Security Notions

Sushmita Ruj

Recap

- OTP and perfect secrecy of OTP
- Construction of Stream ciphers using PRG
- Statistical Tests
- Block Ciphers, DES, AES
- Modes of Operation
- This class: Security definitions and notions

Security So Far

- Perfect security: OTP
- Stream ciphers are not perfectly secure
- Computational security
- Attack models, Ciphertext only, plaintext-only, chosen plaintext attack (CPA), chosen cipher text attack (CCA)
- Adaptive vs non-adaptive attack
- Indistinguishability

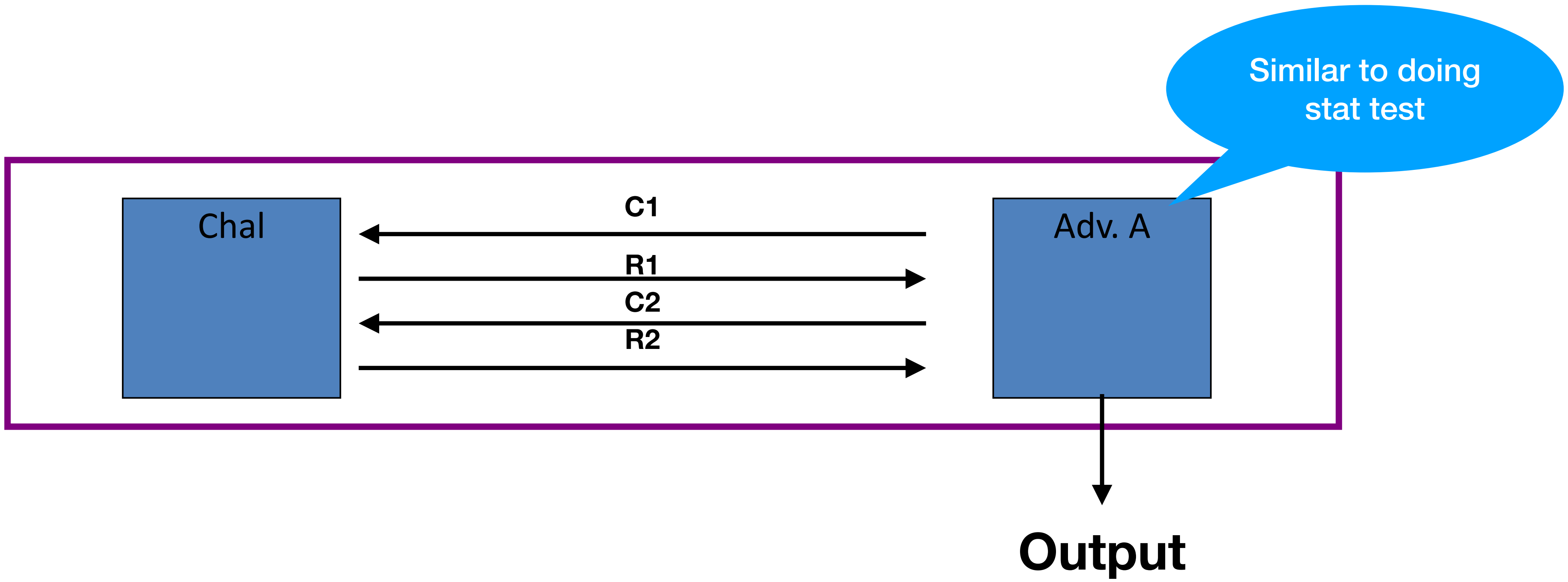
Revisiting SKE

- $\mathscr{E} = (\mathscr{M}, \mathscr{C}, \mathscr{K})$
- $KeyGen(1^k) \rightarrow k \in \mathscr{K}$
- $For\ \ m \in \mathscr{M}, k \in \mathscr{K}, E(m, k) \rightarrow c$
- $D(c, k) \rightarrow m'$
- Correctness: $\forall k \in \mathscr{K}$ and messages $m \in \mathscr{M}$, if we execute $c \overset{R}{\leftarrow} E(m, k), m' \leftarrow D(c, k)$, then $m = m'$ with probability 1
-

Semantic Security

- $\mathscr{E} = (E, D)$, defined over $(\mathscr{M}, \mathscr{C}, \mathscr{K})$
- For all predicates ϕ and all messages $m_0, m_1 \in \mathscr{M}$, k chosen uniformly at random from $\mathscr{K}$
- $Pr[\phi(E(m_0, k))] = Pr[\phi(E(m_1, k))]$
- Instead we also say $|Pr[\phi(E(m_0, k))] - Pr[\phi(E(m_1, k))]| < \epsilon$, ϵ is neg

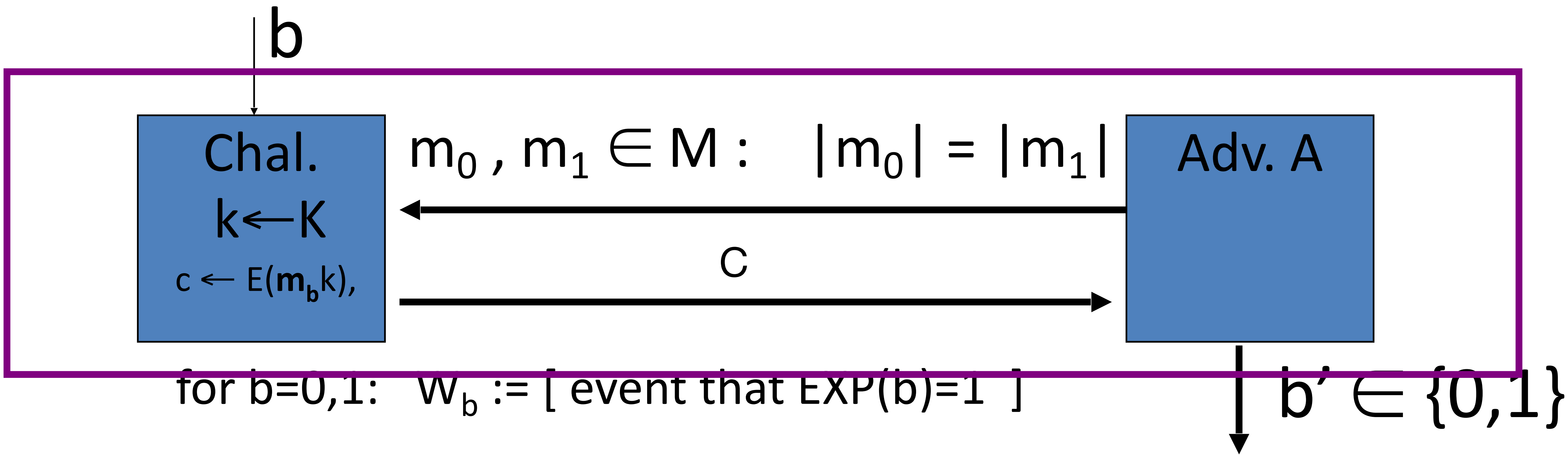
Semantic Security



- Attack game between challenger C and adversary A
- We calculate the Adversary's advantage of winning the game
- Length of messages

Semantic Security (one-time key)

For b=0,1 define experiments EXP(0) and EXP(1) as:



for b=0,1: W_b := [event that EXP(b)=1]

$\mathrm{Adv}_{SS}[A,E] := \Big|\ \Pr[\,W_0\,] - \Pr[\,W_1\,]\ \Big| \in [0,1]$

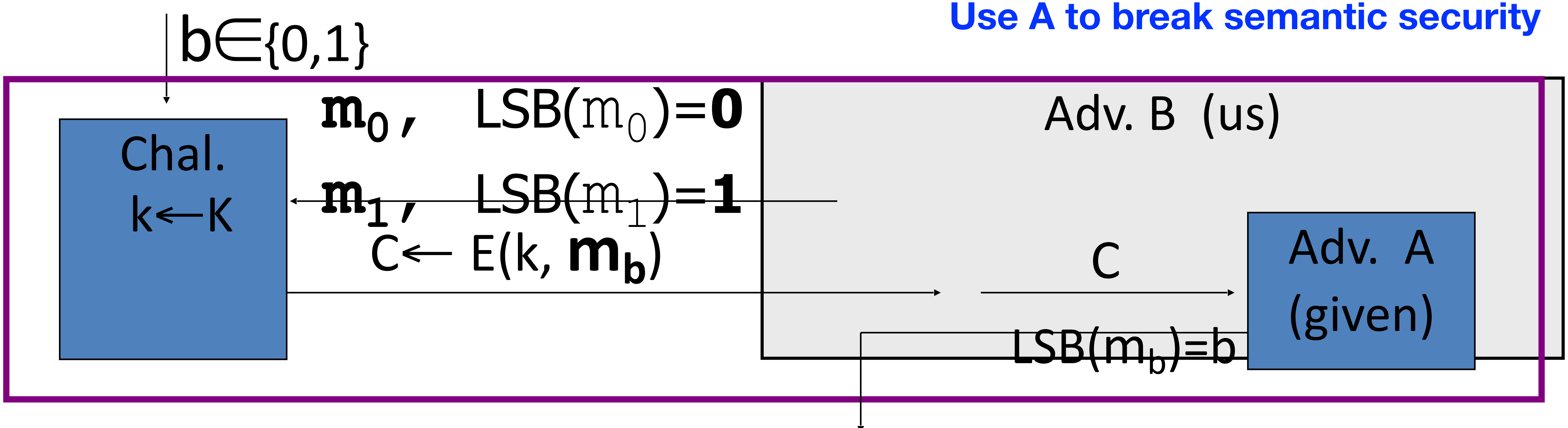
The cipher is Semantically secure if for all efficient adversaries, A, $\mathrm{Adv}_{SS}[A,E]$ is neg

Knowing LSB of PT

Suppose efficient A can always deduce LSB of PT from CT.

$\Rightarrow$ E = (E,D) is not semantically secure.

Use A to break semantic security



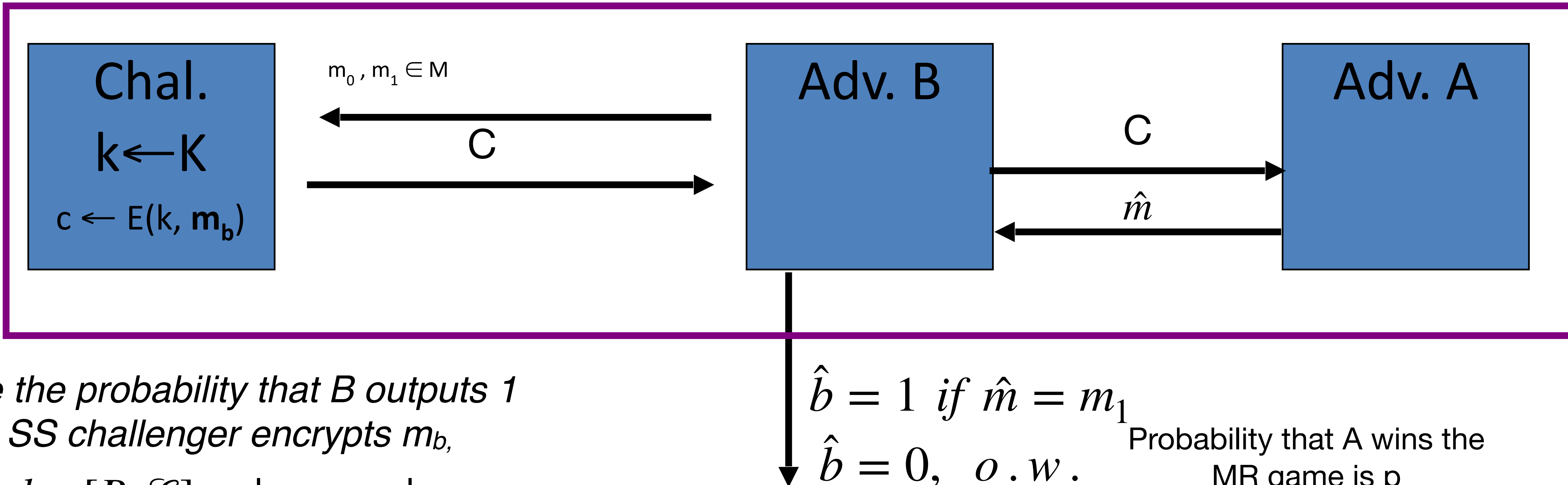
Then $\text{Adv}_{SS}[B, E] = |\ \Pr[\ \textbf{EXP(0)}=1\ ] - \Pr[\ \textbf{EXP(1)}=1\ ]\ | = |0 - 1| = 1$

Message Recovery Attacks

- $\varepsilon = (E, D)$, defined over $(\mathscr{M}, \mathscr{C}, \mathscr{K})$
- Intuitively, in a message recovery attack, an adversary is given an encryption of a random message, and is able to recover the message from the ciphertext with probability significantly better than random guessing, that is, probability $1/|\mathscr{M}|$
- Attack game:
- Challenger computes $m \xleftarrow{R} \mathscr{M}, k \xleftarrow{R} \mathscr{K}, c \xleftarrow{R} E(m, k)$ & sends c to Adv A
- Adv A outputs $\hat{m} \in \mathscr{M}$
- Let W be the event, $\hat{m} = m$
- A wins the game with a message recovery advantage
- $Adv_{MR}[A, \mathscr{E}] = |Pr[W] - 1/|\mathscr{M}||$
- **To show secure against message recovery we show that the above adv is neg**
- Proof sketch: Any efficient adversary *A* that can effictively mount a message recovery attack on $\mathscr{E}$ can be used to build an efficient adversary B that breaks the semantic security of $\mathscr{E}$;
- Since semantic security implies that no such B exists, we may conclude that no such A exists.

Security Reductions

Construct B, such that $Adv_{MR}[A, \mathscr{E}] \leq Adv_{SS}[B, \mathscr{E}]$



$\hat{b} = 1 \; if \; \hat{m} = m_1$

$\hat{b} = 0, \quad o.w.$

Probability that A wins the MR game is p

$\Longrightarrow \; Adv_{MR}[A, \mathscr{E}] = |p - 1/|M||$

p_b be the probability that B outputs 1 if B's SS challenger encrypts m_b,

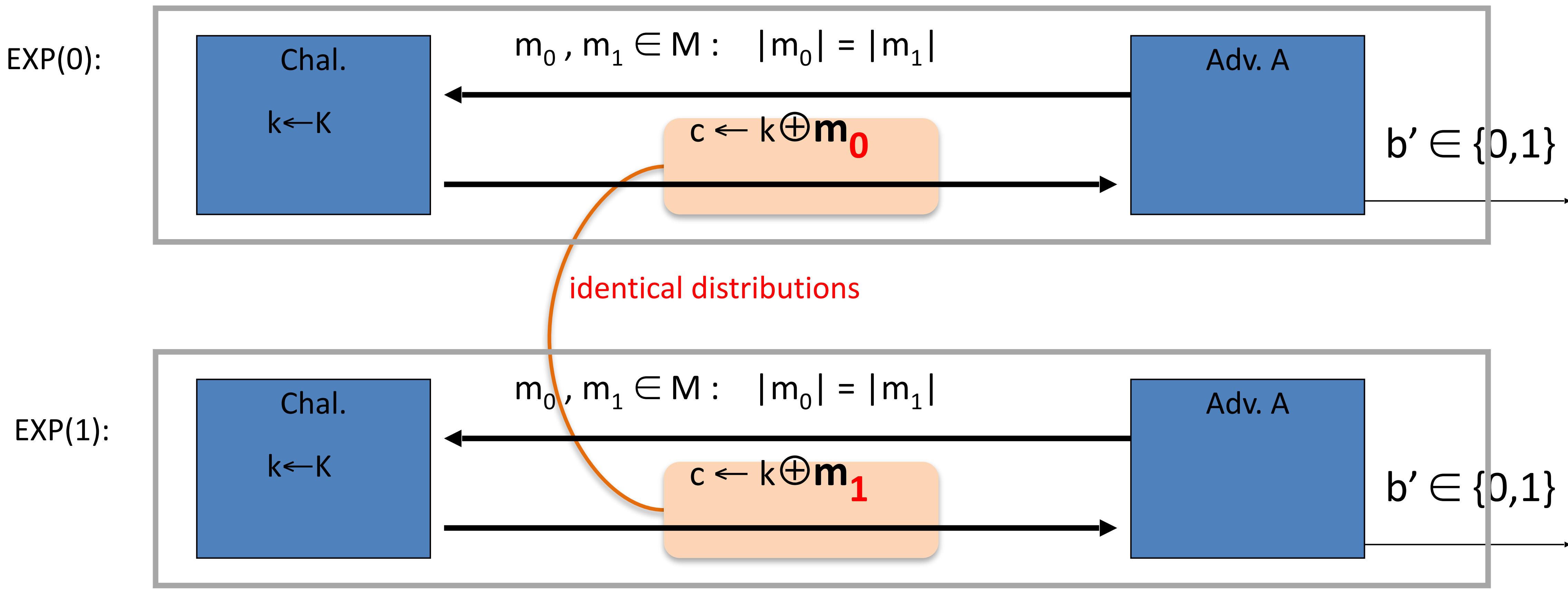
So, $Adv_{SS}[B, \mathscr{E}] = |p_0 - p_1|$

c is an encryption of m_1, the probability p_1 is precisely equal to A's probability of winning the message recovery game, so $p_1 = p$.

c is an encryption of m_0, the adversary A's output is independent of m_1, and so $p_0 = 1/|M|$.

$$Adv_{SS}[B, \mathscr{E}] = |p_1 - p_0| = |p - 1/|M|| = Adv_{MR}[A, \mathscr{E}]$$

OTP is Semantically Secure



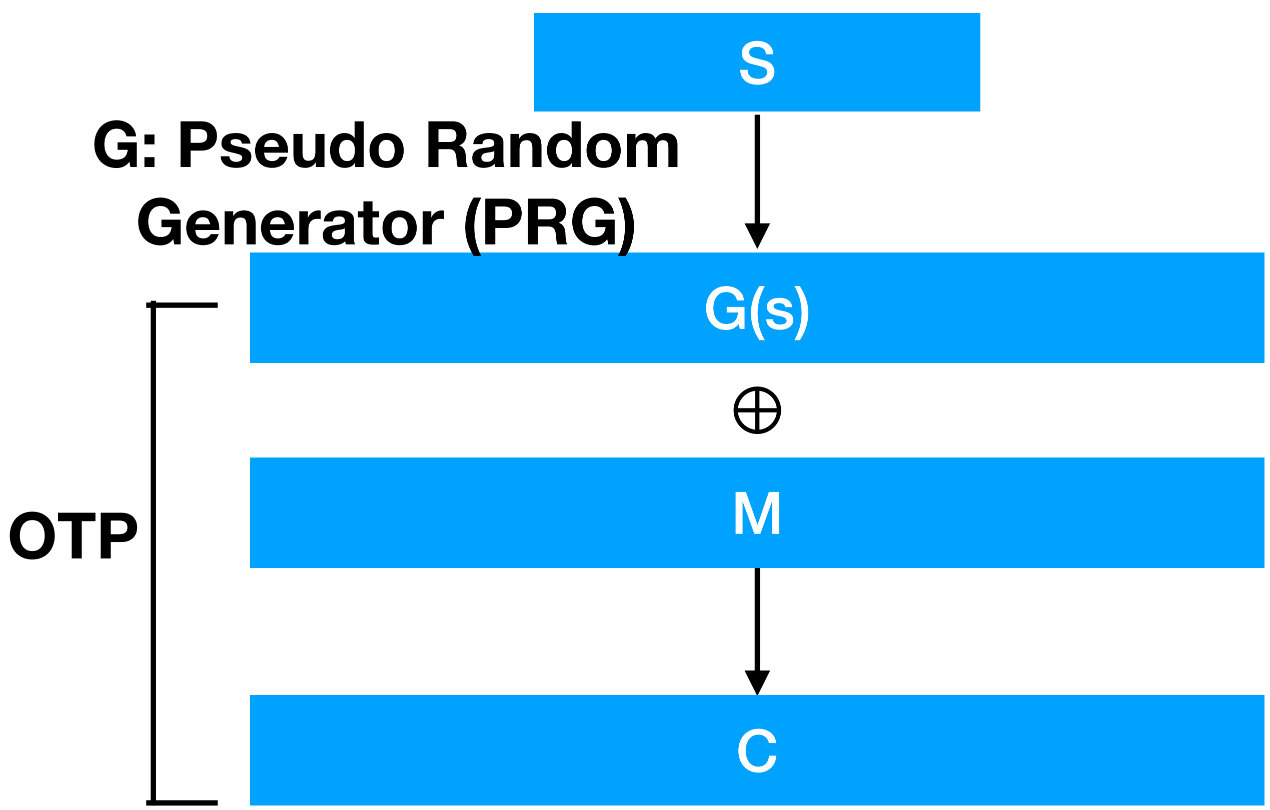
For **all** A: $\mathrm{Adv}_{SS}[A,OTP] = \left| \Pr[\, \mathbf{A(k \oplus m_0)}{=}1 \,] - \Pr[\, \mathbf{A(k \oplus m_1)}{=}1 \,] \right| = 0$

Indistinguishability

Practical OTP

No
Size of K is
smaller than
message

Q1: Does this have prefect secrecy?



Size of message is L

Q1: What is G? What properties does it have?
|s| < |M|. K should look like a random string r of length L .

How to do this?
We use Statistical Tests

Q3: What can we say about the security of this cipher?

$$C = M \oplus G(K)$$

$$M = C \oplus G(K)$$

This does not have prefect secrecy, so we defines a new type of security called "semantic Security"

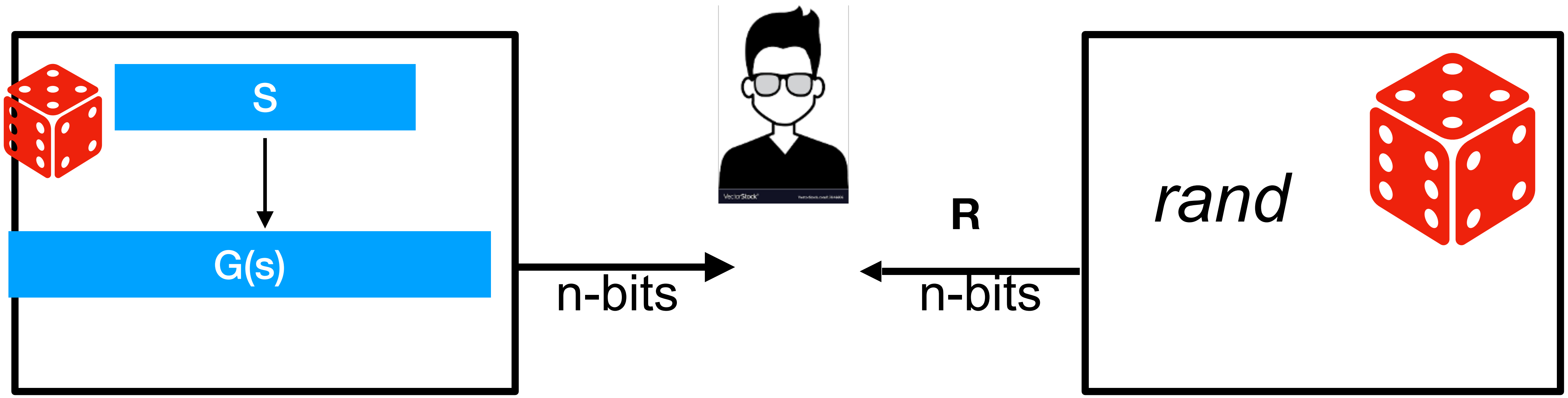
These are called stream ciphers

Turing Tests [1950]

Distinguisher

If robot is intelligent, Bob can't distinguish between Alice and Robot

PRG Indistinguishability test



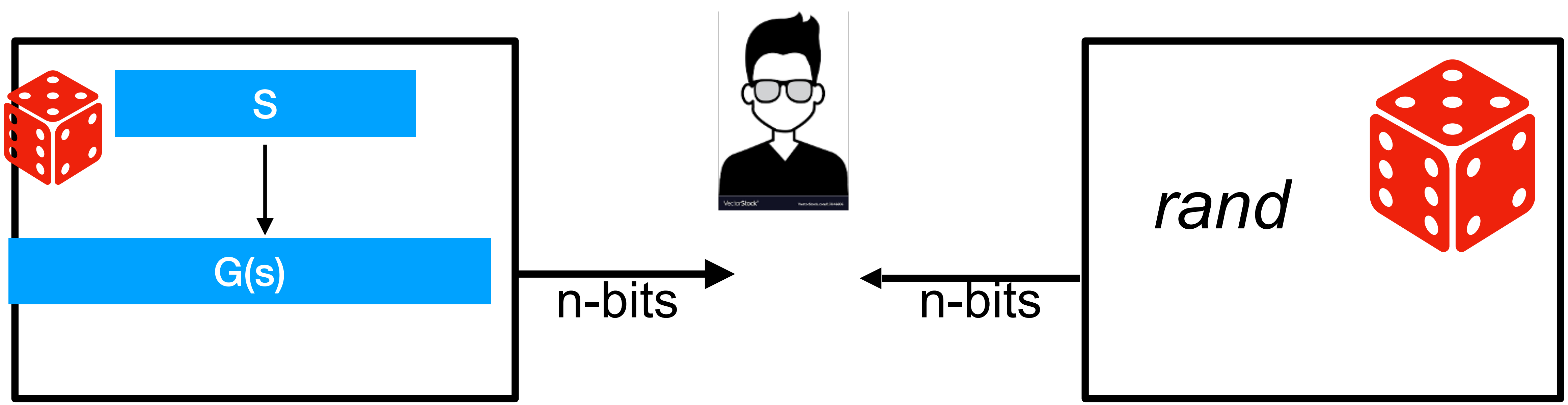
Properties of a distinguisher?

Efficient: Probabilistic polynomial time (PPT) algo. (Poly in length of input)
Should be able to distinguish with non-neg probability

Given n bit input (s.t. |x| =n) is there an efficient algorithm that:
Finds x^2?
Finds the factors of x ?
Find y, such that x= f(y)?

PRG Indistinguishability test

A PRG is secure if no efficient adversary can effectively tell the difference between G(s) and r: the two are computationally indistinguishable.



Semantic Security of PRG

Thm: $G: K \longrightarrow \{0,1\}^n$ is a secure PRG $\Rightarrow$

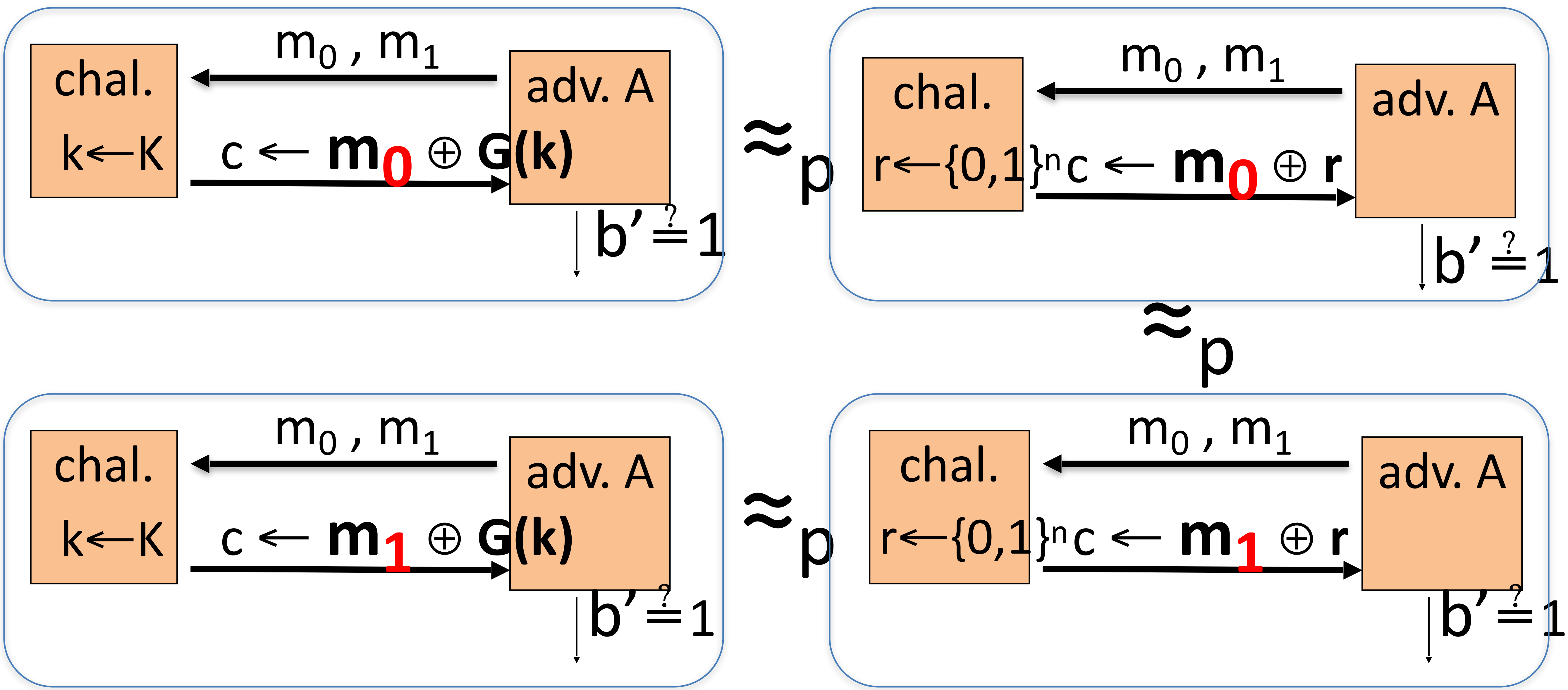
stream cipher E derived from G is semantically secure.

We prove that:

$\forall$ SS adversary A , $\exists$a PRG adversary B s.t.

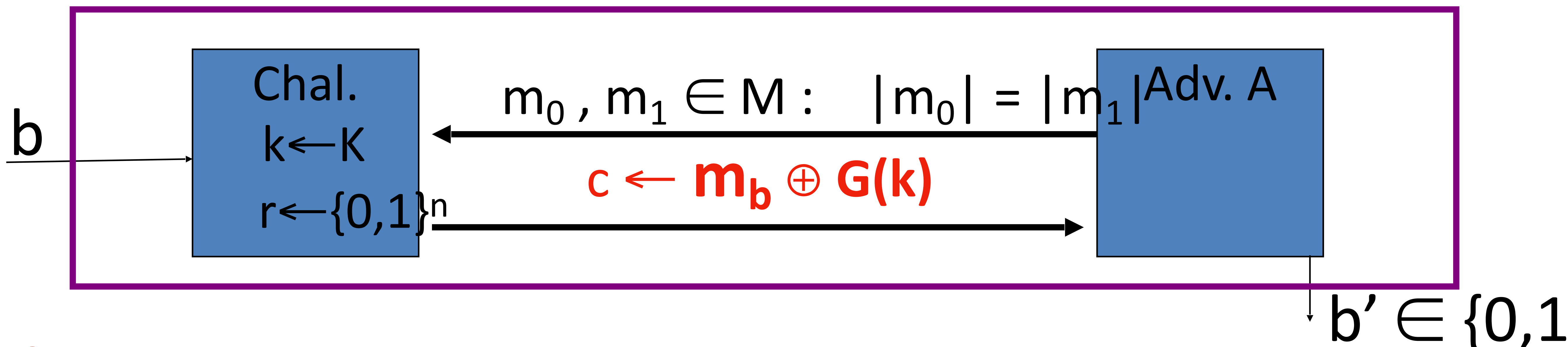
$$\mathrm{Adv}_{SS}[A,E] \leq 2 \cdot \mathrm{Adv}_{PRG}[B,G]$$

Proof: Intuition



Proof

Proof: Let A be a SS adversary.



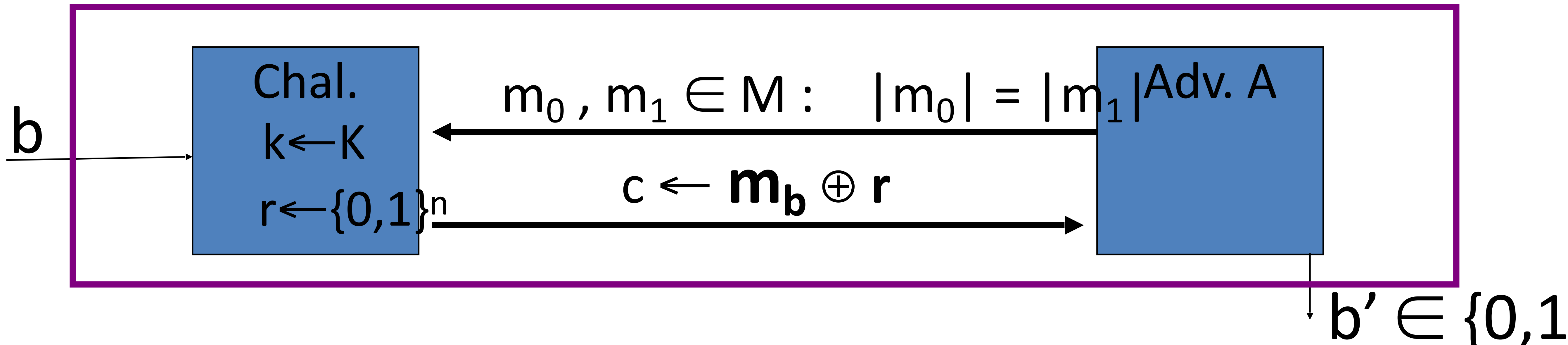
Original semantic security game

For b=0,1: W_b := [event that b'=1, when receiving enc of m_b].

$$\mathrm{Adv}_{SS}[A,E] = \Big|\ \Pr[\ W_0\ ] - \Pr[\ W_1\ ]\ \Big|$$

Proof

Proof: Let A be a SS adversary.



Original semantic security game

For b=0,1: W_b := [event that b'=1, when receiving enc of m_b].

$$Adv_{SS}[A,E] = \left| \Pr[W_0] - \Pr[W_1] \right|$$

Security game from random key in OTP

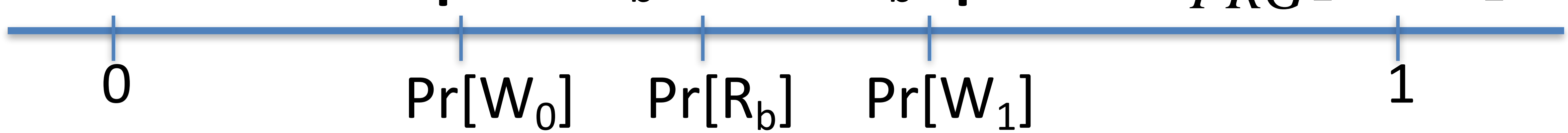
For b=0,1: R_b := [event that b'=1, when receiving OTP enc of m_b]

Proof

Proof: Let A be a SS adversary.

Claim 1: $\left|\Pr[R_0] - \Pr[R_1]\right| = Adv_{SS}[A, OTP] = 0$

Claim 2: $\exists B$: $\left|\Pr[W_b] - \Pr[R_b]\right| = Adv_{PRG}[B, G]$

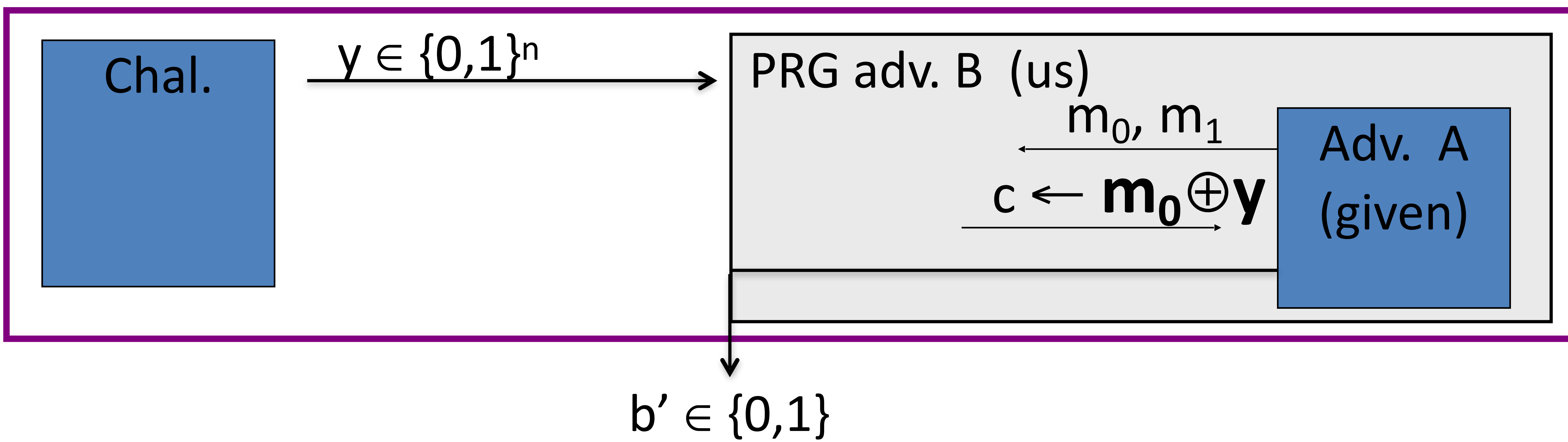


$\Rightarrow$ $\mathrm{Adv}_{SS}[A,E] = \left|\Pr[W_0] - \Pr[W_1]\right| \leq 2 \cdot \mathrm{Adv}_{PRG}[B,G]$

Proof

Proof of claim 2: $\exists B$: $\Big|\Pr[W_0] - \Pr[R_0]\Big| = \mathrm{Adv}_{\mathrm{PRG}}[B,G]$

Algorithm B:



$$\mathrm{Adv}_{\mathrm{PRG}}[B,G] = \left|Pr_{r \xleftarrow{R} \{0,1\}^n}[B(r) = 1] - Pr_{k \xleftarrow{R} \mathcal{K}}[B(G(k)) = 1]\right| = \left|Pr[R_0] - Pr[W_0]\right|$$

Thank you