCommit}(n+1); f \leftarrow \text{Flip}; \text{ret } x_{n+1} \oplus (x_{n+1} \oplus f)$

By assumption, we can cancel out the Boolean sum:

- $\text{SumCommit}(n+2) := x_{n+1} \leftarrow \text{SumCommit}(n+1); \text{read Flip}$

In the presence of this simplified definition, we can rewrite the channels $\text{Out}(-)$ to the following:

- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

The original formulation of $\text{SumCommit}(n+2)$ will be more convenient for our purposes, so we rewrite it back to end up with the following protocol:

- $\text{Flip} := \text{samp flip}$
- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$

- $\text{LastCommit} := x_{n+1} \leftarrow \text{SumCommit}(n+1); f \leftarrow \text{Flip}; x_{n+1} \oplus f$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); x_j \oplus c_j & \text{for } 0 \leq j \leq n \end{cases}$
- $\text{SumCommit}(n+2) := x_{n+1} \leftarrow \text{SumCommit}(n+1); c_{n+1} \leftarrow \text{LastCommit}; x_{n+1} \oplus c_{n+1}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n$
- $\text{Committed}(n+1) := \text{ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

The channel Flip now only occurs in the channel LastCommit, so we can fold it in:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{LastCommit} := x_{n+1} \leftarrow \text{SumCommit}(n+1); f \leftarrow \text{samp flip}; x_{n+1} \oplus f$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); x_j \oplus c_j & \text{for } 0 \leq j \leq n \end{cases}$
- $\text{SumCommit}(n+2) := x_{n+1} \leftarrow \text{SumCommit}(n+1); c_{n+1} \leftarrow \text{LastCommit}; x_{n+1} \oplus c_{n+1}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n$
- $\text{Committed}(n+1) := \text{ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

By assumption, the distribution flip is invariant under taking a Boolean sum with a fixed bit:

- $\text{LastCommit} := x_{n+1} \leftarrow \text{SumCommit}(n+1); \text{ samp flip}$

We can unfold the sampling back into a new internal channel $\text{Commit}(n+1)$:

- $\begin{cases} \text{Commit}(i) := \text{ samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{ read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\text{LastCommit} := x_{n+1} \leftarrow \text{SumCommit}(n); \text{ read Commit}(n+1)$
- $\begin{cases} \text{SumCommit}(0) := \text{ ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); x_j \oplus c_j & \text{for } 0 \leq j \leq n \end{cases}$
- $\text{SumCommit}(n+2) := x_{n+1} \leftarrow \text{SumCommit}(n+1); c_{n+1} \leftarrow \text{LastCommit}; x_{n+1} \oplus c_{n+1}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ ret } \checkmark \text{ for } 0 \leq i \leq n$
- $\text{Committed}(n+1) := \text{ ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{ read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{ read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{ read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{ read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{ read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{ read Out}(i) & \text{otherwise} \end{cases}$

The internal channel LastCommit can now be substituted away:

- $\begin{cases} \text{Commit}(i) := \text{ samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{ read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); x_j \oplus c_j & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ ret } \checkmark \text{ for } 0 \leq i \leq n$
- $\text{Committed}(n+1) := \text{ ret } \checkmark$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{ read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{ read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{ read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{ read Opened}(i) \text{ for } 0 \leq i \leq n+1$

- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

Finally, we rewrite the channel $\text{Committed}(n+1)$ to include a gratuitous dependency on $\text{Commit}(n+1)$:

- $\begin{cases} \text{Commit}(i) := \text{samp flip} & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Commit}(i) := \text{read AdvCommit}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SumCommit}(0) := \text{ret false} \\ \text{SumCommit}(j+1) := x_j \leftarrow \text{SumCommit}(j); c_j \leftarrow \text{Commit}(j); x_j \oplus c_j & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Committed}(i) := c_i \leftarrow \text{Commit}(i); \text{ret } \checkmark \text{ for } 0 \leq i \leq n+1$
- $\text{LeakCommitted}(i)_{\text{adv}}^{\text{comm}} := \text{read Committed}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Open}(i) := x_{n+2} \leftarrow \text{SumCommit}(n+2); \text{ret } \checkmark & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Open}(i) := \text{read AdvOpen}_{\text{party}(i)}^{\text{adv}} & \text{otherwise} \end{cases}$
- $\begin{cases} \text{AllOpen}(0) := \text{ret } \checkmark \\ \text{AllOpen}(j+1) := _ \leftarrow \text{AllOpen}(j); _ \leftarrow \text{Open}(j); \text{ret } \checkmark & \text{for } 0 \leq j \leq n+1 \end{cases}$
- $\text{Opened}(i) := _ \leftarrow \text{Open}(i); \text{read Commit}(i) \text{ for } 0 \leq i \leq n+1$
- $\text{LeakOpened}(i)_{\text{adv}}^{\text{comm}} := \text{read Opened}(i) \text{ for } 0 \leq i \leq n+1$
- $\begin{cases} \text{Out}(i) := _ \leftarrow \text{AllOpen}(n+2); \text{read SumCommit}(n+2) & \text{if } 0 \leq i \leq n+1 \text{ honest} \\ \text{Out}(i) := \text{read Out}(i) & \text{otherwise} \end{cases}$

But this is precisely the cleaned-up version of the real protocol.

8 Two-Party GMW Protocol

In the two-party GMW protocol, Alice and Bob jointly compute the value of a given Boolean circuit built out of *xor*-, *and*-, and *not* gates. The inputs to the circuit are divided between Alice and Bob, and neither party has access to the inputs of the other. For each gate, Alice and Bob maintain their respective *shares* of the actual value v computed by the gate, with Alice's share computed only from the information available to Alice, and analogously for Bob. The respective shares for Alice and Bob sum up to v . We prove the protocol secure against a semi-honest attacker in the case when Alice is corrupt and Bob is honest.

Formally, we assume a coin-flip distribution $\text{flip} : 1 \rightarrow \text{Bool}$; a Boolean sum function $\oplus : \text{Bool} \times \text{Bool} \rightarrow \text{Bool}$, where we write $x \oplus y$ in place of $\oplus(x, y)$; a Boolean multiplication function $*$: $\text{Bool} \times \text{Bool} \rightarrow \text{Bool}$, where we write $x * y$ in place of $*$ (x, y); and a Boolean negation function $\neg : \text{Bool} \rightarrow \text{Bool}$, where we write $\neg x$ in place of $\neg x$.

We represent Boolean circuits using the syntax below, where we assume an ambient (finite) set I of inputs. Starting from the empty circuit ϵ we add one gate at a time: an *input* gate allows us to plug into a specified input i ; a *not* gate negates the value carried on wire k ; an *xor* gate computes the Boolean sum of the two values carried on wires k and l ; and an *and* gate does the same for Boolean product.

Inputs	$i \in I$
Wires	$k, l \in \mathbb{N}$
Circuits	$C ::= \epsilon \mid C; \text{input-gate}(i) \mid C; \text{not-gate}(k) \mid C; \text{xor-gate}(k, l) \mid C; \text{and-gate}(k, l)$

A circuit C with $n \in \mathbb{N}$ wires is considered well-formed if each logical gate combines previously defined wires only:

$$\begin{array}{c}
\frac{}{\epsilon \text{ circuit}(0)} \qquad \frac{C \text{ circuit}(n)}{C; \text{input-gate}(i) \text{ circuit}(n+1)} \qquad \frac{C \text{ circuit}(n) \quad k < n}{C; \text{not-gate}(k) \text{ circuit}(n+1)} \\
\\
\frac{C \text{ circuit}(n) \quad k < n \quad l < n}{C; \text{xor-gate}(k, l) \text{ circuit}(n+1)} \qquad \frac{C \text{ circuit}(n) \quad k < n \quad l < n}{C; \text{and-gate}(k, l) \text{ circuit}(n+1)}
\end{array}$$

For our specific setup, we assume Alice has $N \geq 0$ inputs labeled $\{0, \dots, N-1\}$, and Bob has $M \geq 0$ inputs labeled $\{0, \dots, M-1\}$. The set of inputs to our ambient Boolean circuit C (with, let us say, K wires) is therefore $M + N$. We furthermore assume that a subset of the wires $\{0, \dots, K-1\}$ is designated as outputs.

8.1 The Assumptions

At the expression level, we assume that the Boolean sum and product operations are commutative and associative:

- $x : \text{Bool}, y : \text{Bool} \vdash x \oplus y = y \oplus x : \text{Bool}$,
- $x : \text{Bool}, y : \text{Bool} \vdash x * y = y * x : \text{Bool}$,
- $x : \text{Bool}, y : \text{Bool}, z : \text{Bool} \vdash (x \oplus y) \oplus z = x \oplus (y \oplus z) : \text{Bool}$, and
- $x : \text{Bool}, y : \text{Bool}, z : \text{Bool} \vdash (x * y) * z = x * (y * z) : \text{Bool}$.

Furthermore, Boolean multiplication distributes over Boolean sum:

- $x : \text{Bool}, y : \text{Bool}, z : \text{Bool} \vdash (x \oplus y) * z = (x * y) \oplus (y * z) : \text{Bool}$.

Summing up a Boolean with itself yields `false` and summing up a Boolean with `false` yields the original Boolean:

- $x : \text{Bool} \vdash x \oplus x = \text{false} : \text{Bool}$, and
- $x : \text{Bool} \vdash x \oplus \text{false} = x : \text{Bool}$.

Negating a Boolean equals summing it up with `true`:

- $x : \text{Bool} \vdash x \oplus \text{true} = \neg x : \text{Bool}$.

Finally, multiplying a Boolean with `false` or `true` yields `false` or the original Boolean, respectively:

- $x : \text{Bool} \vdash x * \text{false} = \text{false} : \text{Bool}$, and
- $x : \text{Bool} \vdash x * \text{true} = x : \text{Bool}$.

At the distribution level, we assume that the distribution flip on Booleans is invariant under the operation of Boolean sum with a fixed Boolean (as is indeed the case when flip is uniform):

- $x : \text{Bool} \vdash (y \leftarrow \text{flip}; \text{ret } x \oplus y) = \text{flip} : \text{Bool}$

8.2 The Ideal Protocol

The leakage from the ideal functionality includes the timing information for Bob's inputs plus the value of Alice's inputs (since she is semi-honest):

- $\text{In}(A, i)_{\text{adv}}^{\text{id}} := \text{In}(A, i) \text{ for } 0 \leq i < N$
- $\text{InRcvd}(B, i)_{\text{adv}}^{\text{id}} := x \leftarrow \text{In}(B, i); \text{ret } \checkmark \text{ for } 0 \leq i < M$

In the inductive phase, the functionality computes the value carried by each wire $k < K$ of the ambient circuit by induction on the circuit:

- $\text{Wires}(\epsilon, 0)$ is the protocol 0

- $\text{Wires}(C; \text{input-gate}(i), K+1)$ is the composition of the protocol $\text{Wires}(C, K)$ with the single-reaction protocol
 - $\begin{cases} \text{Wire}(K) := \text{read In}(A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Wire}(K) := \text{read In}(B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{Wires}(C; \text{not-gate}(k), K+1)$ is the composition of the protocol $\text{Wires}(C, K)$ with the single-reaction protocol
 - $\text{Wire}(K) := x \leftarrow \text{Wire}(k); \text{ret } \neg x$
- $\text{Wires}(C; \text{xor-gate}(k, l), K+1)$ is the composition of the protocol $\text{Wires}(C, K)$ with the single-reaction protocol
 - $\text{Wire}(K) := x \leftarrow \text{Wire}(k); y \leftarrow \text{Wire}(l); \text{ret } x \oplus y$
- $\text{Wires}(C; \text{and-gate}(k, l), K+1)$ is the composition of the protocol $\text{Wires}(C, K)$ with the single-reaction protocol
 - $\text{Wire}(K) := x \leftarrow \text{Wire}(k); y \leftarrow \text{Wire}(l); \text{ret } x * y$

After performing the above computation, the ideal functionality outputs the computed value for each wire marked as an output, and leaks the outputs to the adversary on behalf of Alice:

- $\begin{cases} \text{Out}(A, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(A, k) := \text{read Out}(A, k) & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(B, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(B, k) := \text{read Out}(B, k) & \text{otherwise} \end{cases}$
- $\text{Out}(A, k)_{\text{adv}}^{\text{id}} := \text{read Out}(A, k) \text{ for } 0 \leq k < K$

Finally, the channels $\text{Wire}(-)$ coming from the inductive protocol $\text{Wires}(C, K)$ are designated as internal.

8.3 The Real Protocol

The real protocol consists of the two parties, plus an instance of an ideal 1-Out-Of-4 Oblivious Transfer (OT) functionality for each gate, with Alice the sender and Bob the receiver. The code for each party is separated into three parts: in the initial phase, each party computes and distributes everyone's shares for each of its inputs. In the inductive phase, each party computes their share of each wire by induction on the ambient circuit. At last, in the final phase, Alice and Bob send their shares of each output wire to each other and add them up to compute the result.

8.3.1 Alice: The Initial Phase

Alice generates her own shares randomly and sends Bob the sum of her share and the actual value of the input. Alice's share of Bob's input is sent to her by Bob. As Alice is semi-honest, she leaks the value of her inputs. After storing each share, Alice leaks it to the adversary. Furthermore, when sending Bob's share of her input to Bob, she simultaneously leaks it to the adversary, and after receiving her share of Bob's input from Bob, she forwards it along to the adversary.

- $\text{In}(A, i)_{\text{adv}}^A := \text{read In}(A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(A, A, i) := x \leftarrow \text{In}(A, i); \text{samp flip for } 0 \leq i < N$
- $\text{InputShare}(A, B, i) := \text{read SendInputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i)_{\text{adv}}^A := \text{read InputShare}(A, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(A, B, i)_{\text{adv}}^A := \text{read InputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i) := x \leftarrow \text{In}(A, i); x_A \leftarrow \text{InputShare}(A, A, i); \text{ret } x \oplus x_A \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(B, A, i)_{\text{adv}}^A := \text{read SendInputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i)_{\text{adv}}^A := \text{read SendInputShare}(A, B, i) \text{ for } 0 \leq i < M$

8.3.2 Bob: The Initial Phase

Bob generates Alice's shares randomly, and sets his own share to be the sum of Alice's share and the actual value of the input. His share of Alice's input is sent to him by Alice. Since Bob is honest, the only leakage from him is the timing of his inputs.

- $\text{InRcvd}(B, i)_{\text{adv}}^B := x \leftarrow \text{In}(B, i); \text{ ret } \checkmark \text{ for } 0 \leq i < M$
- $\text{InputShare}(B, A, i) := \text{read SendInputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(B, B, i) := x \leftarrow \text{In}(B, i); x_A \leftarrow \text{SendInputShare}(A, B, i); \text{ ret } x \oplus x_A \text{ for } 0 \leq i < M$
- $\text{SendInputShare}(A, B, i) := x \leftarrow \text{In}(B, i); \text{ samp flip for } 0 \leq i < M$

8.3.3 Alice: The Inductive Phase

In the case of an *input* gate, Alice uses her corresponding input share from the initial stage. In the case of a *not* gate, she simply copies her share x_A of the incoming wire. If the gate is an *xor* gate, the resulting share is the sum $x_A \oplus y_A$ of the shares of the incoming two wires. The case of an *and* gate is the most complex. The sum of Alice's and Bob's respective shares must equal $(x_A \oplus x_B) * (y_A \oplus y_B)$, where x_A, y_A and x_B, y_B are the respective shares of Alice and Bob on the incoming two wires. We have

$$(x_A \oplus x_B) * (y_A \oplus y_B) = (x_A * y_A) \oplus (x_A * y_B) \oplus (x_B * y_A) \oplus (x_B * y_B)$$

and the quantity $(x_A * y_B) \oplus (x_B * y_A)$ cannot be directly computed by either Alice or Bob, as neither of them has access to the shares of the other. Instead, Alice and Bob engage in an idealized 1-Out-Of-4 OT exchange: there are four possible combinations of values that x_B, y_B can take, and Alice computes the value of $(x_A * y_B) \oplus (x_B * y_A)$ for each. This offers Bob four messages to choose from, and he selects the one corresponding to the actual values of x_B, y_B . A small caveat: in the exchange as described above, Bob would still be able to infer the value of Alice's shares in certain cases: *e.g.*, if $x_B = 0$ and $y_B = 1$, Bob gets the share x_A as the result of the exchange. To prevent this, Alice encodes her messages by xor-ing them with a random bit b that only she knows.

To stay consistent throughout the cases, we set up our protocol so that each gate induces the same set of outputs, even though some of these channels may not be relevant to the specific case in question. For example, at each gate Alice will construct a channel $\text{OTBit}(A, B, -)$ to *potentially* store the aforementioned random bit b , in the case that the gate happens to be an *and* gate and she needs to engage in a 1-Out-Of-4 OT exchange with Bob. Similar remarks apply to all the OT channels, which are likewise only relevant for Boolean multiplication. Irrelevant channels will simply diverge, which makes them effectively nonexistent.

- $A(\epsilon, 0)$ is the protocol 0
- $A(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $A(C, K)$ with the protocol we now describe. As mentioned before, Alice maintains a divergent Boolean channel $\text{OTBit}(A, B, K)$, accompanied by the corresponding vacuous leakage:
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$

Alice's share is the input share as determined in the initial part of the protocol:

- $\begin{cases} \text{Share}(A, K) := \text{read InputShare}(A, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(A, K) := \text{read InputShare}(A, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$

The 1-Out-Of-4 OT exchange with Bob is vacuous:

- $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
- $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$

- $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
- $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
- $A(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $A(C, K)$ with the following protocol, largely analogous to the previous case. Alice again maintains a divergent Boolean channel $\text{OTBit}(A, B, K)$, accompanied by the corresponding vacuous leakage:

- $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$

Alice's share is the share on wire k :

- $\text{Share}(A, K) := \text{read Share}(A, k)$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$

As before, she engages in a vacuous 1-Out-Of-4 OT exchange with Bob:

- $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
- $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
- $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
- $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$

- $A(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $A(C, K)$ with the following protocol, analogous to the previous two cases. As before, Alice maintains a divergent Boolean channel $\text{OTBit}(A, B, K)$, accompanied by the corresponding vacuous leakage:

- $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$

Alice's share is the sum of shares on wires k and l :

- $\text{Share}(A, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } x_A \oplus y_A$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$

As before, Alice engages in a vacuous 1-Out-Of-4 OT exchange with Bob:

- $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
- $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
- $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
- $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$

- $A(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $A(C, K)$ with the protocol we now describe. First, Alice uniformly generates a random bit for the OT exchange with Bob:

- $\text{OTBit}(A, B, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{samp flip}$
- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)$

Her share is the encoded product of shares on wires k and l , where the encoding is the summation with the above random bit:

- $\text{Share}(A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } (x_A * y_A) \oplus b_A$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$

Alice's 1-Out-Of-4 OT exchange with Bob is now proper:

- $\text{OTMsg}(A, B, K, 0) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
- $\text{OTMsg}(A, B, K, 1) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
- $\text{OTMsg}(A, B, K, 2) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
- $\text{OTMsg}(A, B, K, 3) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$

8.3.4 Bob: The Inductive Phase

In the case of an *input* gate, Bob uses his corresponding input share from the initial stage. In the case of a *not* gate, the resulting share is a negation of the share x_B of the incoming wire. If the gate is an *xor* gate, the resulting share is the sum $x_B \oplus y_B$ of the shares of the incoming two wires. Finally, in the case of an *and* gate, Bob engages in an idealized 1-Out-Of-4 exchange with Alice as described in the previous section. To compute his share, he adds the result of the OT exchange to the product $x_B * y_B$ of the shares of the incoming two wires.

- $B(\epsilon, 0)$ is the protocol 0
- $B(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $B(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\begin{cases} \text{Share}(B, K) := \text{read InputShare}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(B, K) := \text{read InputShare}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$

As for Alice, we include the requisite vacuous OT channels to stay consistent throughout the cases.

- $B(C; \text{not-gate}(k), K + 1)$ the composition of the protocol $B(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(B, K) := x_B \leftarrow \text{Share}(B, k); \text{ret } \neg x_B$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
- $B(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $B(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(B, K) := x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } x_B \oplus y_B$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
- $B(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $B(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTOut}(A, B, K)$
 - $\text{Share}(B, K) := b_B \leftarrow \text{OTBit}(B, A, K); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read Share}(B, k)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read Share}(B, l)$

8.3.5 Alice: The Final Phase

For each output wire, Alice sends her share to Bob while simultaneously leaking it to the adversary. Each share received from Bob is likewise forwarded to the adversary. Finally, Alice computes the output by summing up her and Bob's respective shares, and leaks the result to the adversary.

- $\begin{cases} \text{SendFinalShare}(A, k) := \text{read Share}(A, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(A, k) := \text{read SendFinalShare}(A, k) & \text{otherwise} \end{cases}$
- $\text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read SendFinalShare}(A, k)$ for $0 \leq k < K$
- $\text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read SendFinalShare}(B, k)$ for $0 \leq k < K$
- $\text{Out}(A, k) := x_A \leftarrow \text{SendFinalShare}(A, k); x_B \leftarrow \text{SendFinalShare}(B, k); \text{ret } x_A \oplus x_B$ for $0 \leq k < K$
- $\text{Out}(A, k)_{\text{adv}}^A := \text{read Out}(A, k)$ for $0 \leq k < K$

8.3.6 Bob: The Final Phase

For each output wire, Bob sends his share to Alice and computes the output by summing up his and Alice's respective shares.

- $\begin{cases} \text{SendFinalShare}(\mathbf{B}, k) := \text{read Share}(\mathbf{B}, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(\mathbf{B}, k) := \text{read SendFinalShare}(\mathbf{B}, k) & \text{otherwise} \end{cases}$
- $\text{Out}(\mathbf{B}, k) := x_A \leftarrow \text{SendFinalShare}(\mathbf{A}, k); x_B \leftarrow \text{SendFinalShare}(\mathbf{B}, k); \text{ret } x_A \oplus x_B \text{ for } 0 \leq k < K$

8.3.7 1-Out-Of-4 Oblivious Transfer Functionality

For each wire $0 \leq k < K$ we have a separate idealized 1-Out-Of-4 OT functionality $\text{1OutOf4OT}(k)$, which we now describe. The functionality starts by selecting the correct message:

- $\text{OTOut}(\mathbf{A}, \mathbf{B}, k) := m_0 \leftarrow \text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 0); m_1 \leftarrow \text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 1); m_2 \leftarrow \text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 2); m_3 \leftarrow \text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 3); c_0 \leftarrow \text{OTChoice}(\mathbf{B}, \mathbf{A}, K, 0); c_1 \leftarrow \text{OTChoice}(\mathbf{B}, \mathbf{A}, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)

Since Alice is semi-honest, the functionality leaks the value of all messages received from Alice:

- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, k, 0)$
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, k, 1)$
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, k, 2)$
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, k, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, k, 3)$

Since Bob is honest, only the timing information for his inputs is leaked:

- $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}} := c_0 \leftarrow \text{OTChoice}(\mathbf{B}, \mathbf{A}, k, 0); \text{ret } \checkmark$
- $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}} := c_1 \leftarrow \text{OTChoice}(\mathbf{B}, \mathbf{A}, k, 1); \text{ret } \checkmark$

8.3.8 The Real Protocol

The complete code for Alice arises as the composition of Alice's initial, inductive, and final stages, followed by the hiding of the communication internal to Alice - namely, the channels

- $\text{InputShare}(\mathbf{A}, \mathbf{A}, i)$ for $0 \leq i < N$,
- $\text{InputShare}(\mathbf{A}, \mathbf{B}, i)$ for $0 \leq i < M$,
- $\text{OTBit}(\mathbf{A}, \mathbf{B}, k)$ for $0 \leq k < K$, and
- $\text{Share}(\mathbf{A}, k)$ for $0 \leq k < K$.

Analogously, the complete code for Bob arises as the composition of Bob's initial, inductive, and final stages, followed by the hiding of the communication internal to Bob - namely, the channels

- $\text{InputShare}(\mathbf{B}, \mathbf{A}, i)$ for $0 \leq i < N$,
- $\text{InputShare}(\mathbf{B}, \mathbf{B}, i)$ for $0 \leq i < M$,
- $\text{OTBit}(\mathbf{B}, \mathbf{A}, k)$ for $0 \leq k < K$, and
- $\text{Share}(\mathbf{B}, k)$ for $0 \leq k < K$.

Finally, the real protocol is a composition of the two parties plus K copies of the OT functionality,

- $1\text{OutOf4OT}(k)$ for $0 \leq k < K$,

all followed by the hiding of the internal communication among the two parties and the functionality: the channels

- $\text{SendInputShare}(A, B, i)$ for $0 \leq i < M$,
- $\text{SendInputShare}(B, A, i)$ for $0 \leq i < N$,
- $\text{OTMsg}(A, B, k, 0)$ for $0 \leq k < K$,
- $\text{OTMsg}(A, B, k, 1)$ for $0 \leq k < K$,
- $\text{OTMsg}(A, B, k, 2)$ for $0 \leq k < K$,
- $\text{OTMsg}(A, B, k, 3)$ for $0 \leq k < K$,
- $\text{OTChoice}(B, A, k, 0)$ for $0 \leq k < K$,
- $\text{OTChoice}(B, A, k, 1)$ for $0 \leq k < K$,
- $\text{OTOut}(B, A, k)$ for $0 \leq k < K$,
- $\text{SendFinalShare}(A, k)$ for $0 \leq k < K$, and
- $\text{SendFinalShare}(B, k)$ $0 \leq k < K$.

8.4 Real = Ideal + Simulator

Our goal is to keep simplifying the real protocol until it becomes clear how to extract out a suitable simulator. We first restructure the entire protocol as a composition of an initial part, an inductive part, and a final part, followed by the hiding of the channels

- $\text{InputShare}(A, A, i)$ for $0 \leq i < N$,
- $\text{InputShare}(A, B, i)$ for $0 \leq i < M$,
- $\text{InputShare}(B, A, i)$ for $0 \leq i < N$,
- $\text{InputShare}(B, B, i)$ for $0 \leq i < M$,
- $\text{OTBit}(A, B, k)$ for $0 \leq k < K$,
- $\text{OTBit}(B, A, k)$ for $0 \leq k < K$,
- $\text{Share}(A, k)$ for $0 \leq k < K$, and
- $\text{Share}(B, k)$ for $0 \leq k < K$.

The initial part arises by composing together the initial parts for Alice and Bob, and declaring the channels $\text{SendInputShare}(B, A, -)$ and $\text{SendInputShare}(A, B, -)$ as internal:

- $\text{In}(A, i)_{\text{adv}}^A := \text{read } \text{In}(A, i) \text{ for } 0 \leq i < N$
- $\text{InRcvd}(B, i)_{\text{adv}}^B := x \leftarrow \text{In}(B, i); \text{ ret } \checkmark \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i) := x \leftarrow \text{In}(A, i); \text{ samp flip for } 0 \leq i < N$
- $\text{InputShare}(A, B, i) := \text{read } \text{SendInputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{InputShare}(B, A, i) := \text{read } \text{SendInputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(B, B, i) := x_A \leftarrow \text{SendInputShare}(A, B, i); x \leftarrow \text{In}(B, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < M$

- $\text{InputShare}(A, A, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); x \leftarrow \text{In}(A, i); \text{ret } x_A \oplus x \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i) := x \leftarrow \text{In}(B, i); \text{samp flip for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i)_{\text{adv}}^A := \text{read } \text{SendInputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{SendInputShare}(A, B, i) \text{ for } 0 \leq i < M$

The inductive part of the real protocol arises by composing together the inductive parts for Alice and Bob plus the K copies of the OT functionality, and declaring the communication with the OT functionality as internal:

- $\text{Real}(\epsilon, 0)$ is the protocol 0
- $\text{Real}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read } \text{OTBit}(A, B, K)$
 - $\text{OTBit}(B, A, K) := \text{read } \text{OTBit}(B, A, K)$
 - $\begin{cases} \text{Share}(A, K) := \text{read } \text{InputShare}(A, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(A, K) := \text{read } \text{InputShare}(A, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
 - $\begin{cases} \text{Share}(B, K) := \text{read } \text{InputShare}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(B, K) := \text{read } \text{InputShare}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
 - $\text{OTMsg}(A, B, K, 0) := \text{read } \text{OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read } \text{OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read } \text{OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read } \text{OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read } \text{OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read } \text{OTChoice}(B, A, K, 1)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2); m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1); \text{if } c_0 \text{ then (if } c_1 \text{ then ret } m_3 \text{ else ret } m_2) \text{ else (if } c_1 \text{ then ret } m_1 \text{ else ret } m_0)$
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read } \text{OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read } \text{Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read } \text{OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read } \text{OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read } \text{OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read } \text{OTMsg}(A, B, K, 3)$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := c_0 \leftarrow \text{OTChoice}(B, A, K, 0); \text{ret } \checkmark$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := c_1 \leftarrow \text{OTChoice}(B, A, K, 1); \text{ret } \checkmark$
- $\text{Real}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read } \text{OTBit}(A, B, K)$
 - $\text{OTBit}(B, A, K) := \text{read } \text{OTBit}(B, A, K)$
 - $\text{Share}(A, K) := \text{read } \text{Share}(A, k)$

- $\text{Share}(B, K) := x_B \leftarrow \text{Share}(B, k); \text{ret } \neg x_B$
- $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
- $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
- $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
- $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
- $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
- $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
- $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
- $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)$
- $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)$
- $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)$
- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := c_0 \leftarrow \text{OTChoice}(B, A, K, 0); \text{ret } \checkmark$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := c_1 \leftarrow \text{OTChoice}(B, A, K, 1); \text{ret } \checkmark$
- $\text{Real}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(A, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } x_A \oplus y_A$
 - $\text{Share}(B, K) := x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } x_B \oplus y_B$
 - $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := c_0 \leftarrow \text{OTChoice}(B, A, K, 0); \text{ret } \checkmark$

- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := c_1 \leftarrow \text{OTChoice}(B, A, K, 1); \text{ret } \checkmark$
- $\text{Real}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{samp flip}$
 - $\text{OTBit}(B, A, K) := \text{OTOut}(A, B, K)$
 - $\text{Share}(A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } (x_A * y_A) \oplus b_A$
 - $\text{Share}(B, K) := b_B \leftarrow \text{OTBit}(B, A, K); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$
 - $\text{OTMsg}(A, B, K, 0) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
 - $\text{OTMsg}(A, B, K, 1) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
 - $\text{OTMsg}(A, B, K, 2) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
 - $\text{OTMsg}(A, B, K, 3) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
 - $\text{OTChoice}(B, A, K, 0) := \text{read Share}(B, k)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read Share}(B, l)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
 if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := c_0 \leftarrow \text{OTChoice}(B, A, K, 0); \text{ret } \checkmark$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := c_1 \leftarrow \text{OTChoice}(B, A, K, 1); \text{ret } \checkmark$

At last, the final part of the real protocol arises by composing together the final parts for Alice and Bob, and declaring the channels $\text{SendFinalShare}(A, -)$ and $\text{SendFinalShare}(B, -)$ as internal:

- $\begin{cases} \text{SendFinalShare}(A, k) := \text{read Share}(A, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(A, k) := \text{read SendFinalShare}(A, k) & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SendFinalShare}(B, k) := \text{read Share}(B, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(B, k) := \text{read SendFinalShare}(B, k) & \text{otherwise} \end{cases}$
- $\text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read SendFinalShare}(A, k) \text{ for } 0 \leq k < K$
- $\text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read SendFinalShare}(B, k) \text{ for } 0 \leq k < K$
- $\text{Out}(A, k) := x_A \leftarrow \text{SendFinalShare}(A, k); x_B \leftarrow \text{SendFinalShare}(B, k); \text{ret } x_A \oplus x_B \text{ for } 0 \leq k < K$
- $\text{Out}(B, k) := x_A \leftarrow \text{SendFinalShare}(A, k); x_B \leftarrow \text{SendFinalShare}(B, k); \text{ret } x_A \oplus x_B \text{ for } 0 \leq k < K$
- $\text{Out}(A, k)_{\text{adv}}^A := \text{read Out}(A, k) \text{ for } 0 \leq k < K$

8.4.1 Simplifying The Real Protocol: The Initial Phase

Our goal here is to eliminate the internal channels $\text{SendInputShare}(B, A, -)$ and $\text{SendInputShare}(A, B, -)$. We first replace any mention of these in channels $\text{InputShare}(B, B, i)$, $\text{SendInputShare}(B, A, i)_{\text{adv}}^A$, $\text{SendInputShare}(A, B, i)_{\text{adv}}^A$ by the corresponding channels $\text{InputShare}(B, A, -)$ and $\text{InputShare}(A, B, -)$:

- $\text{In}(A, i)_{\text{adv}}^A := \text{read } \text{In}(A, i) \text{ for } 0 \leq i < N$
- $\text{InRcvd}(B, i)_{\text{adv}}^B := x \leftarrow \text{In}(B, i); \text{ ret } \checkmark \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i) := x \leftarrow \text{In}(A, i); \text{ samp flip for } 0 \leq i < N$
- $\text{InputShare}(A, B, i) := \text{read } \text{SendInputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{InputShare}(B, A, i) := \text{read } \text{SendInputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(B, B, i) := x_A \leftarrow \text{InputShare}(A, B, i); x \leftarrow \text{In}(B, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); x \leftarrow \text{In}(A, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i) := x \leftarrow \text{In}(B, i); \text{ samp flip for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i)_{\text{adv}}^A := \text{read } \text{InputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i) \text{ for } 0 \leq i < M$

Now the only place where the channels $\text{SendInputShare}(B, A, -)$ and $\text{SendInputShare}(A, B, -)$ show up is in the very channels $\text{InputShare}(B, A, -)$ and $\text{InputShare}(A, B, -)$, respectively. So we can fold them in:

- $\text{In}(A, i)_{\text{adv}}^A := \text{read } \text{In}(A, i) \text{ for } 0 \leq i < N$
- $\text{InRcvd}(B, i)_{\text{adv}}^B := x \leftarrow \text{In}(B, i); \text{ ret } \checkmark \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i) := x \leftarrow \text{In}(A, i); \text{ samp flip for } 0 \leq i < N$
- $\text{InputShare}(A, B, i) := x \leftarrow \text{In}(B, i); \text{ samp flip for } 0 \leq i < M$
- $\text{InputShare}(B, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); x \leftarrow \text{In}(A, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < N$
- $\text{InputShare}(B, B, i) := x_A \leftarrow \text{InputShare}(A, B, i); x \leftarrow \text{In}(B, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i)_{\text{adv}}^A := \text{read } \text{InputShare}(B, A, i) \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i) \text{ for } 0 \leq i < M$

8.4.2 Simplifying The Real Protocol: The Inductive Stage

Our next order of business is to eliminate all channels interacting with the OT functionality. In the case of *input*-, *not*-, and *xor* gates, the OT channels are vacuous and only appear in the corresponding leakage channels. The leakage channels themselves are therefore vacuous: in the presence of

- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, i) := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, i),$

the two channel definitions

- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, i)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, i),$ and
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, i)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, i)_{\text{adv}}^{\text{ot}}$

are equivalent. Similarly, in the presence of

- $\text{OTChoice}(\mathbf{B}, \mathbf{A}, K, j) := \text{read OTChoice}(\mathbf{B}, \mathbf{A}, K, j),$

the two channel definitions

- $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, K, j)_{\text{adv}}^{\text{ot}} := c_j \leftarrow \text{OTChoice}(\mathbf{B}, \mathbf{A}, K, j); \text{ret } \checkmark,$ and
- $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, K, j)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, K, j)_{\text{adv}}^{\text{ot}}$

are equivalent. In the case of an *and* gate, we start by eliminating any mention of the OT channels from the leakage channels. By substituting the channels $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, -)$ into the channels $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, -)_{\text{adv}}^{\text{ot}}$, we obtain

- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); \text{ret } b_A$
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); \text{ret } b_A \oplus x_A$
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); \text{ret } b_A \oplus y_A$
- $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); \text{ret } b_A \oplus x_A \oplus y_A$

By substituting the channels $\text{OTChoice}(\mathbf{B}, \mathbf{A}, K, -)$ into the channels $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, K, -)_{\text{adv}}^{\text{ot}}$, we get

- $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, K, 0)_{\text{adv}}^{\text{ot}} := x_B \leftarrow \text{Share}(\mathbf{B}, k); \text{ret } \checkmark$
- $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, K, 1)_{\text{adv}}^{\text{ot}} := y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } \checkmark$

Substituting the channels $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, -)$ and $\text{OTChoice}(\mathbf{B}, \mathbf{A}, K, -)$ into $\text{OTOut}(\mathbf{B}, \mathbf{A}, K)$ yields

- $\text{OTOut}(\mathbf{B}, \mathbf{A}, K) := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{if } x_B \text{ then (if } y_B \text{ then ret } b_A \oplus x_A \oplus y_A \text{ else ret } b_A \oplus y_A) \text{ else (if } y_B \text{ then ret } b_A \oplus x_A \text{ else ret } b_A)$

The above is just a fancy way of saying the following:

- $\text{OTOut}(\mathbf{B}, \mathbf{A}, K) := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$

Substituting this new definition of $\text{OTOut}(K)$ into the channel $\text{OTBit}(\mathbf{B}, \mathbf{A}, K)$ yields

- $\text{OTBit}(\mathbf{B}, \mathbf{A}, K) := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$

Summarizing, we can rewrite the inductive part of the real protocol as follows:

- $\text{Real}(\epsilon, 0)$ is the protocol 0
- $\text{Real}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(\mathbf{A}, \mathbf{B}, K) := \text{read OTBit}(\mathbf{A}, \mathbf{B}, K)$

- $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
- $\begin{cases} \text{Share}(A, K) := \text{read InputShare}(A, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(A, K) := \text{read InputShare}(A, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\begin{cases} \text{Share}(B, K) := \text{read InputShare}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(B, K) := \text{read InputShare}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
- $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
- $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
- $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
- $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
- $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
- $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
- $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Real}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(A, K) := \text{read Share}(A, k)$
 - $\text{Share}(B, K) := x_B \leftarrow \text{Share}(B, k); \text{ret } \neg x_B$
 - $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$

- $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Real}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(A, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } x_A \oplus y_A$
 - $\text{Share}(B, K) := x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } x_B \oplus y_B$
 - $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Real}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Real}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{samp flip}$
 - $\text{OTBit}(B, A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k);$
 $y_B \leftarrow \text{Share}(B, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$
 - $\text{Share}(A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } (x_A * y_A) \oplus b_A$
 - $\text{Share}(B, K) := b_B \leftarrow \text{OTBit}(B, A, K); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$
 - $\text{OTMsg}(A, B, K, 0) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
 - $\text{OTMsg}(A, B, K, 1) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
 - $\text{OTMsg}(A, B, K, 2) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
 - $\text{OTMsg}(A, B, K, 3) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
 - $\text{OTChoice}(B, A, K, 0) := \text{read Share}(B, k)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read Share}(B, l)$

- $\text{OTOut}(B, A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k);$
 $y_B \leftarrow \text{Share}(B, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$
- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
- $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
- $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
- $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := x_B \leftarrow \text{Share}(B, k); \text{ret } \checkmark$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := y_B \leftarrow \text{Share}(B, l); \text{ret } \checkmark$

We can now split the real part of the protocol into four parts, each defined by induction on the circuit. The first part $\text{Alice}(C, K)$ defines the channels that can be seen as comprising Alice's part of the computation, $\text{OTBit}(A, B, -)$ and $\text{Share}(A, -)$:

- $\text{Alice}(\epsilon, 0)$ is the protocol 0
- $\text{Alice}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Alice}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\begin{cases} \text{Share}(A, K) := \text{read InputShare}(A, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(A, K) := \text{read InputShare}(A, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{Alice}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Alice}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K) := \text{read Share}(A, k)$
- $\text{Alice}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Alice}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } x_A \oplus y_A$
- $\text{Alice}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Alice}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{samp flip}$
 - $\text{Share}(A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } (x_A * y_A) \oplus b_A$

Analogously, the part $\text{Bob}(C, K)$ defines the channels that can be seen as comprising Bob's part of the computation, $\text{OTBit}(B, A, -)$ and $\text{Share}(B, -)$:

- $\text{Bob}(\epsilon, 0)$ is the protocol 0
- $\text{Bob}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\begin{cases} \text{Share}(B, K) := \text{read InputShare}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(B, K) := \text{read InputShare}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{Bob}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$

- $\text{Share}(\mathbf{B}, K) := x_B \leftarrow \text{Share}(\mathbf{B}, k); \text{ret } \neg x_B$
- $\text{Bob}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(\mathbf{B}, \mathbf{A}, K) := \text{read OTBit}(\mathbf{B}, \mathbf{A}, K)$
 - $\text{Share}(\mathbf{B}, K) := x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } x_B \oplus y_B$
- $\text{Bob}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(\mathbf{B}, \mathbf{A}, K) := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$
 - $\text{Share}(\mathbf{B}, K) := b_B \leftarrow \text{OTBit}(\mathbf{B}, \mathbf{A}, K); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } b_B \oplus (x_B * y_B)$

The third part $\text{Adv}(C, K)$ defines all the leakage channels intended for the adversary:

- $\text{Adv}(\epsilon, 0)$ is the protocol 0
- $\text{Adv}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(\mathbf{A}, \mathbf{B}, K)_{\text{adv}}^{\mathbf{A}} := \text{read OTBit}(\mathbf{A}, \mathbf{B}, K)_{\text{adv}}^{\mathbf{A}}$
 - $\text{Share}(\mathbf{A}, K)_{\text{adv}}^{\mathbf{A}} := \text{read Share}(\mathbf{A}, K)$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(\mathbf{A}, \mathbf{B}, K)_{\text{adv}}^{\mathbf{A}} := \text{read OTBit}(\mathbf{A}, \mathbf{B}, K)_{\text{adv}}^{\mathbf{A}}$
 - $\text{Share}(\mathbf{A}, K)_{\text{adv}}^{\mathbf{A}} := \text{read Share}(\mathbf{A}, K)$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(\mathbf{A}, \mathbf{B}, K)_{\text{adv}}^{\mathbf{A}} := \text{read OTBit}(\mathbf{A}, \mathbf{B}, K)_{\text{adv}}^{\mathbf{A}}$
 - $\text{Share}(\mathbf{A}, K)_{\text{adv}}^{\mathbf{A}} := \text{read Share}(\mathbf{A}, K)$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(\mathbf{A}, \mathbf{B}, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(\mathbf{B}, \mathbf{A}, k, 1)_{\text{adv}}^{\text{ot}}$

- $\text{Adv}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
 - $\text{OTChoiceRcvd}(B, A, k, 0)_{\text{adv}}^{\text{ot}} := x_B \leftarrow \text{Share}(B, k); \text{ret } \checkmark$
 - $\text{OTChoiceRcvd}(B, A, k, 1)_{\text{adv}}^{\text{ot}} := y_B \leftarrow \text{Share}(B, l); \text{ret } \checkmark$

Finally, $\text{part 1OutOf4OT}(C, K)$ defines the channels intended for communication with the OT functionality:

- $\text{1OutOf4OT}(\epsilon, 0)$ is the protocol 0
- $\text{1OutOf4OT}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{1OutOf4OT}(C, K)$ with the protocol
 - $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2); m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
 if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
- $\text{1OutOf4OT}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{1OutOf4OT}(C, K)$ with the protocol
 - $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$
 - $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2); m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
 if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
- $\text{1OutOf4OT}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{1OutOf4OT}(C, K)$ with the protocol
 - $\text{OTMsg}(A, B, K, 0) := \text{read OTMsg}(A, B, K, 0)$
 - $\text{OTMsg}(A, B, K, 1) := \text{read OTMsg}(A, B, K, 1)$
 - $\text{OTMsg}(A, B, K, 2) := \text{read OTMsg}(A, B, K, 2)$
 - $\text{OTMsg}(A, B, K, 3) := \text{read OTMsg}(A, B, K, 3)$
 - $\text{OTChoice}(B, A, K, 0) := \text{read OTChoice}(B, A, K, 0)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read OTChoice}(B, A, K, 1)$

- $\text{OTOut}(B, A, K) := m_0 \leftarrow \text{OTMsg}(A, B, K, 0); m_1 \leftarrow \text{OTMsg}(A, B, K, 1); m_2 \leftarrow \text{OTMsg}(A, B, K, 2);$
 $m_3 \leftarrow \text{OTMsg}(A, B, K, 3); c_0 \leftarrow \text{OTChoice}(B, A, K, 0); c_1 \leftarrow \text{OTChoice}(B, A, K, 1);$
if c_0 then (if c_1 then ret m_3 else ret m_2) else (if c_1 then ret m_1 else ret m_0)
- $1\text{OutOf4OT}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $1\text{OutOf4OT}(C, K)$ with the protocol
 - $\text{OTMsg}(A, B, K, 0) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
 - $\text{OTMsg}(A, B, K, 1) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
 - $\text{OTMsg}(A, B, K, 2) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
 - $\text{OTMsg}(A, B, K, 3) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
 - $\text{OTChoice}(B, A, K, 0) := \text{read Share}(B, k)$
 - $\text{OTChoice}(B, A, K, 1) := \text{read Share}(B, l)$
 - $\text{OTOut}(B, A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k);$
 $y_B \leftarrow \text{Share}(B, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$

We notice that after the earlier simplification, none of the channels defined by $1\text{OutOf4OT}(C, K)$ are utilized anywhere outside of $1\text{OutOf4OT}(C, K)$, and as such we may discard this protocol fragment entirely.

8.4.3 Simplifying The Real Protocol: The Final Stage

Our goal here is to eliminate the internal channels $\text{SendFinalShare}(A, -)$ and $\text{SendFinalShare}(B, -)$. If k is an output wire, this is a simple substitution. Otherwise, the channels $\text{SendFinalShare}(A, k)$ and $\text{SendFinalShare}(B, k)$ diverge, and so do channels $\text{SendFinalShare}(A, k)_{\text{adv}}^A$, $\text{SendFinalShare}(B, k)_{\text{adv}}^A$ and $\text{Out}(A, k)$, $\text{Out}(B, k)$:

- $\begin{cases} \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read Share}(A, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read SendFinalShare}(A, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read Share}(B, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read SendFinalShare}(B, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(A, k) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); \text{ret } x_A \oplus x_B & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(A, k) := \text{read Out}(A, k) & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(B, k) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); \text{ret } x_A \oplus x_B & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(B, k) := \text{read Out}(B, k) & \text{otherwise} \end{cases}$
- $\text{Out}(A, k)_{\text{adv}}^A := \text{read Out}(A, k)$ for $0 \leq k < K$

8.4.4 The Timing of Shares

Since the simulator does not have access to the value of Bob's inputs, any dependency on these needs to be eliminated. And since the value of Bob's shares depends on the value of his inputs, the shares themselves need to be eliminated. Upon examining the inductive part of the real protocol, we see that the only place where we depend on Bob's shares is in $\text{Adv}(C, K)$, when we leak the timing of Bob's messages to the OT functionality in the case of an *and* gate, *i.e.*, in the channels $\text{OTChoiceRcvd}(B, A, -, -)_{\text{adv}}^{\text{ot}}$. But even in this case, the actual *value* of Bob's shares is immaterial - it is only the timing information that matters. To this end, we introduce new internal channels

- $\text{InOk}(A, i) := x \leftarrow \text{In}(A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InOk}(B, i) := x \leftarrow \text{In}(B, i); \text{ret } \checkmark$ for $0 \leq i < M$
- $\text{InputShareOk}(A, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InputShareOk}(A, B, i) := x_A \leftarrow \text{InputShare}(A, B, i); \text{ret } \checkmark$ for $0 \leq i < M$

- $\text{InputShareOk}(B, A, i) := x_B \leftarrow \text{InputShare}(B, A, i)$; ret \checkmark for $0 \leq i < N$
- $\text{InputShareOk}(B, B, i) := x_B \leftarrow \text{InputShare}(B, B, i)$; ret \checkmark for $0 \leq i < M$
- $\text{OTBitOk}(A, B, k) := b_A \leftarrow \text{OTBitOk}(A, B, k)$; ret \checkmark for $0 \leq k < K$
- $\text{OTBitOk}(B, A, k) := b_B \leftarrow \text{OTBitOk}(B, A, k)$; ret \checkmark for $0 \leq k < K$
- $\text{ShareOk}(A, k) := x_A \leftarrow \text{Share}(A, k)$; ret \checkmark for $0 \leq k < K$
- $\text{ShareOk}(B, k) := x_B \leftarrow \text{Share}(B, k)$; ret \checkmark for $0 \leq k < K$

to record the relevant timing information. In the presence of these channels, we may rewrite the protocol $\text{Adv}(C, K)$ so that no explicit reference to the value of Bob's shares occurs:

- $\text{Adv}(\epsilon, 0)$ is the protocol 0
- $\text{Adv}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$

- $\text{Adv}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read ShareOk}(B, k)$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read ShareOk}(B, l)$

By design, Alice's and Bob's respective shares of each wire add up to the actual value carried by the wire. If we knew the latter, let's say by inductively computing the circuit the same way the ideal functionality does, we could get rid of Bob's shares entirely by replacing them with the sum of Alice's shares and the corresponding values. For this to work, however, we first need to arrange the timing so that Bob's computation of each wire happens after Alice's. To this end, we start by amending Bob's shares with a gratuitous dependency on timing:

- $\text{Bob}(\epsilon, 0)$ is the protocol 0
- $\text{Bob}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\begin{cases} \text{Share}(B, K) := _ \leftarrow \text{InputShareOk}(B, A, i); \text{read InputShare}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(B, K) := _ \leftarrow \text{InputShareOk}(B, B, i); \text{read InputShare}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{Bob}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(B, K) := _ \leftarrow \text{ShareOk}(B, k); x_B \leftarrow \text{Share}(B, k); \text{ret } \neg x_B$
- $\text{Bob}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(B, K) := _ \leftarrow \text{ShareOk}(B, k); x_B \leftarrow \text{Share}(B, k); _ \leftarrow \text{ShareOk}(B, l); y_B \leftarrow \text{Share}(B, l); \text{ret } x_B \oplus y_B$
- $\text{Bob}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$
 - $\text{Share}(B, K) := _ \leftarrow \text{OTBitOk}(B, A, K); b_B \leftarrow \text{OTBit}(B, A, K); _ \leftarrow \text{ShareOk}(B, k); x_B \leftarrow \text{Share}(B, k); _ \leftarrow \text{ShareOk}(B, l); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$

Clearly, we can make the timing of the shares independent of their actual value; this was the point of introducing the timing of shares in the first place. We can define the channels

- $\text{OTBitOk}(B, A, k) := b_B \leftarrow \text{OTBit}(B, A, k); \text{ret } \checkmark$ for $0 \leq k < K$
- $\text{ShareOk}(B, k) := x_B \leftarrow \text{Share}(B, k); \text{ret } \checkmark$ for $0 \leq k < K$

equivalently by induction:

- $\text{BobOk}(\epsilon, 0)$ is the protocol 0
- $\text{BobOk}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{BobOk}(C, K)$ with the protocol

- $\text{OTBitOk}(B, A, K) := \text{read OTBitOk}(B, A, K)$
- $\begin{cases} \text{ShareOk}(B, K) := \text{read InputShareOk}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{ShareOk}(B, K) := \text{read InputShareOk}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{BobOk}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{BobOk}(C, K)$ with the protocol
 - $\text{OTBitOk}(B, A, K) := \text{read OTBitOk}(B, A, K)$
 - $\text{ShareOk}(B, K) := \text{read ShareOk}(B, k)$
- $\text{BobOk}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{BobOk}(C, K)$ with the protocol
 - $\text{OTBitOk}(B, A, K) := \text{read OTBitOk}(B, A, K)$
 - $\text{ShareOk}(B, K) := _ \leftarrow \text{ShareOk}(B, k); _ \leftarrow \text{ShareOk}(B, l); \text{ret } \checkmark$
- $\text{BobOk}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{BobOk}(C, K)$ with the protocol
 - $\text{OTBitOk}(B, A, K) := _ \leftarrow \text{OTBitOk}(A, B, K); _ \leftarrow \text{ShareOk}(A, k); _ \leftarrow \text{ShareOk}(A, l);$
 $_ \leftarrow \text{ShareOk}(B, k); _ \leftarrow \text{ShareOk}(B, l); \text{ret } \checkmark$
 - $\text{ShareOk}(B, K) := _ \leftarrow \text{OTBitOk}(B, A, K); _ \leftarrow \text{ShareOk}(B, k); _ \leftarrow \text{ShareOk}(B, l); \text{ret } \checkmark$

We can likewise express the channels

- $\text{InputShareOk}(B, A, i) := x_B \leftarrow \text{InputShare}(B, A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InputShareOk}(B, B, i) := x_B \leftarrow \text{InputShare}(B, B, i); \text{ret } \checkmark$ for $0 \leq i < M$

explicitly as

- $\text{InputShareOk}(B, A, i) := _ \leftarrow \text{InputShareOk}(A, A, i); _ \leftarrow \text{InOk}(A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InputShareOk}(B, B, i) := _ \leftarrow \text{InputShareOk}(A, B, i); _ \leftarrow \text{InOk}(B, i); \text{ret } \checkmark$ for $0 \leq i < M$

We now carry out the same procedure for Alice. We characterize the channels

- $\text{OTBitOk}(A, B, k) := b_A \leftarrow \text{OTBitOk}(A, B, k); \text{ret } \checkmark$ for $0 \leq k < K$
- $\text{ShareOk}(A, k) := x_A \leftarrow \text{Share}(A, k); \text{ret } \checkmark$ for $0 \leq k < K$

by induction as follows:

- $\text{AliceOk}(\epsilon, 0)$ is the protocol 0
- $\text{AliceOk}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{AliceOk}(C, K)$ with the protocol
 - $\text{OTBitOk}(A, B, K) := \text{read OTBitOk}(A, B, K)$
 - $\begin{cases} \text{ShareOk}(A, K) := \text{read InputShareOk}(A, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{ShareOk}(A, K) := \text{read InputShareOk}(A, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{AliceOk}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{AliceOk}(C, K)$ with the protocol
 - $\text{OTBitOk}(A, B, K) := \text{read OTBitOk}(A, B, K)$
 - $\text{ShareOk}(A, K) := \text{read ShareOk}(A, k)$
- $\text{AliceOk}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{AliceOk}(C, K)$ with the protocol
 - $\text{OTBitOk}(A, B, K) := \text{read OTBitOk}(A, B, K)$
 - $\text{ShareOk}(A, K) := _ \leftarrow \text{ShareOk}(A, k); _ \leftarrow \text{ShareOk}(A, l); \text{ret } \checkmark$
- $\text{AliceOk}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{AliceOk}(C, K)$ with the protocol

- $\text{OTBitOk}(A, B, K) := _ \leftarrow \text{ShareOk}(A, k); _ \leftarrow \text{ShareOk}(A, l); \text{ret } \checkmark$
- $\text{ShareOk}(A, K) := _ \leftarrow \text{OTBitOk}(A, B, K); _ \leftarrow \text{ShareOk}(A, k); _ \leftarrow \text{ShareOk}(A, l); \text{ret } \checkmark$

We can likewise express the channels

- $\text{InputShareOk}(A, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InputShareOk}(A, B, i) := x_A \leftarrow \text{InputShare}(A, B, i); \text{ret } \checkmark$ for $0 \leq i < M$

explicitly as

- $\text{InputShareOk}(A, A, i) := \text{read InOk}(A, i)$ for $0 \leq i < N$
- $\text{InputShareOk}(A, B, i) := \text{read InOk}(B, i)$ for $0 \leq i < M$

The timing of Bob's and Alice's shares is now easily seen to be the same: specifically, we can write the channels

- $\text{InputShareOk}(B, A, i) := _ \leftarrow \text{InputShareOk}(A, A, i); _ \leftarrow \text{InOk}(A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InputShareOk}(B, B, i) := _ \leftarrow \text{InputShareOk}(A, B, i); _ \leftarrow \text{InOk}(B, i); \text{ret } \checkmark$ for $0 \leq i < M$

equivalently as

- $\text{InputShareOk}(B, A, i) := \text{read InputShareOk}(A, A, i)$ for $0 \leq i < N$
- $\text{InputShareOk}(B, B, i) := \text{read InputShareOk}(A, B, i)$ for $0 \leq i < M$

and express the inductively defined protocol fragment $\text{BobOk}(C, K)$ simply as

- $\text{OTBitOk}(B, A, k) := \text{read OTBitOk}(A, B, k)$ for $0 \leq k < K$
- $\text{ShareOk}(B, k) := \text{read ShareOk}(A, k)$ for $0 \leq k < K$

The closed-form expression for the timing of Alice's shares is more useful, so we revert the channels

- $\text{InputShareOk}(A, A, i) := \text{read InOk}(A, i)$ for $0 \leq i < N$
- $\text{InputShareOk}(A, B, i) := \text{read InOk}(B, i)$ for $0 \leq i < M$

back to

- $\text{InputShareOk}(A, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); \text{ret } \checkmark$ for $0 \leq i < N$
- $\text{InputShareOk}(A, B, i) := x_A \leftarrow \text{InputShare}(A, B, i); \text{ret } \checkmark$ for $0 \leq i < M$

and revert the inductively defined protocol fragment $\text{AliceOk}(C, K)$ back to

- $\text{OTBitOk}(A, B, k) := b_A \leftarrow \text{OTBit}(A, B, k); \text{ret } \checkmark$ for $0 \leq k < K$
- $\text{ShareOk}(A, k) := x_A \leftarrow \text{Share}(A, k); \text{ret } \checkmark$

In the presence of these latest definitions for timing, we can rewrite the timing dependency in the protocol $\text{Bob}(C, K)$ as follows:

- $\text{Bob}(\epsilon, 0)$ is the protocol 0
- $\text{Bob}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\begin{cases} \text{Share}(B, K) := x_A \leftarrow \text{InputShare}(A, A, i); \text{read InputShare}(B, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(B, K) := x_A \leftarrow \text{InputShare}(A, B, i); \text{read InputShare}(B, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
- $\text{Bob}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol

- $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
- $\text{Share}(B, K) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); \text{ret } \neg x_B$
- $\text{Bob}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
 - $\text{Share}(B, K) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); y_A \leftarrow \text{Share}(A, l); y_B \leftarrow \text{Share}(B, l); \text{ret } x_B \oplus y_B$
- $\text{Bob}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Bob}(C, K)$ with the protocol
 - $\text{OTBit}(B, A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$
 - $\text{Share}(B, K) := b_A \leftarrow \text{OTBit}(A, B, K); b_B \leftarrow \text{OTBit}(B, A, K); x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(A, l); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$

Finally, we can eliminate all references to timing channels from the protocol fragment $\text{Adv}(C, K)$, specifically from the channels $\text{OTChoiceRcvd}(B, A, -, -)_{\text{adv}}^{\text{ot}}$:

- $\text{Adv}(\epsilon, 0)$ is the protocol 0
- $\text{Adv}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$

- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Adv}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Adv}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := _ \leftarrow \text{Share}(A, k); \text{ret } \checkmark$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := _ \leftarrow \text{Share}(A, l); \text{ret } \checkmark$

At this point the timing channels are unused and we can safely discard them.

8.4.5 The Sum Of Shares

As mentioned before, Alice's and Bob's respective shares of each wire sum up to the actual value carried by the wire. To make this invariant explicit, we add new internal channels

- $\text{Wire}(k) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); \text{ret } x_A \oplus x_B$ for $0 \leq k < K$

that record the sum of shares. In the presence of the above, we can rewrite the final part of the real protocol as

- $\begin{cases} \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read Share}(A, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read SendFinalShare}(A, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read Share}(B, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read SendFinalShare}(B, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(A, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(A, k) := \text{read Out}(A, k) & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(B, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(B, k) := \text{read Out}(B, k) & \text{otherwise} \end{cases}$
- $\text{Out}(A, k)_{\text{adv}}^A := \text{read Out}(A, k)$ for $0 \leq k < K$

Right now, Bob's shares are computed inductively and the channels $\text{Wire}(-)$ have a closed form. By induction on circuits, we can flip this around: we characterize the channels

- $\text{Wire}(k) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); \text{ret } x_A \oplus x_B$ for $0 \leq k < K$

inductively as the protocol $\text{Wires}(C, K)$ that's part of the ideal functionality. At the same time, we split the protocol $\text{B}(C, K)$ into a closed-form part

- $\text{Share}(B, k) := x_A \leftarrow \text{Share}(A, k); x \leftarrow \text{Wire}(k); \text{ret } x_A \oplus x$ for $0 \leq k < K$

and an inductive part $\text{BobOTBit}(C, K)$:

- $\text{BobOTBit}(\epsilon, 0)$ is the protocol 0

- $\text{BobOTBit}(C; \text{input-gate}(i), K+1)$ is the composition of the protocol $\text{BobOTBit}(C, K)$ with the single-reaction protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
- $\text{BobOTBit}(C; \text{not-gate}(k), K+1)$ is the composition of the protocol $\text{BobOTBit}(C, K)$ with the single-reaction protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
- $\text{BobOTBit}(C; \text{xor-gate}(k, l), K+1)$ is the composition of the protocol $\text{BobOTBit}(C, K)$ with the single-reaction protocol
 - $\text{OTBit}(B, A, K) := \text{read OTBit}(B, A, K)$
- $\text{BobOTBit}(C; \text{and-gate}(k, l), K+1)$ is the composition of the protocol $\text{BobOTBit}(C, K)$ with the single-reaction protocol
 - $\text{OTBit}(B, A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_A \oplus (x_A * y_B) \oplus (x_B * y_A)$

To see why this works, we consider each gate in turn.

- In the case of an *input* gate, let us assume i is an input of Alice; the case for Bob is entirely analogous. We start by substituting the channels $\text{Share}(A, K)$ and $\text{Share}(B, K)$ into the channel
 - $\text{Wire}(K) := x_A \leftarrow \text{Share}(A, K); x_B \leftarrow \text{Share}(B, K); \text{ret } x_A \oplus x_B$, yielding
 - $\text{Wire}(K) := x_A \leftarrow \text{InputShare}(A, A, i); x_B \leftarrow \text{InputShare}(B, A, i); \text{ret } x_A \oplus x_B$

Substituting this new definition of $\text{Wire}(K)$ along with the channel $\text{Share}(A, K)$ into the channel

- $\text{Share}(B, K) := x_A \leftarrow \text{Share}(A, K); x \leftarrow \text{Wire}(K); \text{ret } x_A \oplus x$ yields
- $\text{Share}(B, K) := x_A \leftarrow \text{InputShare}(A, A, i); x_B \leftarrow \text{InputShare}(B, A, i); \text{ret } x_A \oplus (x_A \oplus x_B)$

After canceling out the two applications of \oplus and simplifying, we get

- $\text{Share}(B, K) := x_A \leftarrow \text{InputShare}(A, A, i); \text{read InputShare}(B, A, i)$

which is precisely the desired inductive formulation of $\text{Share}(B, K)$.

We continue to work on the channel $\text{Wire}(K)$. A further substitution of the channel $\text{InputShare}(B, A, i)$ into the channel $\text{Wire}(K)$ yields

- $\text{Wire}(K) := x_A \leftarrow \text{InputShare}(A, A, i); x \leftarrow \text{In}(A, i); \text{ret } x_A \oplus (x_A \oplus x)$

After canceling out the two applications of \oplus and simplifying, we get

- $\text{Wire}(K) := x_A \leftarrow \text{InputShare}(A, A, i); \text{read In}(A, i)$

Dropping the gratuitous dependency on the channel $\text{InputShare}(A, A, i)$ yields

- $\text{Wire}(K) := \text{read In}(A, i)$

which is precisely the desired inductive formulation of $\text{Wire}(K)$.

- In the case of a *not* gate, we substitute the channels $\text{Share}(A, K)$ and $\text{Share}(B, K)$ into the channel
 - $\text{Wire}(K) := x_A \leftarrow \text{Share}(A, K); x_B \leftarrow \text{Share}(B, K); \text{ret } x_A \oplus x_B$ to obtain
 - $\text{Wire}(K) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); \text{ret } x_A \oplus (\neg x_B)$

Substituting this new definition of $\text{Wire}(K)$ along with the channel $\text{Share}(A, K)$ into the channel

- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, K); x \leftarrow \text{Wire}(K); \text{ret } x_A \oplus x$ yields
- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); x_B \leftarrow \text{Share}(\mathbf{B}, k); \text{ret } x_A \oplus (x_A \oplus (\neg x_B))$

After canceling out the two applications of \oplus , we get

- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); x_B \leftarrow \text{Share}(\mathbf{B}, k); \text{ret } \neg x_B$

which is precisely the desired inductive formulation of $\text{Share}(\mathbf{B}, K)$.

We continue to work on the channel $\text{Wire}(K)$. The negation can be brought to the top level:

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); x_B \leftarrow \text{Share}(\mathbf{B}, k); \text{ret } \neg(x_A \oplus x_B)$

This is precisely what we get when we substitute the channel $\text{Wire}(k)$ into the channel

- $\text{Wire}(K) := x \leftarrow \text{Wire}(k); \text{ret } \neg x$

using our inductive hypothesis, thereby yielding the desired inductive formulation of $\text{Wire}(K)$.

- In the case of an *xor* gate, we substitute the channels $\text{Share}(\mathbf{A}, K)$ and $\text{Share}(\mathbf{B}, K)$ into the channel

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(\mathbf{A}, K); x_B \leftarrow \text{Share}(\mathbf{B}, K); \text{ret } x_A \oplus x_B$ to obtain
- $\text{Wire}(K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l);$
 $\text{ret } (x_A \oplus y_A) \oplus (x_B \oplus y_B)$

Substituting this new definition of $\text{Wire}(K)$ along with the channel $\text{Share}(\mathbf{A}, K)$ into the channel

- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, K); x \leftarrow \text{Wire}(K); \text{ret } x_A \oplus x$ yields
- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l);$
 $\text{ret } (x_A \oplus y_A) \oplus (x_A \oplus y_A) \oplus (x_B \oplus y_B)$

After canceling out the two top-level applications of \oplus , we get

- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } x_B \oplus y_B$

After rearranging, the above becomes

- $\text{Share}(\mathbf{B}, K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } x_B \oplus y_B$

which is precisely the desired inductive formulation of $\text{Share}(\mathbf{B}, K)$.

We continue to work on the channel $\text{Wire}(K)$. Since \oplus is commutative, we can write the channel Wire as

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l);$
 $\text{ret } (x_A \oplus x_B) \oplus (y_A \oplus y_B)$

After rearranging, the above becomes

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(\mathbf{A}, k); x_B \leftarrow \text{Share}(\mathbf{B}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); y_B \leftarrow \text{Share}(\mathbf{B}, l);$
 $\text{ret } (x_A \oplus x_B) \oplus (y_A \oplus y_B)$

This is precisely what we get when we substitute the channels $\text{Wire}(k)$ and $\text{Wire}(l)$ into the channel

- $\text{Wire}(K) := x \leftarrow \text{Wire}(k); y \leftarrow \text{Wire}(l); \text{ret } x \oplus y$

using our inductive hypothesis twice, thereby yielding the desired inductive formulation of $\text{Wire}(K)$.

- In the case of an *and* gate, we again start by substituting the channels $\text{Share}(\mathbf{A}, K)$ and $\text{Share}(\mathbf{B}, K)$ into the channel

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(\mathbf{A}, K); x_B \leftarrow \text{Share}(\mathbf{B}, K); \text{ret } x_A \oplus x_B$ to obtain
- $\text{Wire}(K) := b_A \leftarrow \text{OTBit}(\mathbf{A}, \mathbf{B}, K); x_A \leftarrow \text{Share}(\mathbf{A}, k); y_A \leftarrow \text{Share}(\mathbf{A}, l); b_B \leftarrow \text{OTBit}(\mathbf{B}, \mathbf{A}, K);$
 $x_B \leftarrow \text{Share}(\mathbf{B}, k); y_B \leftarrow \text{Share}(\mathbf{B}, l); \text{ret } ((x_A * y_A) \oplus b_A) \oplus (b_B \oplus (x_B * y_B))$

Substituting this new definition of $\text{Wire}(K)$ along with the channel $\text{Share}(A, K)$ into the channel

- $\text{Share}(B, K) := x_A \leftarrow \text{Share}(A, K); x \leftarrow \text{Wire}(K); \text{ret } x_A \oplus x$ yields
- $\text{Share}(B, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); b_B \leftarrow \text{OTBit}(B, A, K); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } ((x_A * y_A) \oplus b_A) \oplus ((x_A * y_A) \oplus b_A) \oplus (b_B \oplus (x_B * y_B))$

After canceling out the two top-level applications of \oplus we get

- $\text{Share}(B, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); b_B \leftarrow \text{OTBit}(B, A, K); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$

After rearranging, the above becomes

- $\text{Share}(B, K) := b_A \leftarrow \text{OTBit}(A, B, K); b_B \leftarrow \text{OTBit}(B, A, K); x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); y_A \leftarrow \text{Share}(A, l); y_B \leftarrow \text{Share}(B, l); \text{ret } b_B \oplus (x_B * y_B)$

which is precisely the desired inductive formulation of $\text{Share}(B, K)$.

We continue to work on the channel $\text{Wire}(K)$. A further substitution of the channel $\text{OTBit}(B, A, K)$ yields

- $\text{Wire}(K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } ((x_A * y_A) \oplus b_A) \oplus (b_A \oplus (x_A * y_B) \oplus (x_B * y_A) \oplus (x_B * y_B))$

or, reassociated,

- $\text{Wire}(K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } (x_A * y_A) \oplus (b_A \oplus b_A \oplus (x_A * y_B) \oplus (x_B * y_A)) \oplus (x_B * y_B)$

After canceling out the two applications of \oplus with b_A , we get

- $\text{Wire}(K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } (x_A * y_A) \oplus (x_A * y_B) \oplus (x_B * y_A) \oplus (x_B * y_B)$

Dropping the gratuitous dependency on $\text{OTBit}(A, B, K)$ yields

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } (x_A * y_A) \oplus (x_A * y_B) \oplus (x_B * y_A) \oplus (x_B * y_B)$

Applying distributivity yields

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); x_B \leftarrow \text{Share}(B, k); y_B \leftarrow \text{Share}(B, l); \text{ret } (x_A \oplus x_B) * (y_A \oplus y_B)$

After rearranging, the above becomes

- $\text{Wire}(K) := x_A \leftarrow \text{Share}(A, k); x_B \leftarrow \text{Share}(B, k); y_A \leftarrow \text{Share}(A, l); y_B \leftarrow \text{Share}(B, l); \text{ret } (x_A \oplus x_B) * (y_A \oplus y_B)$

This is precisely what we get when we substitute the channels $\text{Wire}(k)$ and $\text{Wire}(l)$ into the channel

- $\text{Wire}(K) := x \leftarrow \text{Wire}(k); y \leftarrow \text{Wire}(l); \text{ret } x * y$

using our inductive hypothesis twice, thereby yielding the desired inductive formulation of $\text{Wire}(K)$.

Since we have a closed form for computing Bob's shares, we can discard the protocol fragment $\text{BobOTBit}(C, K)$ entirely. Moreover, at this point the only places where we refer to Bob's side of the computation is when leaking Bob's initial and final shares, *i.e.*, in the channels $\text{SendInputShare}(B, A, -)_{\text{adv}}^A$ and $\text{SendFinalShare}(B, -)_{\text{adv}}^A$. This can be easily remedied by performing the appropriate substitutions. Substituting the channels $\text{InputShare}(B, A, -)$ into the channels $\text{SendInputShare}(B, A, -)_{\text{adv}}^A$ yields the following version of the initial part of the real protocol:

- $\text{In}(A, i)_{\text{adv}}^A := \text{read In}(A, i) \text{ for } 0 \leq i < N$

- $\text{InRcvd}(B, i)_{\text{adv}}^B := x \leftarrow \text{In}(B, i); \text{ ret } \checkmark \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i) := x \leftarrow \text{In}(A, i); \text{ samp flip for } 0 \leq i < N$
- $\text{InputShare}(A, B, i) := x \leftarrow \text{In}(B, i); \text{ samp flip for } 0 \leq i < M$
- $\text{InputShare}(B, A, i) := x_A \leftarrow \text{InputShare}(A, A, i); x \leftarrow \text{In}(A, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < N$
- $\text{InputShare}(B, B, i) := x_A \leftarrow \text{InputShare}(A, B, i); x \leftarrow \text{In}(B, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < M$
- $\text{InputShare}(A, A, i)_{\text{adv}}^A := \text{read InputShare}(A, A, i) \text{ for } 0 \leq i < N$
- $\text{InputShare}(A, B, i)_{\text{adv}}^A := \text{read InputShare}(A, B, i) \text{ for } 0 \leq i < M$
- $\text{SendInputShare}(B, A, i)_{\text{adv}}^A := x_A \leftarrow \text{InputShare}(A, A, i); x \leftarrow \text{In}(A, i); \text{ ret } x_A \oplus x \text{ for } 0 \leq i < N$
- $\text{SendInputShare}(A, B, i)_{\text{adv}}^A := \text{read InputShare}(A, B, i) \text{ for } 0 \leq i < M$

Similarly, substituting the channels

- $\text{Share}(B, k) := x_A \leftarrow \text{Share}(A, k); x \leftarrow \text{Wire}(k); \text{ ret } x_A \oplus x \text{ for } 0 \leq k < K$

into the channels $\text{SendFinalShare}(B, -)_{\text{adv}}^A$ yields the following version of the final part of the real protocol:

- $\begin{cases} \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read Share}(A, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read SendFinalShare}(A, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SendFinalShare}(B, k)_{\text{adv}}^A := x_A \leftarrow \text{Share}(A, k); x \leftarrow \text{Wire}(k); \text{ ret } x_A \oplus x & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read SendFinalShare}(B, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(A, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(A, k) := \text{read Out}(A, k) & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(B, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(B, k) := \text{read Out}(B, k) & \text{otherwise} \end{cases}$
- $\text{Out}(A, k)_{\text{adv}}^A := \text{read Out}(A, k) \text{ for } 0 \leq k < K$

At this point we can discard all the channels coming from Bob's side:

- $\text{InputShare}(B, A, i) \text{ for } 0 \leq i < N,$
- $\text{InputShare}(B, B, i) \text{ for } 0 \leq i < M,$ and
- $\text{Share}(B, k) \text{ for } 0 \leq k < K.$

This yields the final version of the real protocol.

8.5 The Simulator

The protocol $\text{Wire}(C, K)$ and the channels

- $\begin{cases} \text{Out}(A, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(A, k) := \text{read Out}(A, k) & \text{otherwise} \end{cases}$
- $\begin{cases} \text{Out}(B, k) := \text{read Wire}(k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{Out}(B, k) := \text{read Out}(B, k) & \text{otherwise} \end{cases}$

can now be separated out as coming from the functionality, and the remainder of the protocol is turned into a simulator. The simulator arises as a composition of an initial part, an inductive part, and a final part – all described below – followed by the hiding of the channels

- $\text{InputShare}(A, A, i)$ for $0 \leq i < N$,
- $\text{InputShare}(A, B, i)$ for $0 \leq i < M$,
- $\text{InputShare}(B, A, i)$ for $0 \leq i < N$,
- $\text{InputShare}(B, B, i)$ for $0 \leq i < M$,
- $\text{OTBit}(A, B, k)$ for $0 \leq k < K$,
- $\text{OTBit}(B, A, k)$ for $0 \leq k < K$,
- $\text{Share}(A, k)$ for $0 \leq k < K$, and
- $\text{Share}(B, k)$ for $0 \leq k < K$.

Plugging the simulator into the ideal functionality and substituting away the channels $\text{In}(A, -)_{\text{adv}}^{\text{id}}$, $\text{InRcvd}(B, -)_{\text{adv}}^{\text{id}}$, and $\text{Out}(A, -)_{\text{adv}}^{\text{id}}$ that originally served as a line of communication for the adversary yields the final version of the real protocol, as desired.

8.5.1 The Simulator: The Initial Phase

The code for the initial part of the simulator is as follows:

- $\text{In}(A, i)_{\text{adv}}^A := \text{read } \text{In}(A, i)_{\text{adv}}^{\text{id}}$ for $0 \leq i < N$
- $\text{InRcvd}(B, i)_{\text{adv}}^B := \text{read } \text{InRcvd}(B, i)_{\text{adv}}^{\text{id}}$ for $0 \leq i < M$
- $\text{InputShare}(A, A, i) := x \leftarrow \text{In}(A, i)_{\text{adv}}^{\text{id}}$; samp flip for $0 \leq i < N$
- $\text{InputShare}(A, B, i) := _ \leftarrow \text{InRcvd}(B, i)_{\text{adv}}^{\text{id}}$; samp flip for $0 \leq i < M$
- $\text{InputShare}(A, A, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, A, i)$ for $0 \leq i < N$
- $\text{InputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i)$ for $0 \leq i < M$
- $\text{SendInputShare}(B, A, i)_{\text{adv}}^A := x_A \leftarrow \text{InputShare}(A, A, i)$; $x \leftarrow \text{In}(A, i)_{\text{adv}}^{\text{id}}$; ret $x_A \oplus x$ for $0 \leq i < N$
- $\text{SendInputShare}(A, B, i)_{\text{adv}}^A := \text{read } \text{InputShare}(A, B, i)$ for $0 \leq i < M$

8.5.2 The Simulator: The Inductive Phase

The inductive part of the simulator $\text{Sim}(C, K)$ is the composition of the three protocols $\text{Alice}(C, K)$, $\text{Wires}(C, K)$, and $\text{Adv}(C, K)$:

- $\text{Sim}(\epsilon, 0)$ is the protocol 0
- $\text{Sim}(C; \text{input-gate}(i), K + 1)$ is the composition of the protocol $\text{Sim}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read } \text{OTBit}(A, B, K)$
 - $\begin{cases} \text{Share}(A, K) := \text{read } \text{InputShare}(A, A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Share}(A, K) := \text{read } \text{InputShare}(A, B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$
 - $\begin{cases} \text{Wire}(K) := \text{read } \text{In}(A, i) & \text{if } i \text{ is an input of Alice} \\ \text{Wire}(K) := \text{read } \text{In}(B, i) & \text{if } i \text{ is an input of Bob} \end{cases}$

- $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
- $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Sim}(C; \text{not-gate}(k), K + 1)$ is the composition of the protocol $\text{Sim}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K) := \text{read Share}(A, k)$
 - $\text{Wire}(K) := x \leftarrow \text{Wire}(k); \text{ret } \neg x$
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Sim}(C; \text{xor-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Sim}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := \text{read OTBit}(A, B, K)$
 - $\text{Share}(A, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } x_A \oplus y_A$
 - $\text{Wire}(K) := x \leftarrow \text{Wire}(k); y \leftarrow \text{Wire}(l); \text{ret } x \oplus y$
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)_{\text{adv}}^A$
 - $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
 - $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}}$
 - $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := \text{read OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}}$
 - $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := \text{read OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}}$
- $\text{Sim}(C; \text{and-gate}(k, l), K + 1)$ is the composition of the protocol $\text{Sim}(C, K)$ with the protocol
 - $\text{OTBit}(A, B, K) := x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{samp flip}$
 - $\text{Share}(A, K) := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } (x_A * y_A) \oplus b_A$
 - $\text{Wire}(K) := x \leftarrow \text{Wire}(k); y \leftarrow \text{Wire}(l); \text{ret } x * y$
 - $\text{OTBit}(A, B, K)_{\text{adv}}^A := \text{read OTBit}(A, B, K)$

- $\text{Share}(A, K)_{\text{adv}}^A := \text{read Share}(A, K)$
- $\text{OTMsg}(A, B, K, 0)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A$
- $\text{OTMsg}(A, B, K, 1)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A$
- $\text{OTMsg}(A, B, K, 2)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus y_A$
- $\text{OTMsg}(A, B, K, 3)_{\text{adv}}^{\text{ot}} := b_A \leftarrow \text{OTBit}(A, B, K); x_A \leftarrow \text{Share}(A, k); y_A \leftarrow \text{Share}(A, l); \text{ret } b_A \oplus x_A \oplus y_A$
- $\text{OTChoiceRcvd}(B, A, K, 0)_{\text{adv}}^{\text{ot}} := _ \leftarrow \text{Share}(A, k); \text{ret } \checkmark$
- $\text{OTChoiceRcvd}(B, A, K, 1)_{\text{adv}}^{\text{ot}} := _ \leftarrow \text{Share}(A, l); \text{ret } \checkmark$

8.5.3 The Simulator: The Final Phase

The code for the final part of the simulator is as follows:

- $\begin{cases} \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read Share}(A, k) & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(A, k)_{\text{adv}}^A := \text{read SendFinalShare}(A, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\begin{cases} \text{SendFinalShare}(B, k)_{\text{adv}}^A := x_A \leftarrow \text{Share}(A, k); x \leftarrow \text{Out}(A, k)_{\text{adv}}^{\text{id}}; \text{ret } x_A \oplus x & \text{if wire } 0 \leq k < K \text{ is output} \\ \text{SendFinalShare}(B, k)_{\text{adv}}^A := \text{read SendFinalShare}(B, k)_{\text{adv}}^A & \text{otherwise} \end{cases}$
- $\text{Out}(A, k)_{\text{adv}}^A := \text{read Out}(A, k)_{\text{adv}}^{\text{id}}$ for $0 \leq k < K$