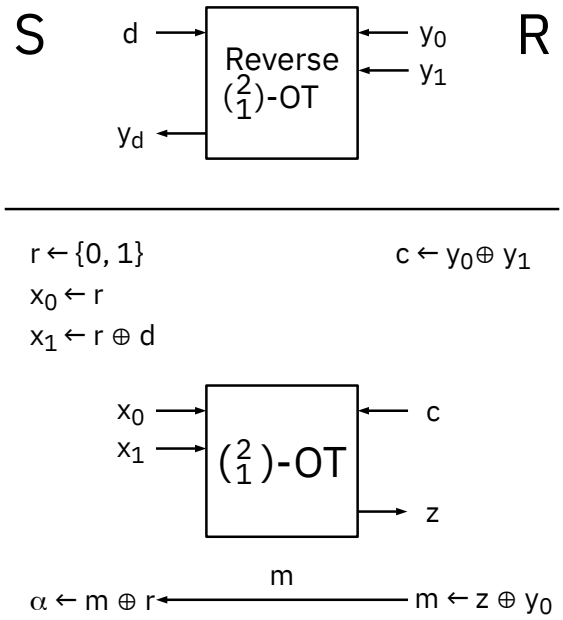
Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2021

Prof. Christian Cachin
Jovana Mićić

Exercise 8

8.1 Reversing oblivious transfer (4pt)

The direction of $\binom{2}{1}$-oblivious transfer of *bits* can be reversed. The following protocol realizes a *Reverse-*$\binom{2}{1}$-OT protocol for sending $y_0, y_1 \in \{0,1\}$ *from* R *to* S, such that S learns y_d for $d \in \{0,1\}$. It gains its security from a $\binom{2}{1}$-OT primitive for sending $x_0, x_1 \in \{0,1\}$ from S to R, such that R learns x_c for $c \in \{0,1\}$.



Recall the three properties of $\binom{2}{1}$-OT. Prove that the Reverse-$\binom{2}{1}$-OT is a secure OT protocol of bits from R to S, assuming that $\binom{2}{1}$-OT is a secure OT protocol of bits.

8.2 More efficient oblivious transfer (6pt)

The $\binom{2}{1}$-OT protocol for bit strings, implemented as shown in class using ElGamal encryption, incurs the following cost:

Computational complexity: Two public-key operations.

Latency: Three rounds, i.e., three message delays between S and R from the start to the end of the protocol.

Communication complexity: The total number of bits exchanged is $O(\ell + \lambda)$ for sending strings of length ℓ and with cryptographic parameters that can be represented using λ bits (i.e., elements of G take λ bits).

For any $n = 2^k$, develop a protocol that implements $\binom{n}{1}$-OT and uses k instances of $\binom{2}{1}$-OT. You may use additional cryptographic primitives and messages. Calculate its cost.