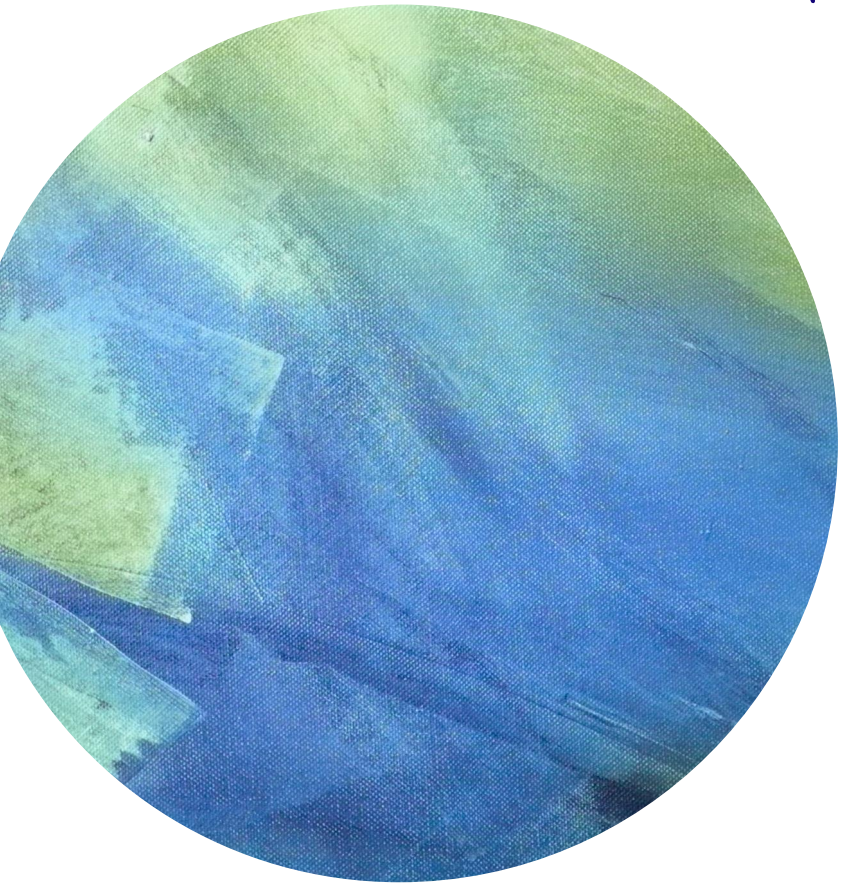
Lecture 18

HW announcements

Scribe: Aishani



Outline

Commitments

Zero-Knowledge

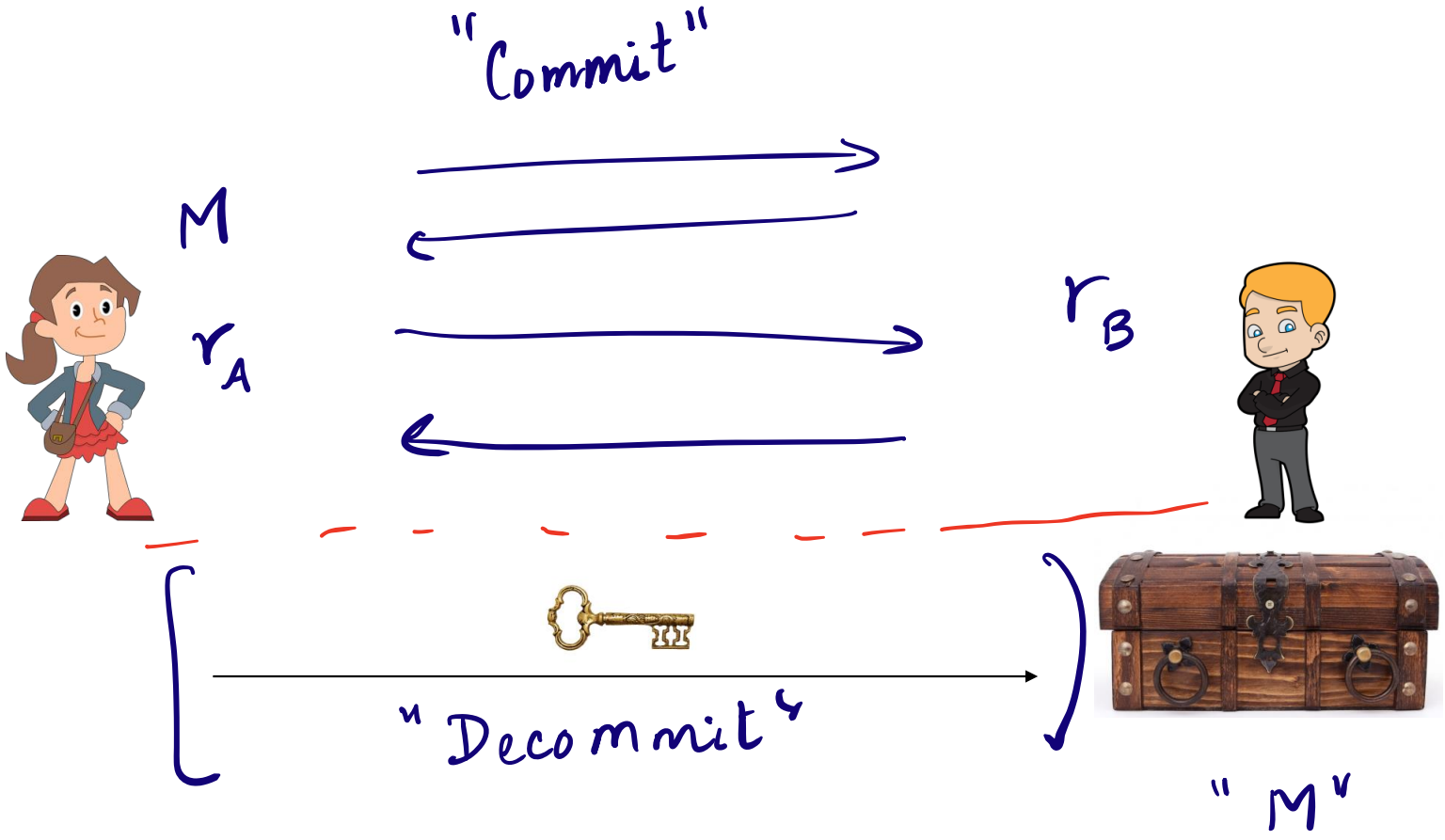
(Next time)

Commitments

Commitments

Commitments

Commitments



Commitments

- Correctness :

$$\text{Decommit}_{CR}(\tau, M, r_A) = M'$$

when $\tau \leftarrow \text{Commit}_{CR}(M; r_A, r_B)$

- Binding

$\forall$ PPT C^*,

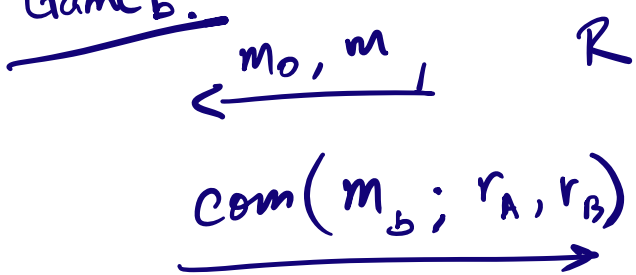
$$\Pr\left[\text{Decommit}^*_{CR}(\tau, r_A') = M_1 \text{ and } \text{Decommit}^*_{CR}(\tau, r_A^2) = M_2\right] = \text{negl}.$$

$r_A', r_A^2 \leftarrow C^*$.

when $\tau \leftarrow \text{Commit}_{C^* R}(r_A, r_B)$

where $M_1 \neq$ FAIL AND $M_2 \neq$ FAIL. AND $M_1 \neq M_2$.

- Hiding



$$\left|\Pr[R = 1 \mid \text{Game}_0] - \Pr[R = 1 \mid \text{Game}_1]\right| = \text{negl}.$$

Examples

- If (g, g^x) a commitment to x?

- Ct = E (k, m) for a symmetric key encryption E

Examples

Commit $(M; r) \rightarrow H(M \| r)$

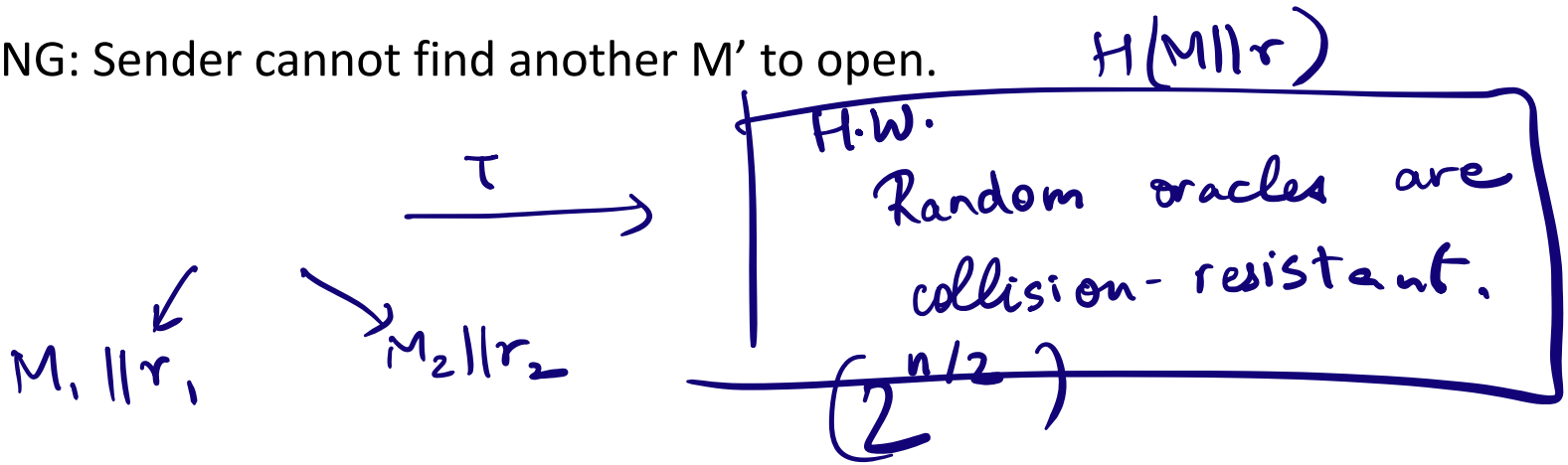
Decommit $(\tau, M, r) \rightarrow$ Accept iff $H(M \| r) = \tau$.

In practice, we use:

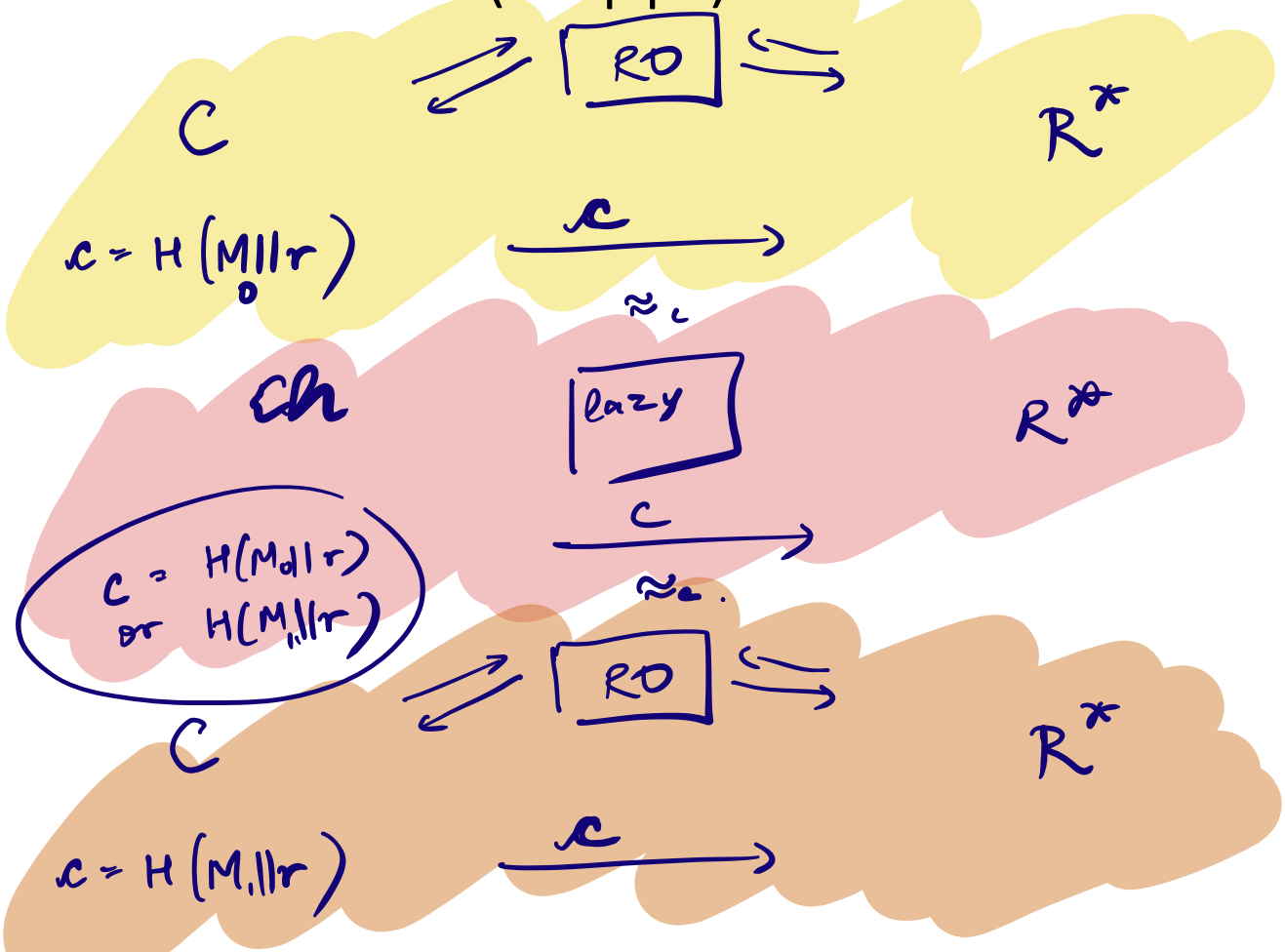
$H(M \| r)$

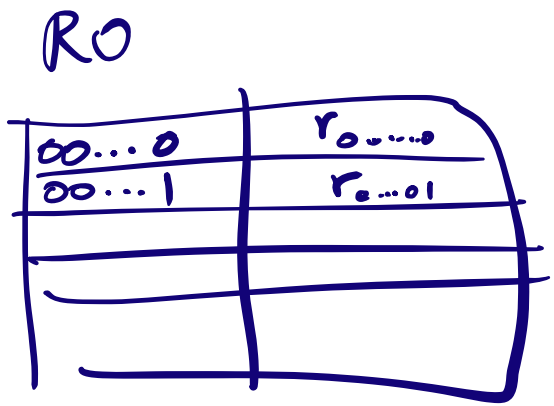
- To commit to message M, choose random, fixed-length r, send H(r || M)
- To open commitment, send r, M

- BINDING: Sender cannot find another M' to open.

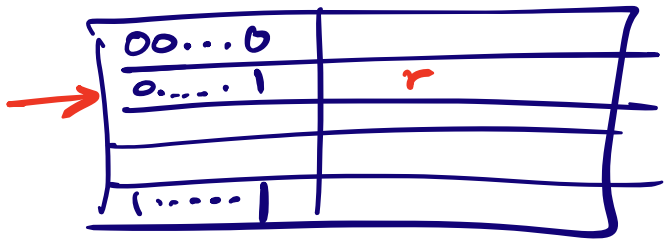


HIDING: H(M||r) "hides" M

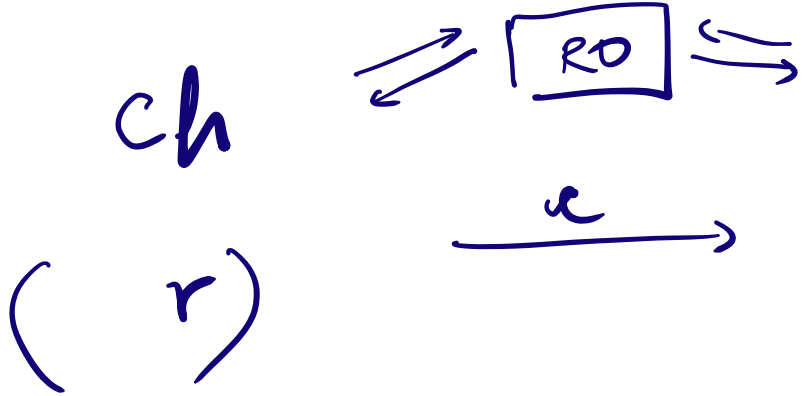




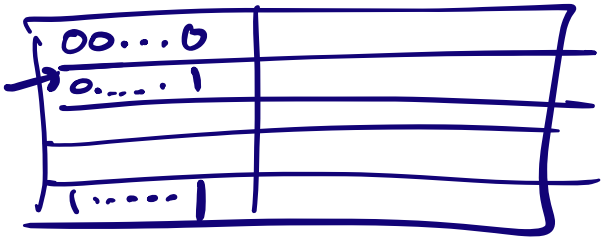
"lazy sampling"



HIDING: H(M||r) "hides" M



"lazy sampling"



$\Pr[R^* \text{'s first query is } (M_0 \| r) \text{ or } (M_1 \| r)] = \frac{1}{2^{|r|}}$

(second ———) $= \frac{1}{2^{|r|}-1}$

$|r| = n.$

n^{th} query is $(M_0 \| r)$ or $(M_1 \| r) = \frac{1}{2^{|r|}-n}$

$Pr[R^*$ ever queries table on $(M_0 \| r)$ or $(M_1 \| r)] = \text{negl}(n)$

Examples

Binding : $x <$ order of group.

- If (g, g^x) a commitment to x?

Hiding : x_0, x_1 ← ; g, g^{x_b} →

- Ct = E (k, m) for a symmetric key encryption E

not necessarily binding

(OTP is not binding)

$k \oplus m_1 = k_2 \oplus m_2$.

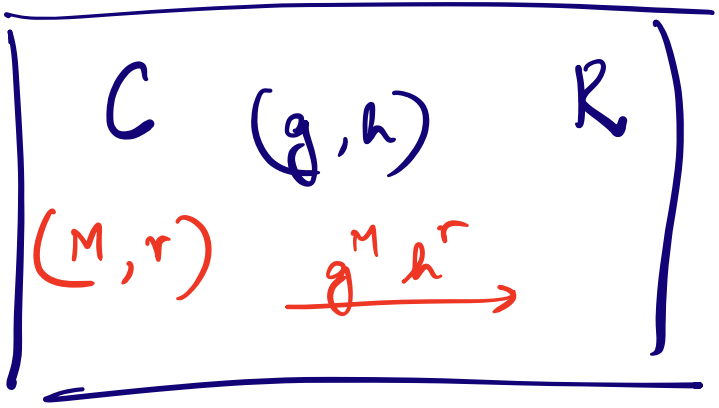
Examples

In practice, we use:

- To commit to message M, choose random, fixed-length r, send H(r || M)
- To open commitment, send r, M
- Receiver cannot fully recover M.

- Sender cannot find another M’ to open.

Pedersen Commitments



- Public parameters: (p,g,h)
  - p: large prime (1024 bit)
  - g: generator
  - h: g^a for hidden a
- Protocol
  - To commit to x, C chooses random r and sends ($g^x h^r$) to R.
  - To open, C sends x and r to R.
- Benefits:
  - One can prove many things about the committed value without opening it

Pedersen Commitments

- Unconditionally hiding
  - Given a commitment c, every value x is equally likely to be the value committed in c.
  - For example, given x,r, and any x', there exists r' such that $g^x h^r = g^{x'} h^{r'}$, in fact $r = (x-x')a^{-1} + r \bmod q$.

Pedersen Commitments

- Computationally binding
  - Suppose committer sent $g^x h^r \bmod p$ for some (x, r)
  - Now it finds $x' \neq x$ and r' such that $c = g^{x'} h^{r'}$.
  - This means that the sender ``knows'' $\log_g(h) = (x'-x)\cdot(r-r')^{-1}$.
  - This means: assuming DL is hard, the sender cannot open the commitment to a different value.

Application: Coin Tossing

- Alice and Bob want to decide on something by tossing a coin over a phone. How to do this securely?
- Solution: Alice commits to a random bit $b_A \leftarrow \{0, 1\}$, and sends Com $(b_A; r)$ to Bob
- Bob selects a random bit $b_B \leftarrow \{0, 1\}$ and sends it to Alice
- Alice decommits b_A
- Alice and Bob output b_A xor b_B