Introduction to Modern Cryptography

Benny Chor

Identification (User Authentication)
Fiat-Shamir Scheme

Lecture 12

Tel-Aviv University

4 January 2010

Model and Major Issues

- Alice wishes to prove to Bob her identity, in order to access a resource, obtain a service, etc.
- Bob may ask the following:
  - Who are you? (prove that you are Alice)
  - Who the &$@* is Alice?
- Eve wishes to impersonate Alice:
  - One time impersonation.
  - Full impersonation (identity theft).

Different Scenarios where Identification Required

- Local identification (identified person is present)
  - Human authenticator.
  - Device (*e.g.* BGU airport; Entry points to the US).

- Remote identification
  - Human authenticator
  - Corporate environment (*e.g.* over a LAN)
  - E-commerce environment
  - Cable TV/Satellite: Pay-per-view; subscription verification
  - Remote login or e-mail from an internet cafe.

Initial Authentication is Highly Vulnerable

- The problem: how does Alice initially convince anyone that she is indeed Alice?
- Solution must often involve a ?real-world? type of authentication – ID card, driver's license, etc.
- Errors due to the human factor are quite frequent.
- A famous incident took place in 2001, when VeriSign, the largest digital-signature certificate authority, was tricked into issuing Class 3 code-signing digital certificates to someone fraudulently claiming to work for Microsoft.
- Even in scenarios where OK for Alice to be whoever she claims she is, may want to at least make sure Alice is human (implemented, e.g. for new users attempting to join Yahoo mail).

Closed Environments

- The initial authentication problem is fully solved by a trusted party, Carol.
- Carol can distribute the identification material in a secure fashion, e.g by hand, or over encrypted and authenticated lines.
- Example – a corporate environment.
- Eve's attack avenue is the Alice-Bob connection.
- We begin by looking at remote authentication, using a specific scheme.

Fiat-Shamir Identification Scheme

- Initialization.
- Set Up.
- Basic Construction.
- Improved Construction.
- Zero Knowledge.
- Removing Interaction.

Fiat-Shamir: Initialization

- Bob gets from Carol $N = pq$ but not its factorization.
- Alice picks m numbers $R_1, R_2, \ldots, R_m$ in Z_N at random.
- Alice computes $S_1 = R_1^2 \pmod N$, ..., $S_m = R_m^2 \pmod N$.
- Alice gives $S_1, \ldots, S_m$ to Bob.
- She keeps $R_1, \ldots, R_m$ secret.

Fiat-Shamir: Set Up

- Bob holds $S_1, \ldots, S_m$.
- Alice keeps $R_1, \ldots, R_m$ secret.

- Who is Alice?
- Anyone who can convince Bob she can produce square roots $\mod N$ of $S_1, \ldots, S_m$ to Bob.
- She keeps $R_1, \ldots, R_m$.

- A stupid way to convince Bob: Send him $R_1, \ldots, R_m$.
- Instead, we seek a method that will give Bob (and Eve) nothing more than being convinced Alice can produce these square roots. (hint: zero knowledge).

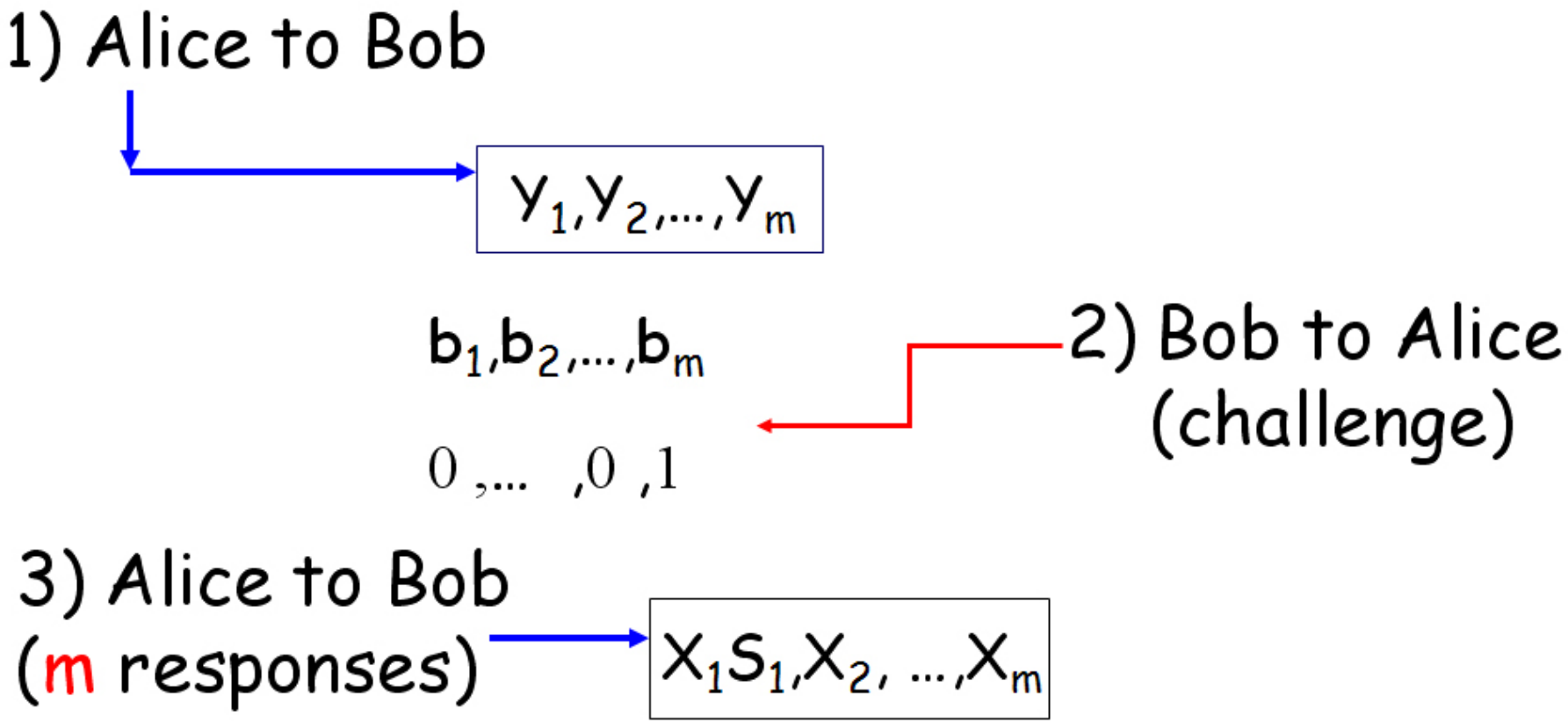
Fiat-Shamir: Basic Protocol

- Let $S_1 = R_1^2 \pmod N$ such that Alice holds R_1.
- To convince Bob that Alice knows a square root $\mod N$ of S_1, Alice picks at random $X_1 \in Z_N$, computes $Y_1 = X_1^2 \pmod N$, and sends Y_1 to Bob.
- Alice to Bob:
  - I know both a square root $\mod N$ of Y_1 (which equals X_1) and a square root $\mod N$ of $Y_1 S_1$ (which equals $X_1 R_1$).
  - Thus I know a square root $\mod N$ of S_1 (which equals R_1). But I'm not going to reveal it.
  - Instead, you (Bob) should make a choice which of the two you want me to reveal.
- Bob flips a coin. The outcome (heads/tails) determines the challenge he poses to Alice.

Fiat-Shamir: Basic Protocol, cont.

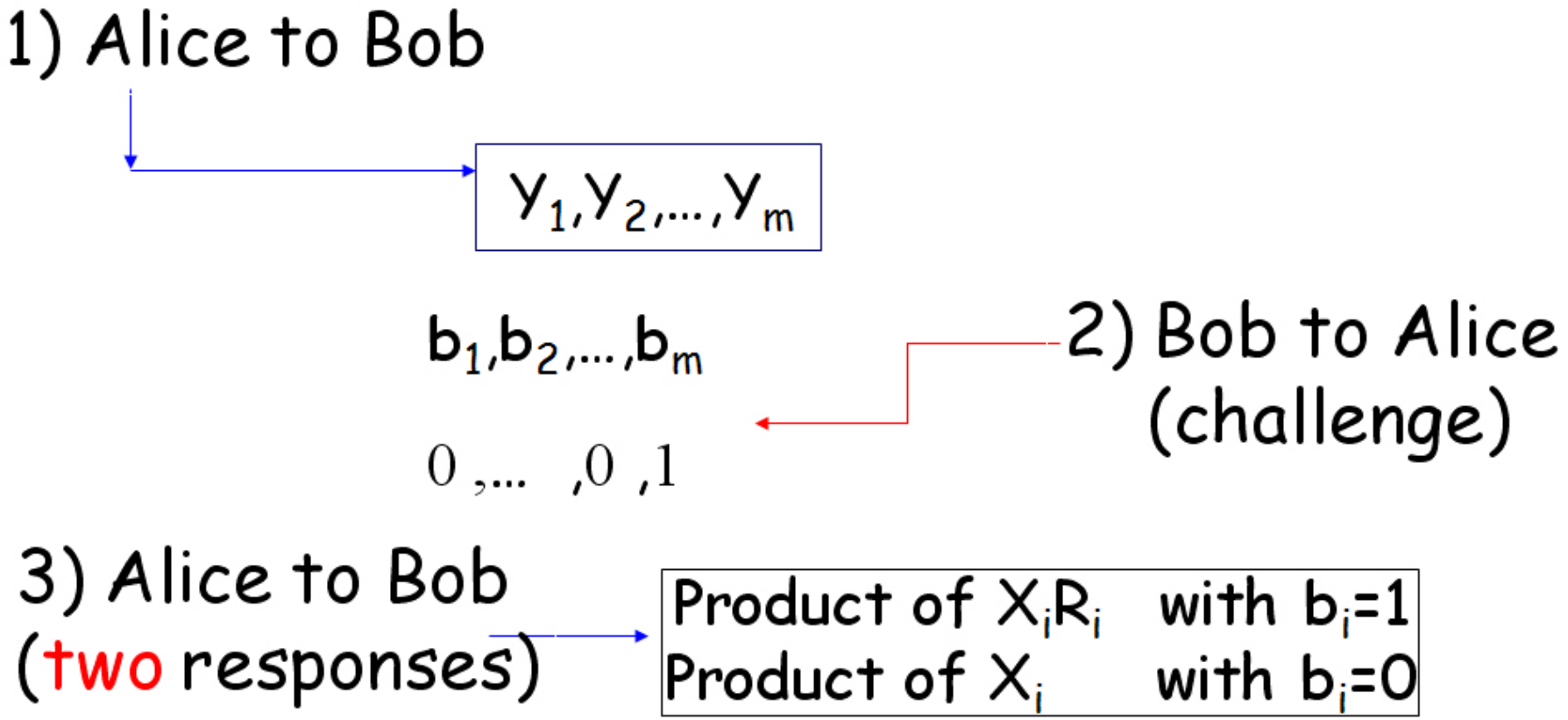
- If Alice knows both a square root of Y_1 (*e.g.* X_1) and a square root $\mod N$ of $Y_1 S_1$ (*e.g.* $X_1 R_1$) then she knows R_1.
- Thus is she does not know a square root of S_1, she does not know at least one of the two square roots above.
- In such case, Bob will catch her cheating with probability at least $1/2$.
- In the protocol, Alice will produce $Y_1, Y_2, \ldots, Y_m$.
- Bob will flip m coins $b_1, b_2 \ldots, b_m$ as challenges.
- Bob accept only if Alice succeeds in all m cases.

Basic Protocol



Bob accepts iff all m challenges are met.

Improved (more efficient) Protocol



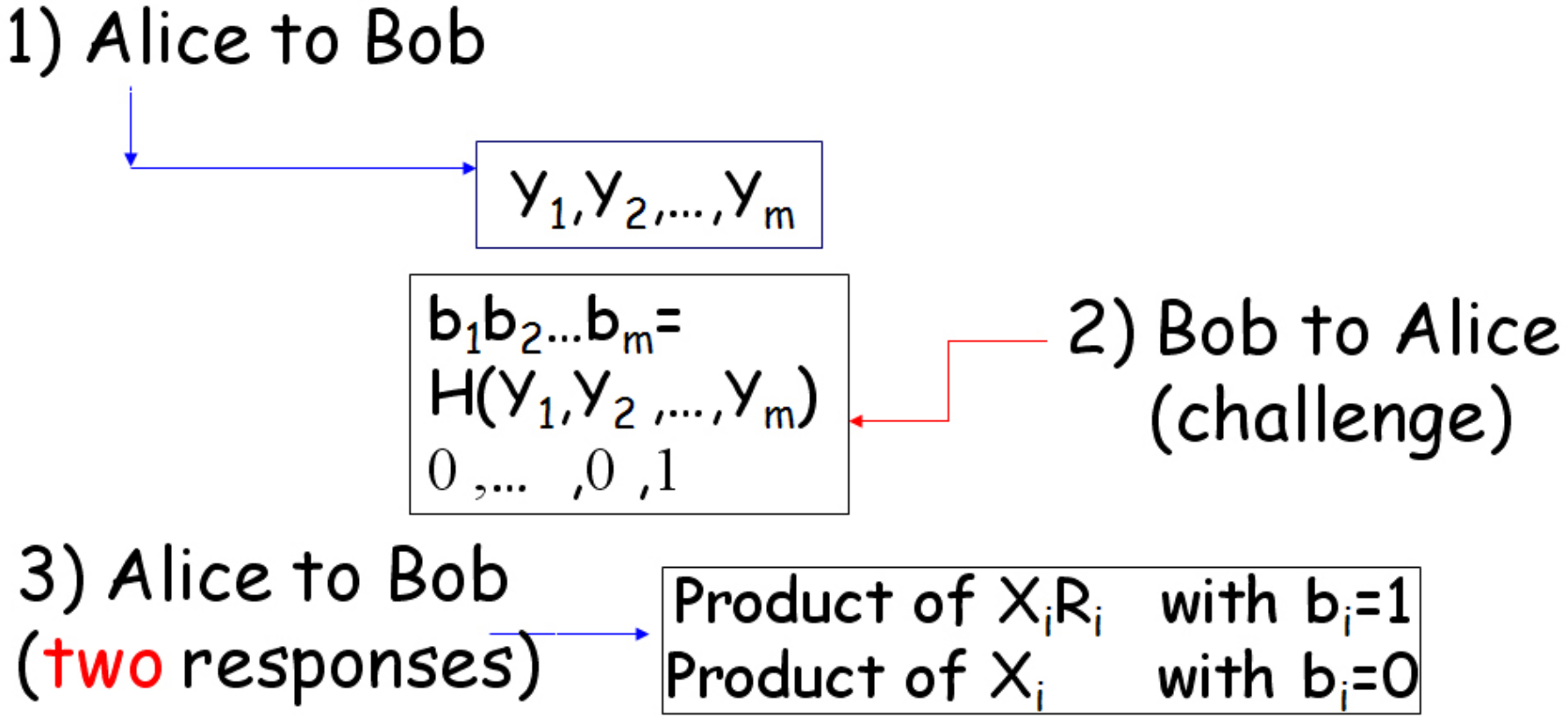
Bob accepts iff two challenges are met.

Correctness of Protocol (Intuition Only)

- A cheating Eve, without knowledge of R_is, will be caught with very high probability.
- Zero Knowledge: By eavesdropping, Eve learns nothing (all she learns, she can simulate on her own).

- Crucial ingredients:
  1. Interaction.
  2. Randomness.

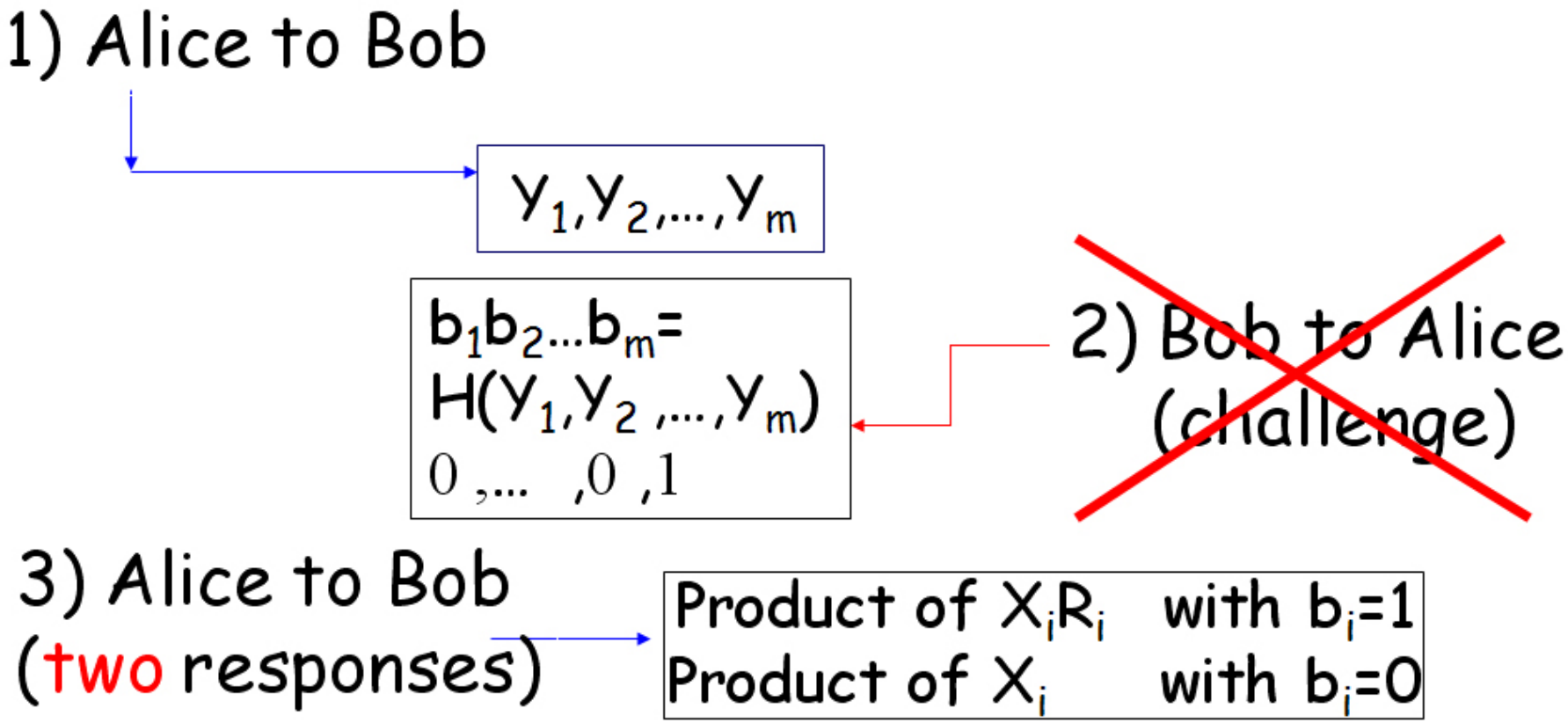
Fiat-Shamir: Final Improvement (more efficient) Protocol



Bob accepts iff two challenges are met.

Fiat-Shamir: Final Improvement – Removing Interaction

Let H be a cryptographically secure hash function.



Bob accepts iff two challenges are met.

Correctness of Protocol (Intuition Only)

- A cheating Eve, without knowledge of R_is, cannot succeed in producing, with non-negligible probability $Y_1, Y_2, \ldots, Y_m$ that will be hashed to a convenient bit vector $b_1, b_2, \ldots, b_m$.
- This is because m is long and H behaves like a random function (so the chances of hitting a bit vector favorable to Eve are negligible).

- Remark: Fiat-Shamir scheme (the improved version) is used in practice.