ENEE 457: Computer Systems Security
10/12/16

Lecture 12
Security Protocols I: TLS and Zero-Knowledge Proofs

Charalampos (Babis) Papamanthou

Department of Electrical and Computer Engineering
University of Maryland, College Park

TLS protocol

- TLS provides transport layer security for Internet applications
- It provides for confidentiality and data integrity over a connection between two end points

- Advantage of TLS
  - applications can use it transparently to securely communicate with each other
  - TLS is visible to applications, making them aware of the cipher suites and authentication certificates negotiated during the set-up phases of a TLS session

14.2 TLS Record Protocol

- TLS Record Protocol layers on top of a reliable connection-oriented transport, such as TCP
- TLS Record Protocol
  - provides data confidentiality using symmetric key cryptography
  - provides data integrity using a keyed message authentication checksum (MAC)
- The keys are generated uniquely for each session based on the security parameters agreed during the TLS handshake

- Basic operation of the TLS Record Protocol
  1. read messages for transmit
  2. fragment messages into manageable chunks of data
  3. compress the data, if compression is required and enabled
  4. encrypt the data
  5. calculate a MAC
  6. transmit the resulting data to the peer

- At the opposite end of the TLS connection, the basic operation of the sender is replicated, but in the reverse order
  1. read received data from the peer
  2. verify the MAC
  3. decrypt the data
  4. decompress the data, if compression is required and enabled
  5. reassemble the message fragments
  6. deliver the message to upper protocol layers

14.3 TLS Handshake Protocol

- TLS Handshake Protocol is layered on top of the TLS Record Protocol
- TLS Handshake Protocol is used to
  - authenticate the client and the server
  - exchange cryptographic keys
  - negotiate the used encryption and data integrity algorithms before the applications start to communicate with each other

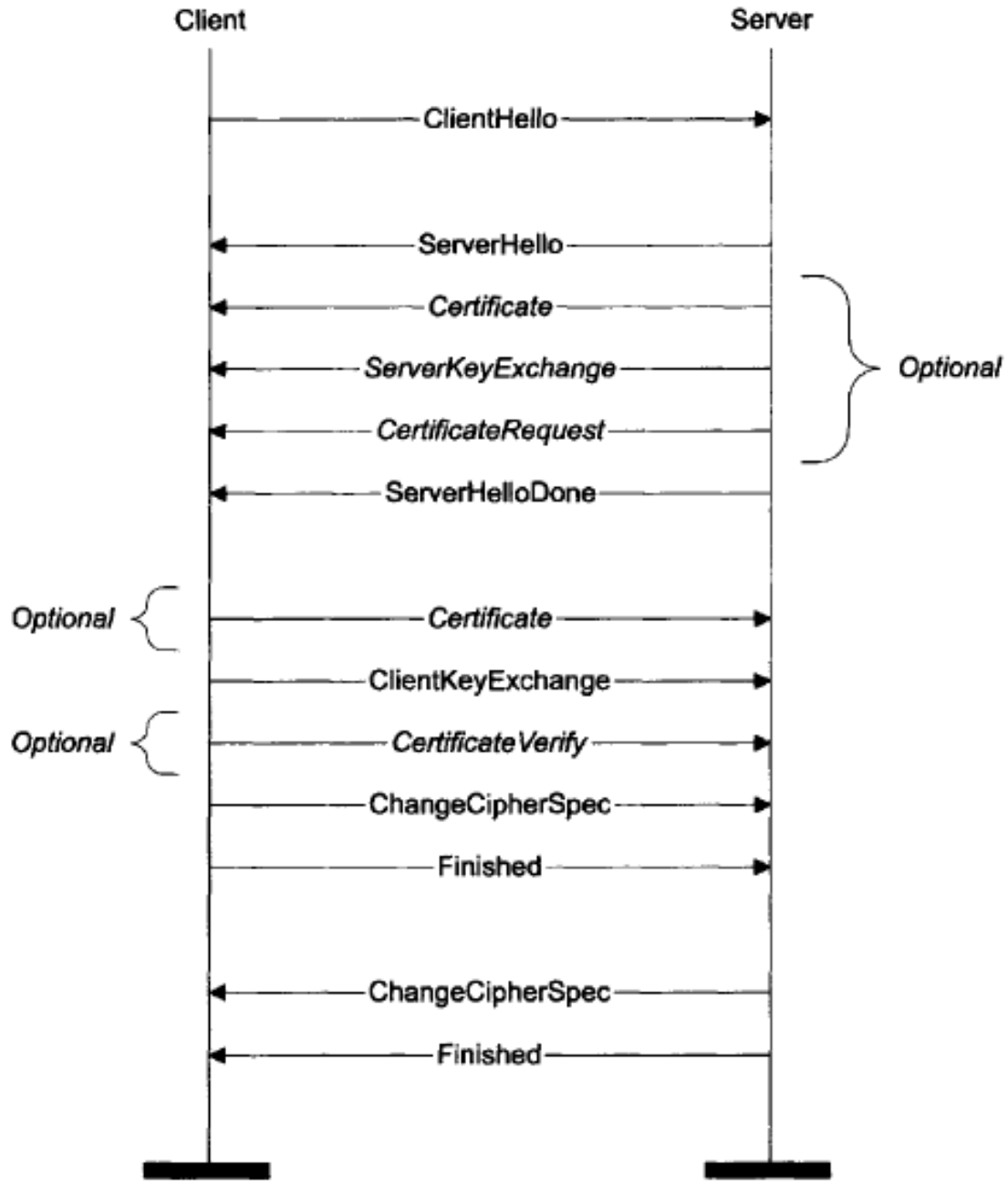


Figure 14.1 The TLS handshake.

Summary

- TLS protocol provides transport layer security for Internet applications and confidentiality using symmetric key cryptography and data integrity using a keyed MAC
- It also includes functionality for client and server authentication using public key cryptography

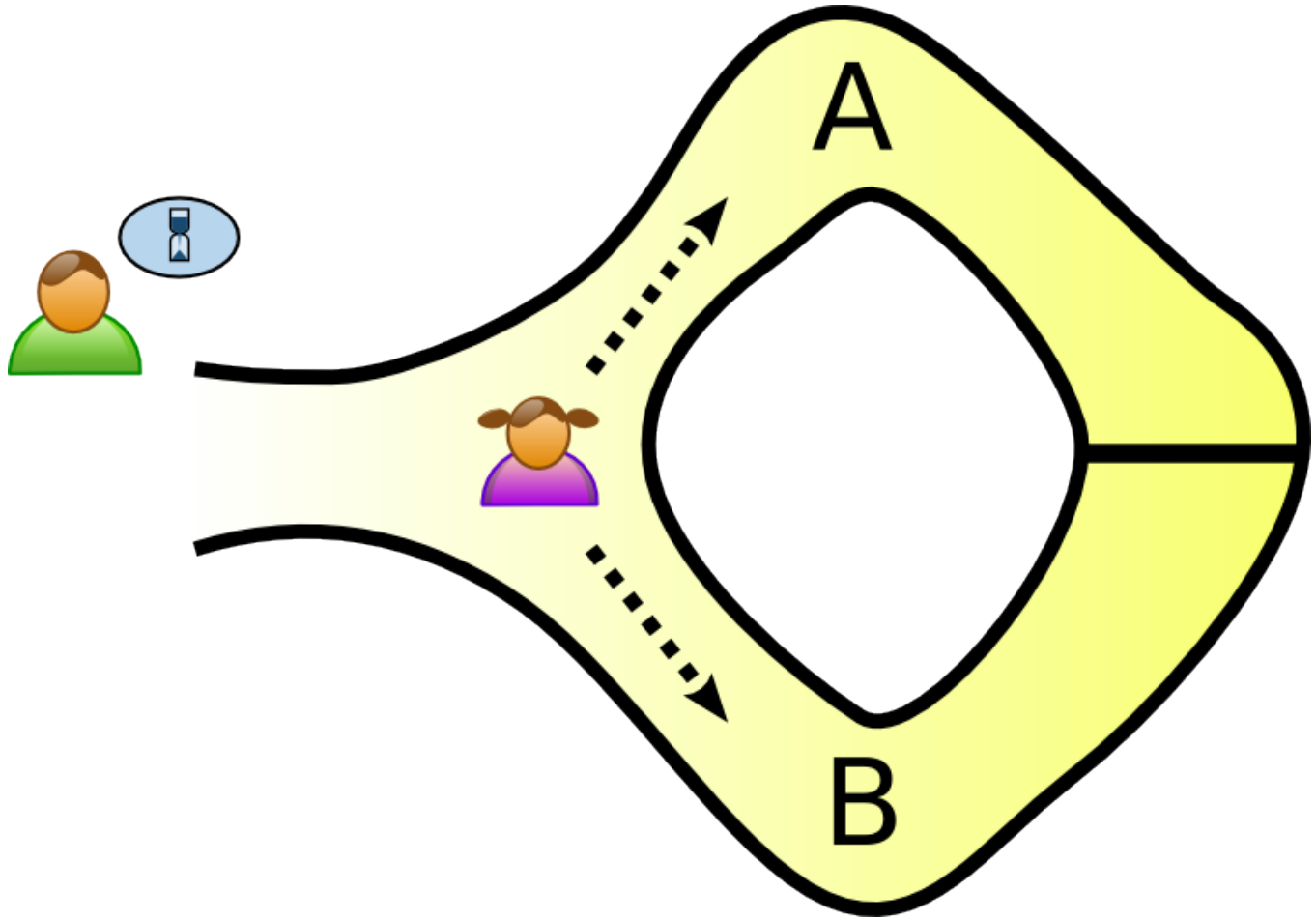
Zero-Knowledge Proofs

- An interactive proof system involves a prover and a verifier
- The prover proves he knows something to the verifier without revealing it
- Application: Log into a server without revealing your password

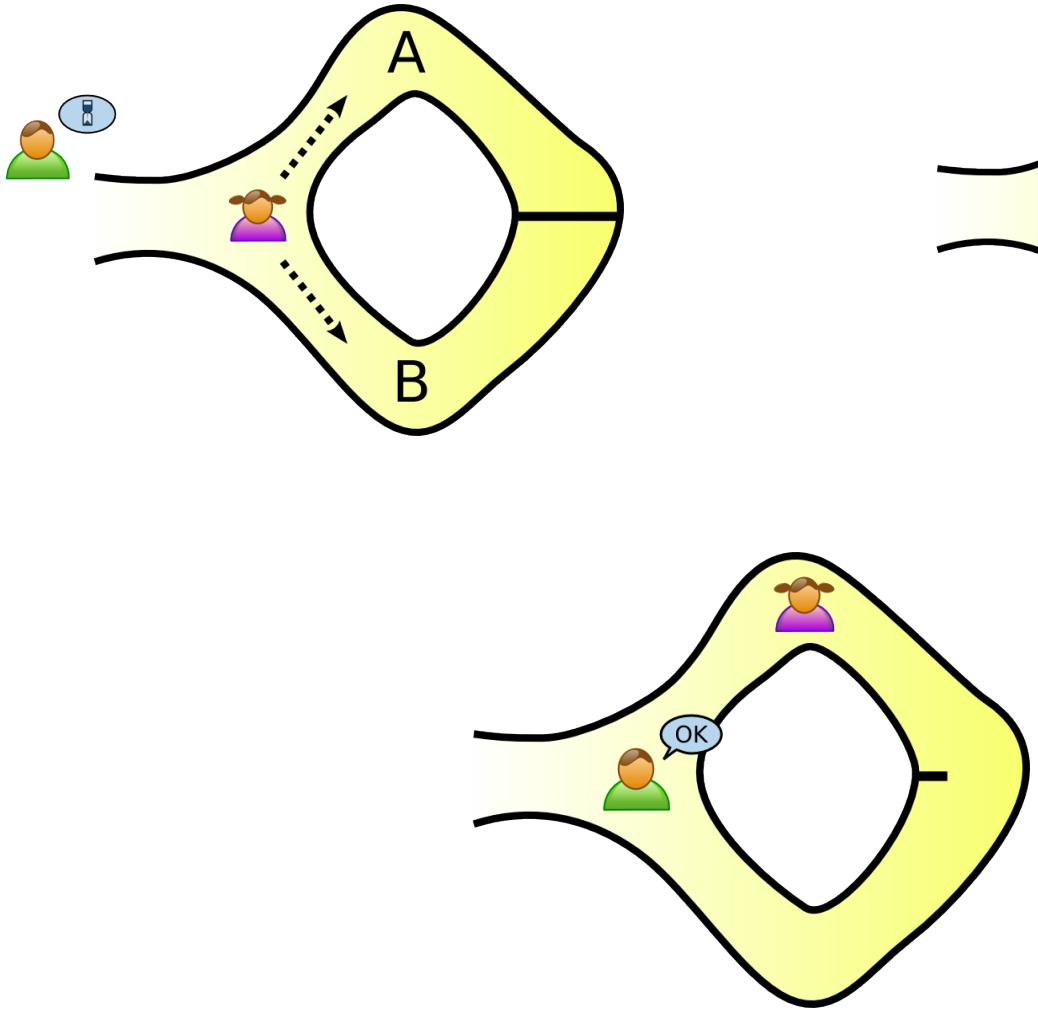
Properties of ZKPK

- Completeness
  - If both prover and verifier are honest, protocol succeeds with overwhelming probability
- Soundness
  - No one who does not know the secret can convince the verifier (except with very small probability)
    - Intuition: the protocol should not enable prover to prove a false statement
- Zero knowledge
  - The proof does not leak any information

An example (wikipedia)

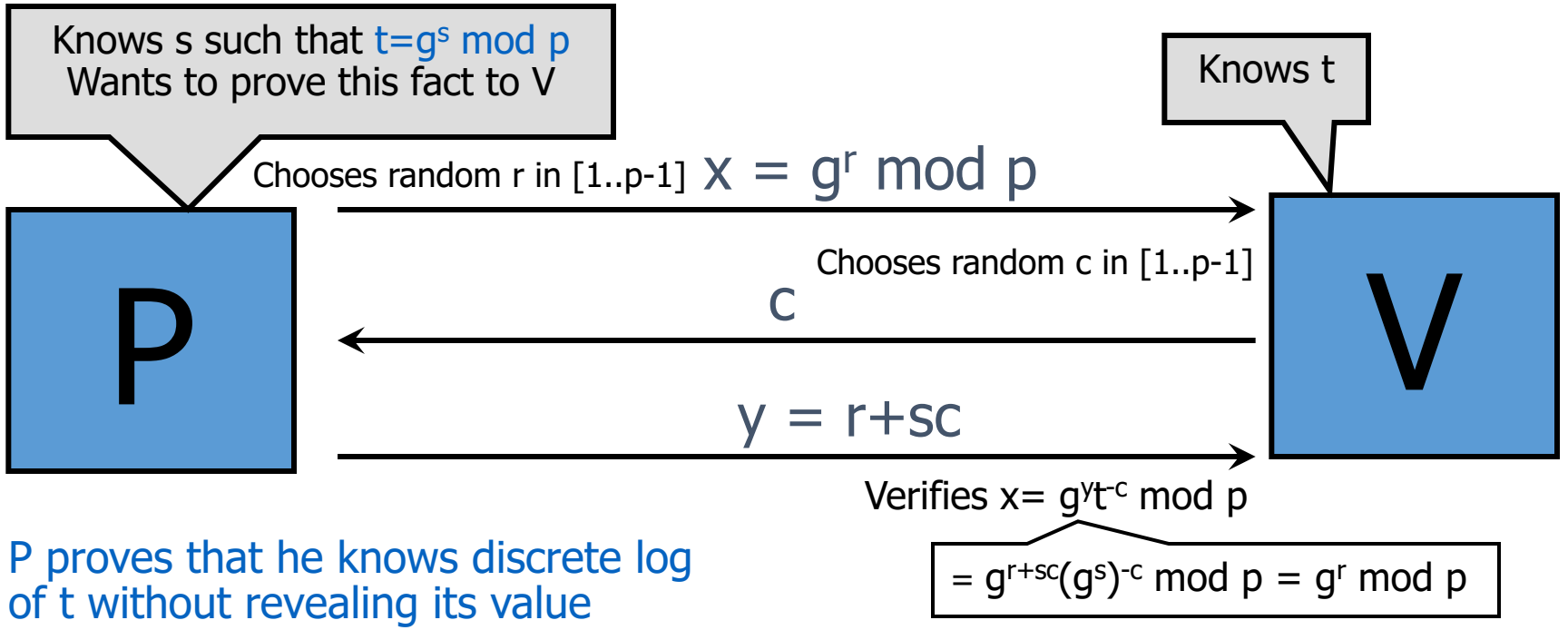


An example (wikipedia)



Schnorr's Id Protocol

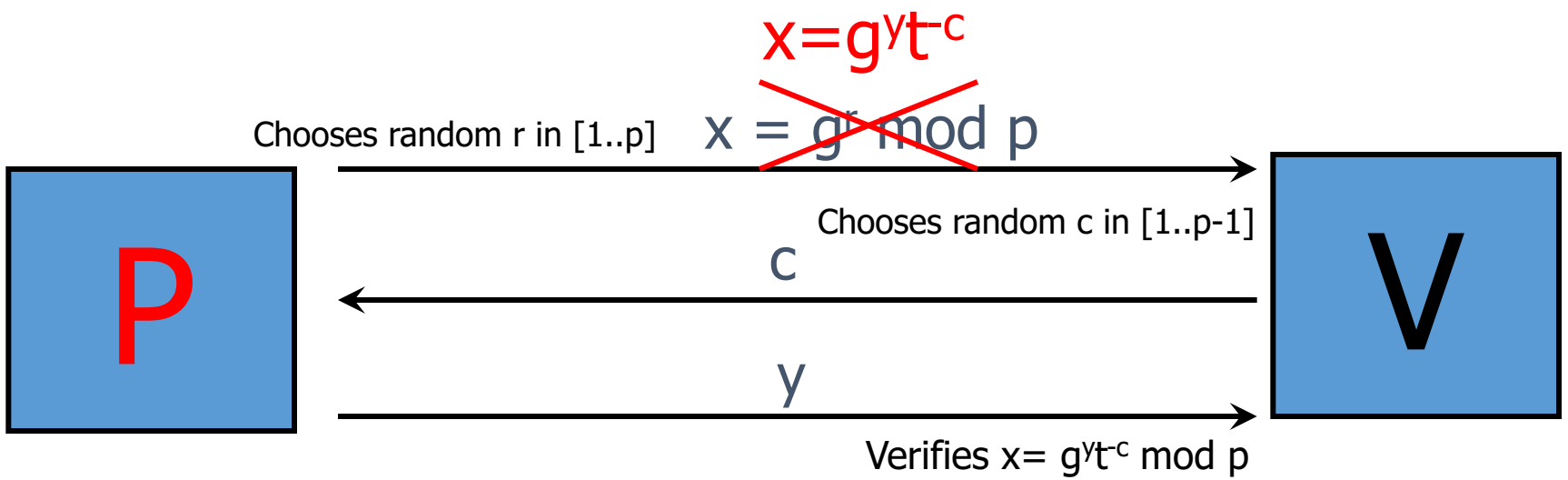
- System parameters
  - Prime p
  - g is a generator of Z_p^*



P proves that he knows discrete log of t without revealing its value

Cheating Prover

- Prover can cheat if he can guess c in advance
  - Guess c, set $x=g^y t^{-c}$ for random y in 1st message
  - What is the probability of guessing c?



P proves that he "knows" discrete log of t even though he does not know s