Public Key Encryption

Rohit Musti

CUNY - Hunter College

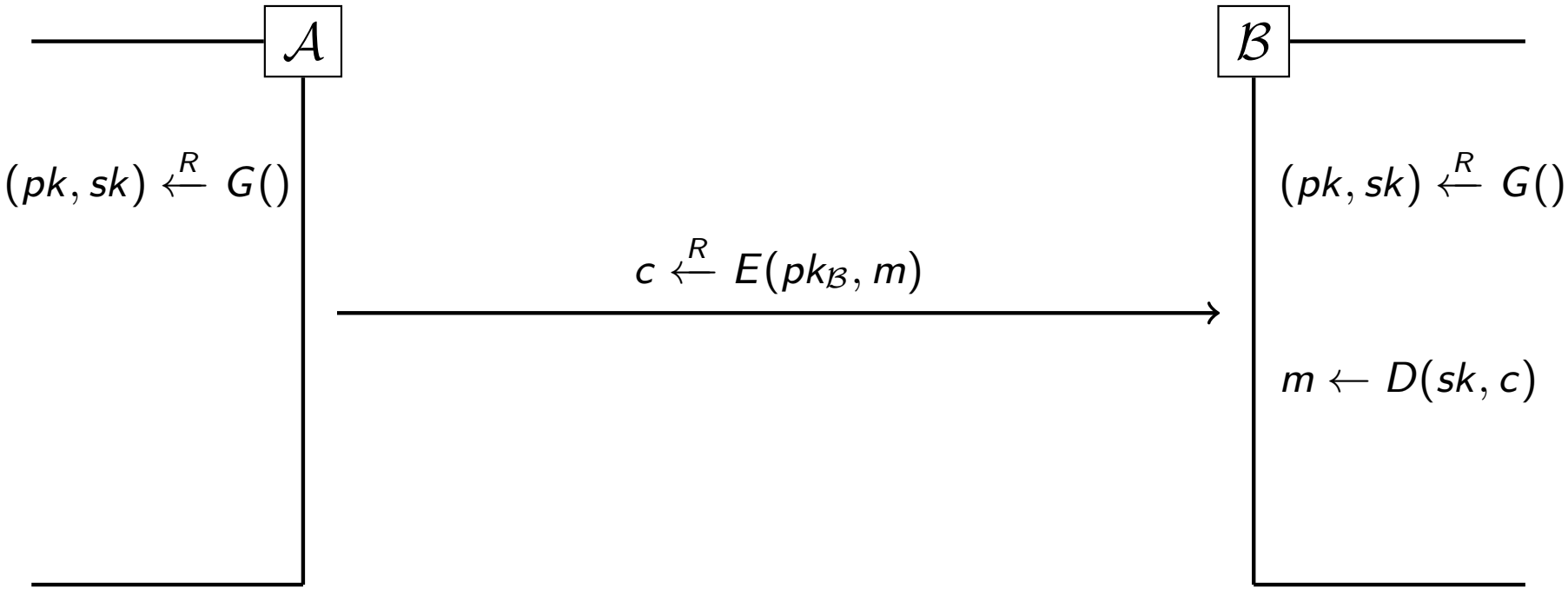
March 23, 2022

Table of Contents

Recap

- Last lecture we discussed an example of how to exchange secret keys "in the clear"
- This allows us to re-use our symmetric key cryptography protocols to exchange information in the public!
- We also discussed two real-world examples of key exchange (Diffie-Hellman and RSA)
- In the lecture prior to that we introduced the notion of assymetric encryption, outlined its basics. Today we will dive into its security!

Public Key Encryption Overview



Benefits

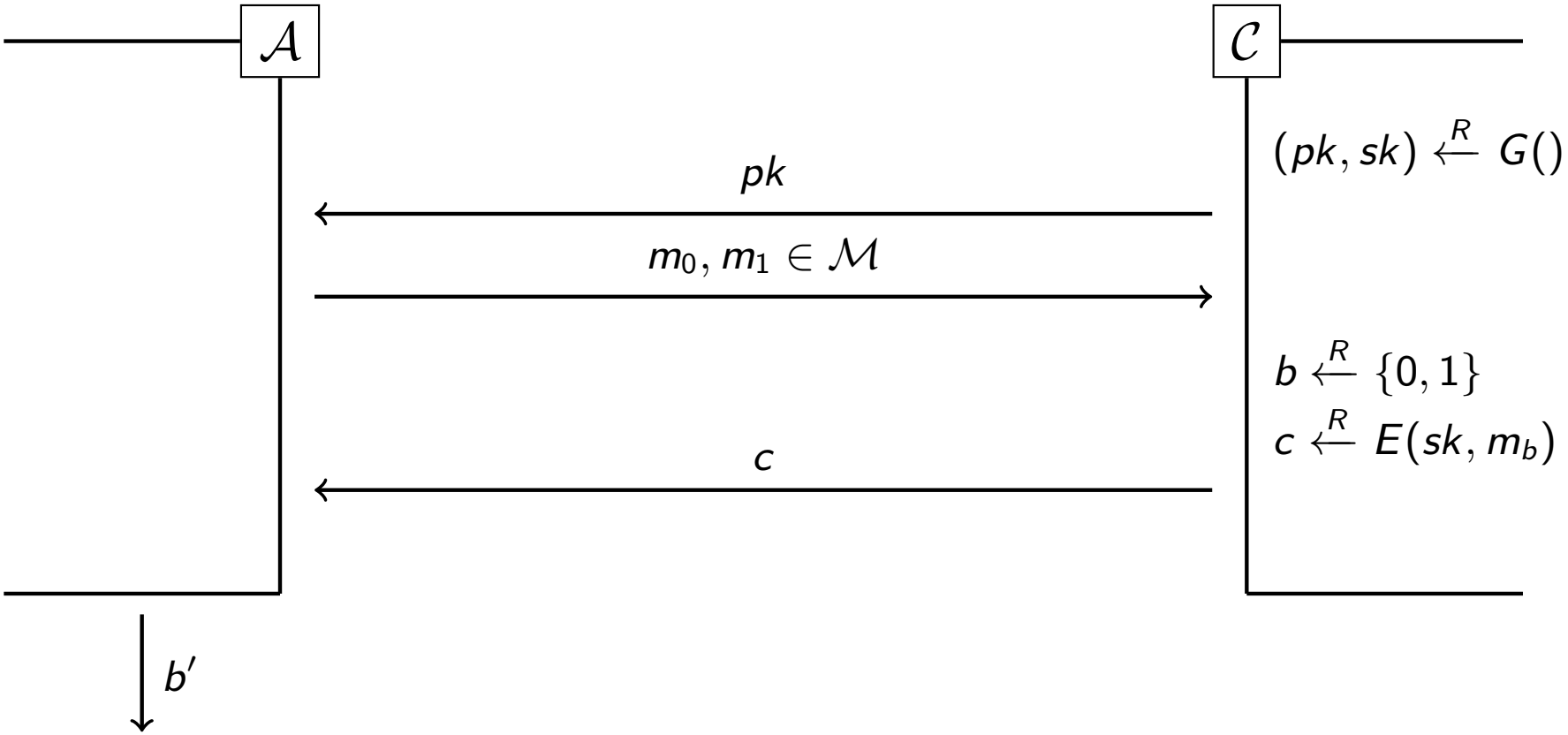
1. Public key encryption is often referred to as *assymetric encryption* because the encryptor and decryptor use different keys (unlike *symmetric encryption* which uses the same keys)
2. After the public key is securely obtained, there is only one interaction to send a message!
3. We can re-use the public key many times
4. Anyone can post their public key for everyone else to see (no key exchange required), this means that the secret keys must not be derivable from public keys

2 Semantic Security

Review of Semantic Security

- The intuition of semantic security is that the probability a computationally bounded adversary can learn anything about a message from its ciphertext is negligible
- Semantic security guarantees that a message cannot be recovered from a ciphertext

Public Key Semantic Security Attack Game



if $b' = b$, then the adversary wins

Semantic Security Randomization

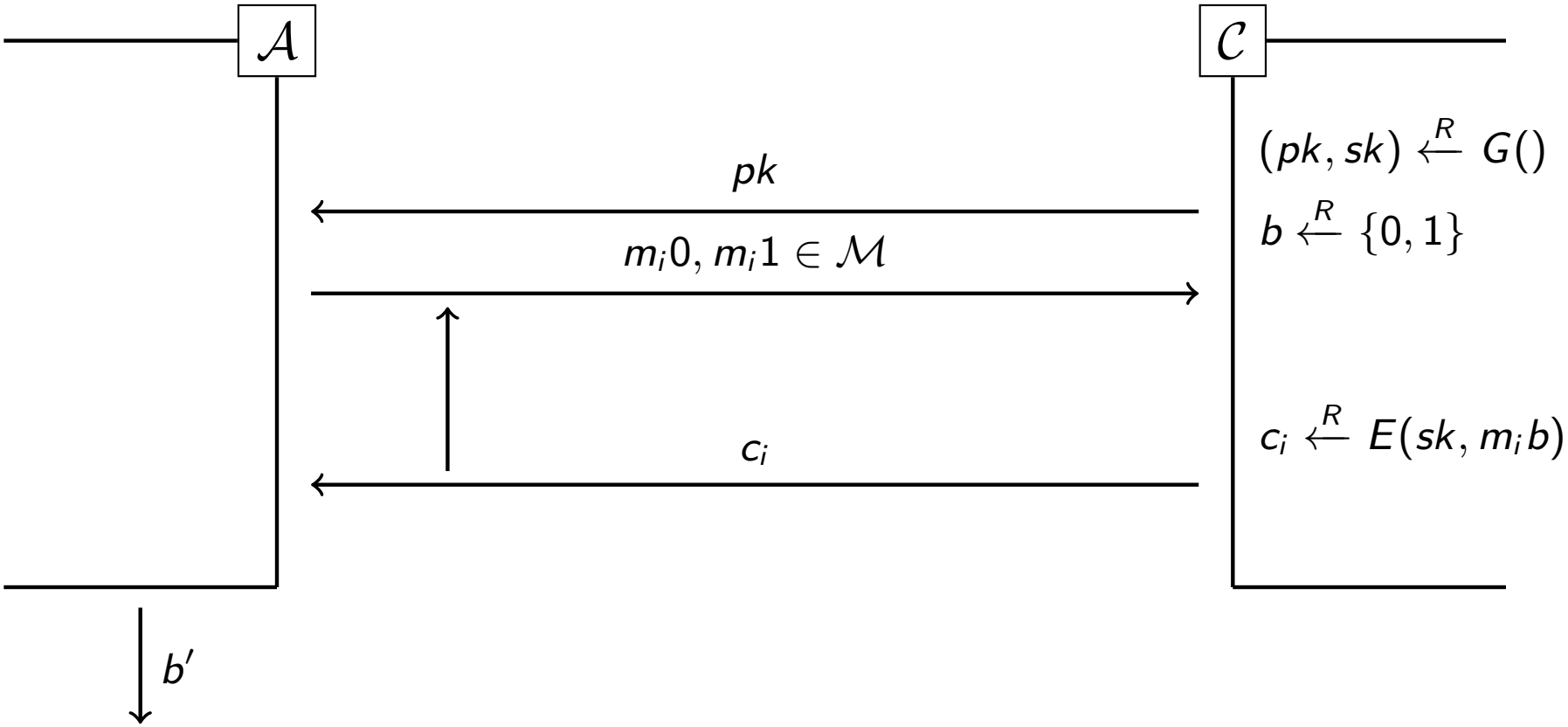
- For public key semantic security, the encryption function must be random. Can we think of an attack???
- Future Homework Assignment!

3 Chosen Plaintext Attack Security

Public Key CPA Security

- Semantic security does not imply CPA security in symmetric key cryptography schemes
- The intuition behind this is that in a symmetric key security setting, the attacker cannot encrypt their own messages into their own cipher texts (because they don't have access to the key)
- In a public key setting, the adversary doesn't even need to interact with the challenger to get cipher texts

Public Key CPA Attack Game



if $b' = b$, then the adversary wins

4 Chosen Ciphertext Attack Security

CCA Motivation

- Imagine I collected homework by email and required that y'all encrypt your homework with my public key pk
- What if another student intercepted that stream of data and strategically flipped bits until the submission read as "from: student1" to "from: student2"
- Therefore, we need our systems to be secure against adversaries generating valid cipher texts

CCA Construction

$$E(pk, m) = [x \xleftarrow{R} \mathcal{X}, y \leftarrow F(pk, x), k \leftarrow H(x), c \xleftarrow{R} E_s(k, m)] \rightarrow (c, y)$$

$$D(pk, (y, c)) = [x \leftarrow I(sk, y), k \leftarrow H(x), m \leftarrow D_s(k, c)] \rightarrow m$$

5 Shamir Secret Sharing

Motivation

- suppose you have a secret that you want to share with your friends
- but you only want your friends to unlock this secret if they are all together
- wouldn't it be cool if there was a mathematical way to ensure they can only unlock the secret if they are all together?

Overview

- Enter polynomial interpolation
- if you have two points, you can find a unique line that intersects them, if you have 3 points, you can identify a unique parabola and so on
- you can encode your secret somewhere along a function, and then tell all of your friends a different point along the curve expressed by the function
- if enough of your friends get together, they can figure out the exact curve and and find the secret!