Announcement

- Guess who have won this year's Turing Award
  - Whitfield Diffie and Martin E. Hellman for their seminal work "Diffie-Hellman Protocol"
- HW2 is due at 7PM on Tuesday, 3/15
- HW2 Q8 has been updated
- Bonus points in HW1
- Dr. Sun will give a talk at 5PM on 3/16 @TH331. Get 2 bonus points if attend.

Last Time

- Digital signatures
  - Provide data integrity and non-repudiation
- Diffie-Hellman Protocol
  - Negotiate a shared secret key over an insecure media
- Man-in-The-Middle attack
- Preserve data confidentiality and data integrity with secret key cryptography and public key cryptography

What is Authentication?

- Short answer: To whom am I speaking
- Long answer: evaluate the authenticity of identity proving credentials
  - Credential: proof of identity
  - Evaluation: process that assesses the correctness of the association between credential and claimed identity

Why Authentication?

- We live in a world of rights, permissions, and duties...
- Authentication establishes our identity so that we can obtain the set of rights
- Q: How does this relate to security?
  - C-I-A Triads
- Computer security is crucially dependent on the proper design, management, and application of authentication systems

Identity & Credential

- Identities give you access, which is largely determined by context (by who is evaluating credentials)
  - Examples:

    Driver's License prove…
- Credentials are evidence used to prove identity
  - Something I know
  - Something I have
  - Something I am

Something I Know

- Passwords and pass-phrases
- Passwords are generally pretty weak
  - University of Michigan: 5% of passwords were goblue
  - Passwords used in more than one place
- Not just because bad ones selected: If you can remember it, then a computer can guess it
  - Computers can often guess very quickly
  - Easy to mount offline attacks

Something I Have

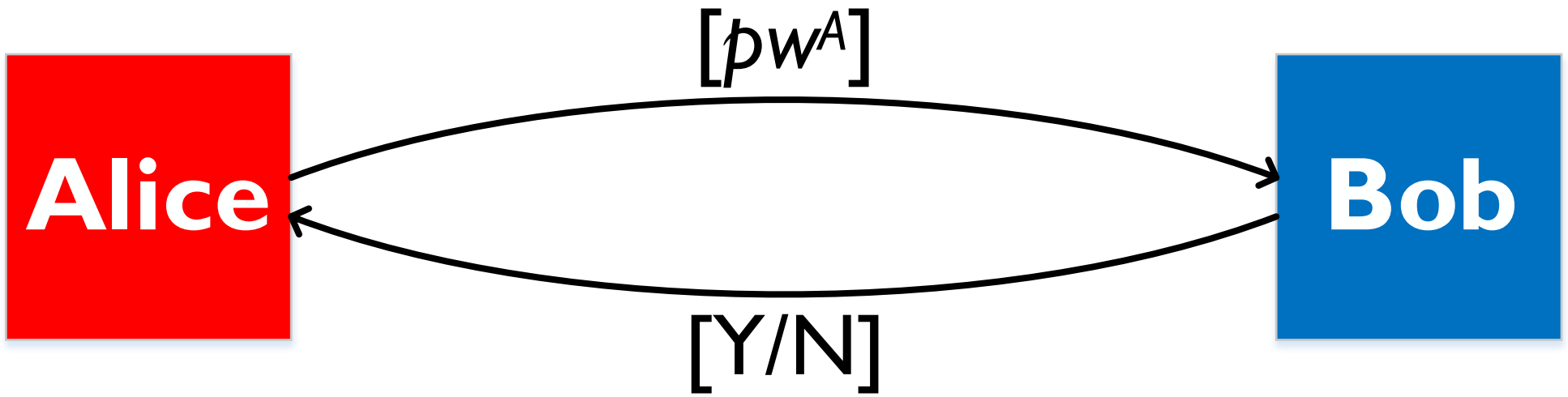
- Keys
- Tokens (transponders, …)
  - Speedpass, EZ-pass, FasTrak
  - SecureID
- Smartcards
  - Embedded CPU and small memory
  - Tamper resistant

Something I am

- Biometrics measure some physical characteristic
  - Fingerprint, face recognition, retina scanners, voice, DNA
  - Can be extremely accurate and fast
- Issues with biometrics?
  - Revocation – lost fingerprint?
  - "fuzzy" credential, e.g., your face changes based on mood ...

Login

- Bob wants to authenticate Alice's identity
  - Alice sends her name and password in cleartext to Bob

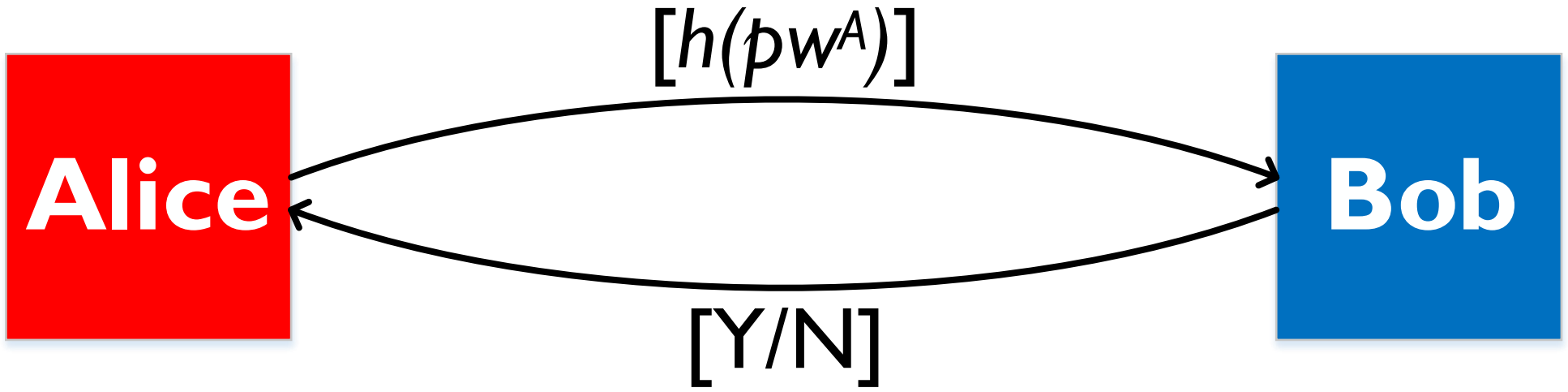


Attacks

- Eavesdropping
  - The attacker can impersonate Alice if he eavesdrops and obtains Alice's password
- Database reading
  - The attacker can impersonate Alice if he can read Bob's database
- Online guessing

Login

- Bob wants to authenticate Alice's identity
  - Alice sends the hash result of her password to Bob

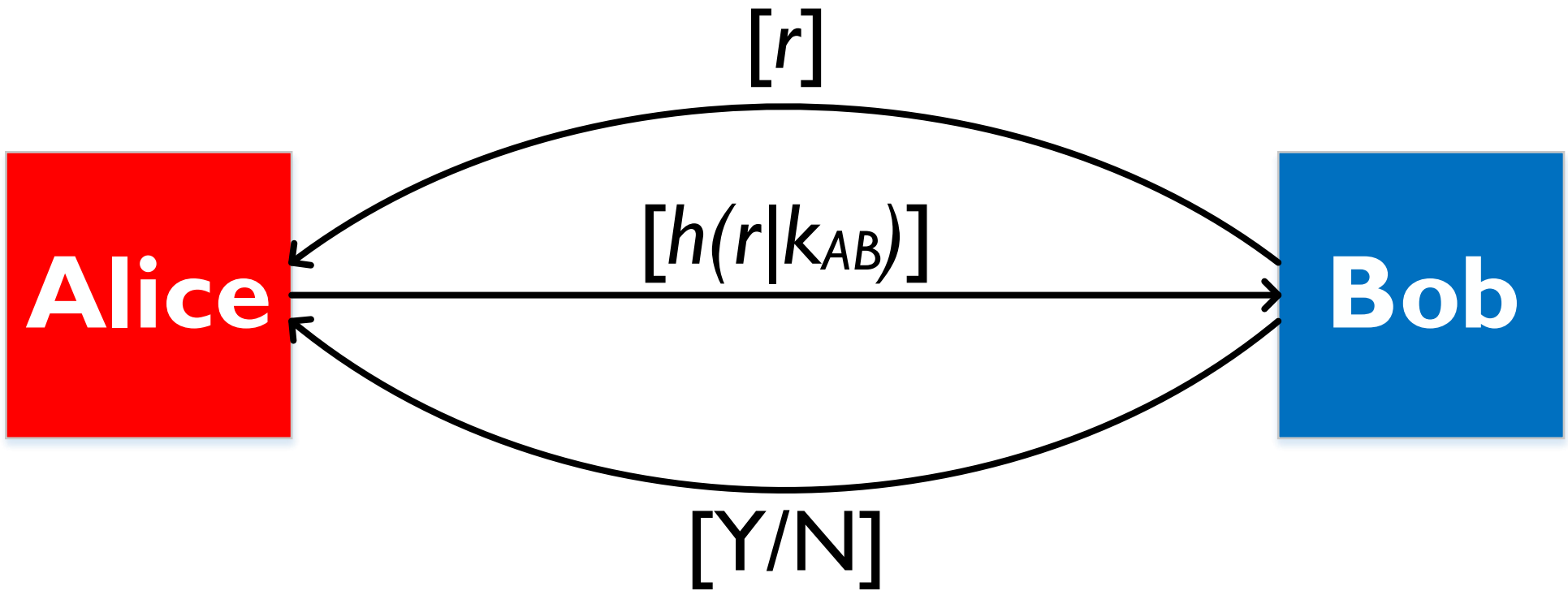


Attacks

- Eavesdropping
  - The attacker can impersonate Alice if he eavesdrops and obtains the hash result of Alice's password
- Online guessing
- Offline guessing
  - The attacker captures the hash result of Alice's password and tries to guess Alice's password from it
- Difference between online guessing and offline guessing

Login

- Bob wants to authenticate Alice's identity
  - Bob sends Alice a random number. Alice computes the hash result on the random number and the shared secret key, and sends the result to Bob

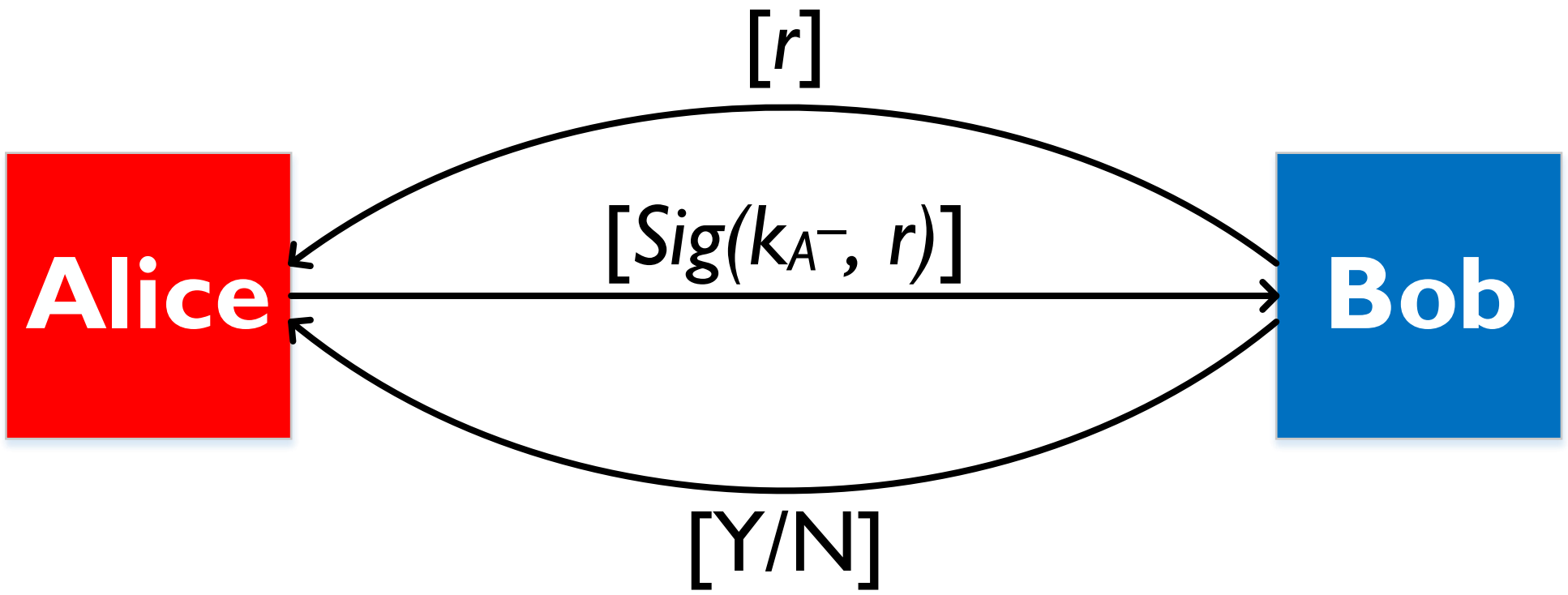


Pros and Cons

- Use random challenges (i.e., random number *r*) to resist eavesdropping
- Cryptographic functions can effectively resist online and offline guessing attacks
- Database reading
  - The attacker can impersonate Alice if he can read the shared secret key k_{AB} from Bob's database

Login

- Bob wants to authenticate Alice's identity
  - Bob sends Alice a random challenge. Alice computes the digital signature on the challenge using her private key, and sends the result to Bob. Bob verifies the signature with Alice's public key.

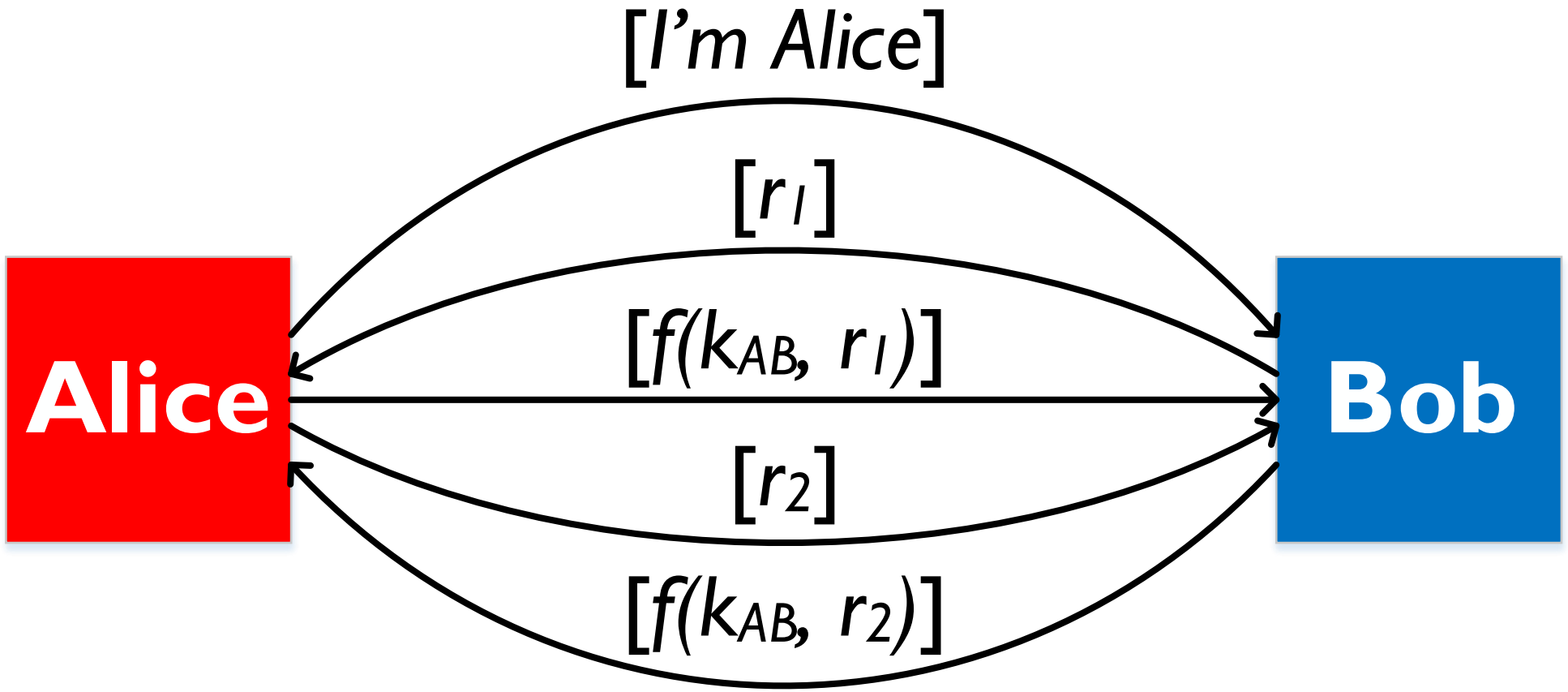


Pros and Cons

- This solution can resist both eavesdropping and database reading attacks (why?)

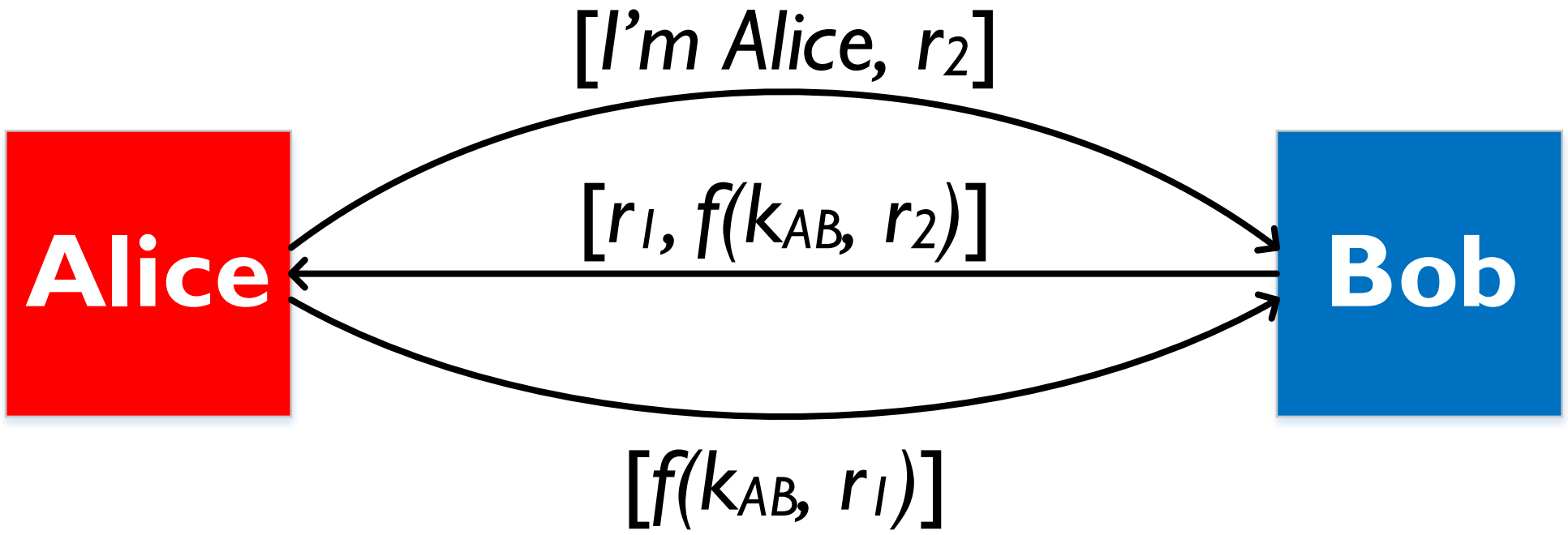
Mutual Authentication

- Alice and Bob want to authenticate the identity of each other



Simplified Solution

- Alice and Bob want to authenticate the identity of each other



Reflection Attack

[*I'm Alice*, r_2]

[r_1, $f(k_{AB}, r_2)$]

Bob

[*I'm Alice*, r_1]

[r_3, $f(k_{AB}, r_1)$]

Bob

Reflection Attack

[*I'm Alice*, r_2]

[r_1, $f(k_{AB}, r_2)$]

[$f(k_{AB}, r_1)$]

Bob

[*I'm Alice*, r_1]

[r_3, $f(k_{AB}, r_1)$]

Bob

Solutions

- PRINCIPLE 1: Do not have Alice and Bob do exactly the same thing
  - Different keys: Have the key used to authenticate Alice be different from the key used to authenticate Bob. E.g., Alice uses k_{AB} and Bob uses $k_{AB}+1$
  - Different challenges: The challenge from Alice looks different from the challenge from bob. E.g., Alice sends an odd number and Bob uses an even number
- PRINCIPLE 2: The initiator should be the first to prove its identity

Midterm

- Time: 19:00-21:30PM, Tuesday, 3/15
- Location: TH429
- Closed-book, closed-notes
- Cover all lecture material and homework assignments
- Include choice questions and short answer questions

Midterm Review

- Problems
  - C-I-A Triad
  - Security Model
- Tools
  - Secret Key Cryptography
  - Public Key Cryptography
  - Hash Function
- Applications

Midterm Review

- C-I-A Triad
  - Confidentiality, Integrity, and Availability
  - Examples
- Security Model
  - Thread model + Trust model

Midterm Review

- Cryptosystem *(E, D, M, K, C)*
- Secret Key Cryptography
  - Definition
  - Transposition cipher and substitution cipher
  - Caesar cipher
  - One-time Pad
  - DES
  - ECB and CBC
  - Brute-force attack

Midterm Review

- Hash Function
  - One-way and collision resistant
  - Message Authentication Code
- Public Key Cryptography
  - Definition
  - RSA
  - Digital Signatures
  - Diffie-Hellman Protocol
  - Man-in-The-Middle attack

Midterm Review

- Data Confidentiality
  - SKC solution and PKC solution
- Data Integrity
  - SKC solution and PKC solution
- Authentication
  - Identities and Credentials
  - Pros and Cons of different authentication mechanisms
  - Reflection attack