Commitment Scheme

Problem

Alice and Bob are going out on a date. Alice wants to see one movie and Bob wants to see another. They decide to flip a random coin to choose the movie. If the coin comes up “heads” they will go to Alice’s choice; otherwise, they will go to Bob’s choice. When Alice and Bob are in close proximity this is easy: one of them, say Bob, flips a coin and they both verify the result. When they are far apart and are speaking on the phone this is harder. Bob can flip a coin on his side and tell Alice the result, but Alice has no reason to believe the outcome.

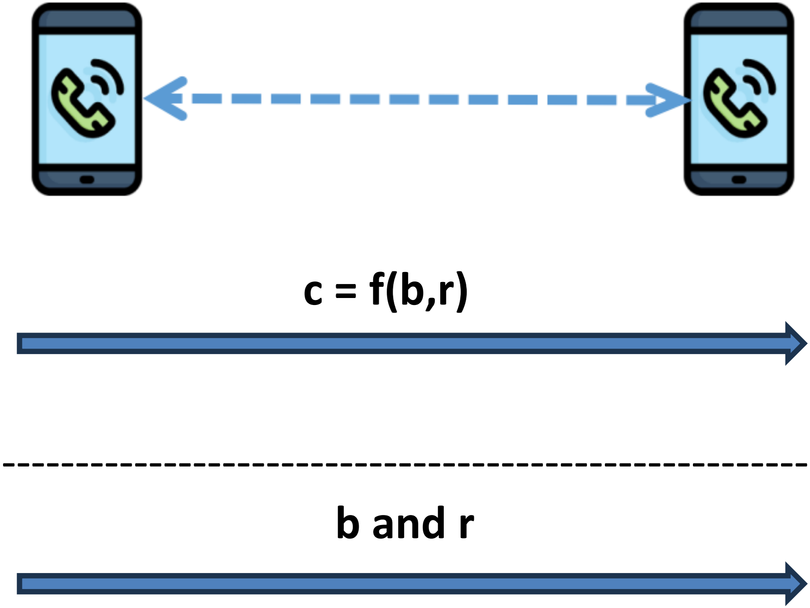
Abstract solution

1. Bob commit to a bit $b \in \{0, 1\}$
2. Later, Bob can open the commitment and convince Alice that b was the value he committed to
3. Committing to a bit b results in a commitment string c, that Bob sends to Alice, and an opening string s that Bob uses for opening the commitment later.

Commitment scheme

b=1, Head
b=0, Tail
r is random number

Bob



Alice

c = f(b,r)

承诺生成阶段

---

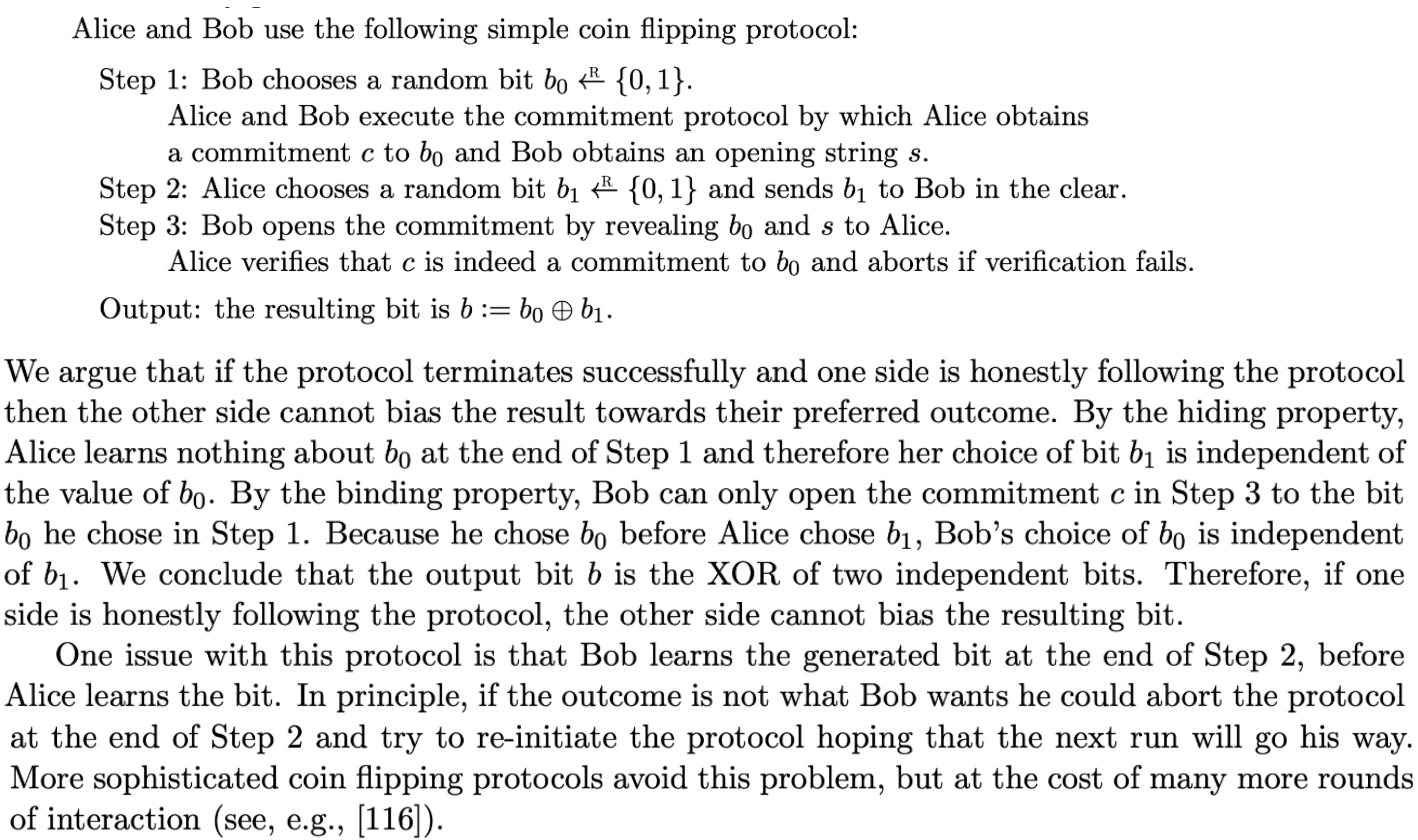
b and r

承诺披露阶段

Compute c’ = f(b,r)

Verify c’ =？ c

More reasonable protocol：



Alice and Bob use the following simple coin flipping protocol:

Step 1: Bob chooses a random bit $b_0 \xleftarrow{R} \{0,1\}$.
Alice and Bob execute the commitment protocol by which Alice obtains
a commitment c to b_0 and Bob obtains an opening string s.
Step 2: Alice chooses a random bit $b_1 \xleftarrow{R} \{0,1\}$ and sends b_1 to Bob in the clear.
Step 3: Bob opens the commitment by revealing b_0 and s to Alice.
Alice verifies that c is indeed a commitment to b_0 and aborts if verification fails.

Output: the resulting bit is $b := b_0 \oplus b_1$.

We argue that if the protocol terminates successfully and one side is honestly following the protocol then the other side cannot bias the result towards their preferred outcome. By the hiding property, Alice learns nothing about b_0 at the end of Step 1 and therefore her choice of bit b_1 is independent of the value of b_0. By the binding property, Bob can only open the commitment c in Step 3 to the bit b_0 he chose in Step 1. Because he chose b_0 before Alice chose b_1, Bob's choice of b_0 is independent of b_1. We conclude that the output bit b is the XOR of two independent bits. Therefore, if one side is honestly following the protocol, the other side cannot bias the resulting bit.

One issue with this protocol is that Bob learns the generated bit at the end of Step 2, before Alice learns the bit. In principle, if the outcome is not what Bob wants he could abort the protocol at the end of Step 2 and try to re-initiate the protocol hoping that the next run will go his way. More sophisticated coin flipping protocols avoid this problem, but at the cost of many more rounds of interaction (see, e.g., [116]).

Properties for Commitment Scheme

Hiding: The commitment string c reveals no information about the committed bit b. More precisely, the distribution on c when committing to the bit 0 is indistinguishable from the distribution on c when committing to the bit 1.

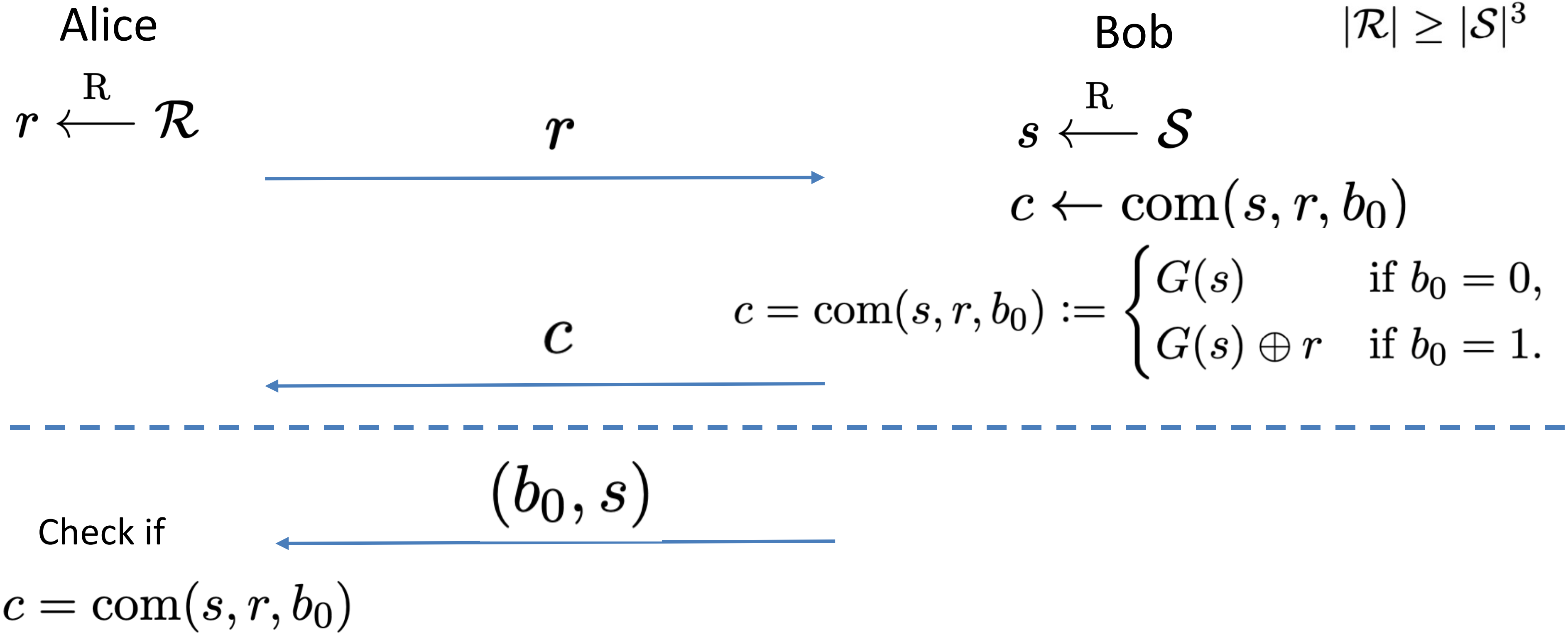
Binding: Let c be a commitment string output by Bob. If Bob can open the commitment as some b $\in$ {0, 1} then he cannot open it as 1-b. This ensures that once Bob commits to a bit b he can open it as b and nothing else.

Bit Commitment from Secure PRG

Bob commits to bit $b_0 \in \{0,1\}$

$G : \mathcal{S} \to \mathcal{R}$

$|\mathcal{R}| \geq |\mathcal{S}|^3$



Alice

Bob

$r \xleftarrow{\text{R}} \mathcal{R}$

$s \xleftarrow{\text{R}} \mathcal{S}$

$\boldsymbol{r}$

$c \leftarrow \mathrm{com}(s, r, b_0)$

$$c = \mathrm{com}(s, r, b_0) := \begin{cases} G(s) & \text{if } b_0 = 0, \\ G(s) \oplus r & \text{if } b_0 = 1. \end{cases}$$

$\boldsymbol{c}$

(b_0, s)

Check if

$c = \mathrm{com}(s, r, b_0)$

Analysis

Hiding: Because the output G(s) is computationally indistinguishable from a uniform random string in R it follows that $G(s) \oplus r$ is also computationally indistinguishable from a uniform random string in R. Therefore, whether b0 = 0 or b0 = 1, the commitment string c is computationally indistinguishable from a uniform string in R, as required.

Binding: Holds unconditionally as long as 1/|S| is negligible. The only way Bob can open a commitment $c \in R$ as both 0 and 1 is if there exist two seeds $s0, s1 \in S$ such that $c = G(s0) = G(s1) \oplus r$ which implies that $G(s0) \oplus G(s1) = r$. Let us say that $r \in R$ is “bad” if there are seeds $s0, s1 \in S$ such that $G(s0) \oplus G(s1) = r$. The number of pairs of seeds (s0, s1) is $|S|^2$, and therefore the number of bad r is at most $|S|^2$. It follows that the probability that Alice chooses a bad r is most $|S|^2/|R| < |S|^2/|S|^3 = 1/|S|$ which is negligible. Therefore, the probability that Bob can open the commitment c as both 0 and 1 is negligible.