


6G7Z1009: Introduction to Computer Forensics and Security

Zero Knowledge


Outline

- What is Zero-Knowledge Proofs?
- Why Zero-Knowledge Proofs
- Interactive Proofs
- Zero Knowledge proofs
- Application: Fiat-Shamir Protocol


What is Zero Knowledge Proof ?

- Zero-knowledge proof system only does authentication. It allows you to prove that you know a secret (something associated with your public key) without actually revealing the secret. A zero-knowledge proof is a proof of some statement which reveals nothing other than the truth of the statement.
- Can you think of any cryptographic algorithm that is a zero-knowledge proof system?

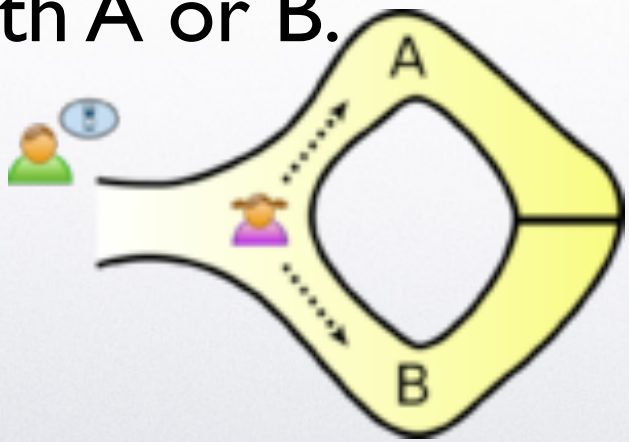
RSA is a Zero-knowledge proof system in the sense that you can prove you know the secret associate with your public key without revealing your private key


Why Zero Knowledge Proof ? - I

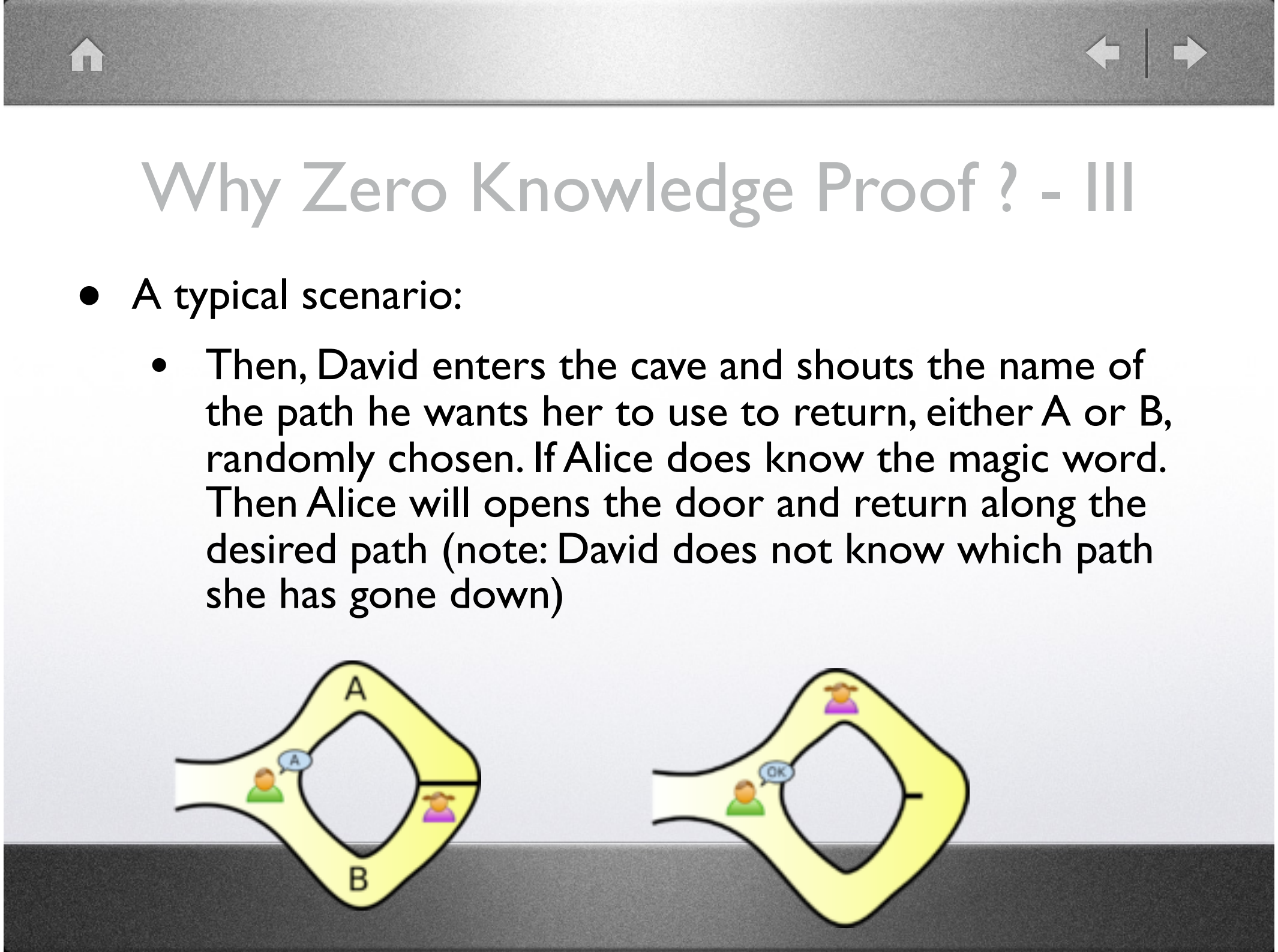
- A typical scenario:
  - Alice has uncovered the secret word used to open a magic door in a cave. The cave is shaped like a circle, with the entrance on one side and the magic door blocking the opposite side.
  - David says he will pay for her for the secret, but not until he is sure that she really knows it
  - Alice says she'll tell her secret until she receives the money
  - Communication among mutually distrusting parties
  - They devise a scheme: Alice can prove that she knows the secret without leaking any secret information to David

Why Zero Knowledge Proof ? - II

- A typical scenario:
  - First, David waits outside the cave as Alice goes in. They label the left and right paths from entrance A and B. Alice randomly takes either path A or B.



source : http://en.wikipedia.org/wiki/Zero-knowledge_proof#cite_note-0



Why Zero Knowledge Proof ? - III

- A typical scenario:
  - Then, David enters the cave and shouts the name of the path he wants her to use to return, either A or B, randomly chosen. If Alice does know the magic word. Then Alice will opens the door and return along the desired path (note: David does not know which path she has gone down)


Why Zero Knowledge Proof ? - IV

- A typical scenario:
  - However, suppose Alice did not know the secret word. Then, she would only be able to return by the named path if David were to give the name of the same path Alice entered by. Since David choose A and B randomly, Alice has a 50% of guessing correctly. If it repeats many times, for instance, 3 times, the probability of guessing will be reduced to 1/8.
  - If Alice can appear at the exit David names, David can conclude she know the secret word


Interactive Proofs - I

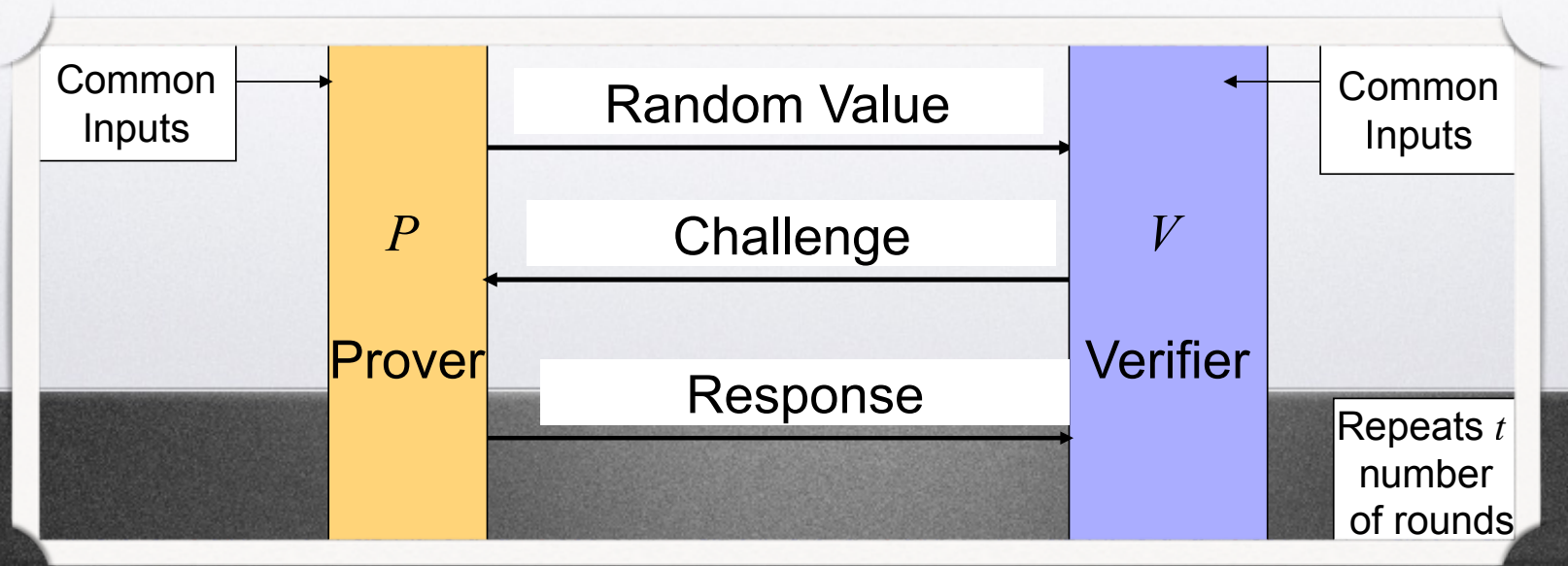
- Two parties (a prover and a verifier) in Zero Knowledge proof are interactive.
- The prover is to convince the verifier the truth of an assertion, e.g., claimed knowledge of a secret.
- The verifier either accepts or rejects the proof. Zero knowledge proofs are instances of interactive proof systems.


Interactive Proofs - II

- To prove is to convince the verifier of some assertion (i.e., prove that you know a secret value ***S***)
- Each party in the protocol does the following:
  - Receive a message from the other party
  - Perform a private computation
  - Send a message to the other party
- Repeats *t* number of rounds


Interactive Proofs - III

- Prover and verifier share common inputs (functions or values)
- The protocol yields Accept if every Response (e.g., a correct password) to the challenge (e.g., asking for a password) is accepted by the verifier
- Otherwise, the protocol yields Reject




Interactive Proofs - IV

- A proof: simply, a proof or equivalently a "proof system" is a randomised protocol by which one party (called the prover) wishes to convince another party (called the verifier) that a given statement is true
  - Mathematically, a proof is a fixed sequence of statements flowing logically
  - In real life, not fixed, but a process by which validity is established, such as cross-examination of a witness.


Interactive Proofs - V

- Interactive proofs used for identification can be formulated as proofs of knowledge.
  - A possesses some secret s, and attempts to convince B it has knowledge of s, by correctly responding to queries which requires knowledge of s, to answer
  - Note that proving knowledge of s differ proving that such s exists.
  - An interactive proof is said to a proof of knowledge if it has both properties of completeness and soundness


Interactive Proofs - VI

- Properties of an interactive proof system
  - Completeness: I'll believe all true statements;
    - Given an honest prover and an honest verifier, if the statement is true, the verifier will be convinced of this fact by an honest prover(i.e., the verifier accepts prover's claim)
  - Soundness: I will never believe a false statement
    - If the statement is true, no cheating prover can convince the honest verifier that it s true, except with some small probability. Note here, in an interactive proof system, we trust the verifier


Zero Knowledge Proofs - VII

- Zero knowledge must satisfy three properties: completeness, soundness and zero knowledge
- Zero knowledge:
  - If the statement is true, no cheating verifier learns anything other than this fact. This is formalised by showing that every cheating verifier has some simulator that can produce a produce a transcript that "looks like" an interaction between the honest prover and the cheating verifier.
  - Note: no access to the prover


Zero Knowledge Proofs - VIII

- Further explanation of Zero knowledge proofs
  - Consider an observer C who witness a zero knowledge interactive proof (ZKIP) involving a prover P convincing a verifier V of some knowledge P has.
  - The proof to V does not guarantees to C. Similarly, a recorded ZKIP conveys no guarantees upon playback.
  - The proofs is simulatable by a verifier along


Zero Knowledge Proofs - IX

- Further explanation of Zero knowledge proofs
  - For every verifier interacting with a prover, there is a simulator
  - The simulator does not have access to the interactive prover, but it can simulate the interaction between the prover and the verifier
  - The verifier did not gain any knowledge from the prover since the same output could have been generated without any access to the prover


Zero Knowledge Proofs - X

- Further explanation of Zero knowledge proofs
  - For every verifier interacting with a prover, there is a simulator
  - The simulator does not have access to the interactive prover, but it can simulate the interaction between the prover and the verifier
  - The verifier did not gain any knowledge from the prover since the same output could have been generated without any access to the prover


Application: Fiat-Shamir Protocol -I

- Alice is known to possess, e.g., a password
- Problems
  - The authenticator must be trusted
  - The secret sniffed or given to untrusted party, attackers can impersonate
- Use zero knowledge


Application: Fiat-Shamir Protocol - II

- One time setup
  - A trusted center selects two large prime integer p and q, computes $n=pq$, and publishes n while p and q are kept secret
  - Creates secret number $\{s_i, i=1,...k\}$, and computes $v_i=s^2 \bmod n$
  - Alice is sent to the numbers s_i, these are her secret login numbers. David is sent the number v_i.


Application: Fiat-Shamir Protocol - III

- Procedure
  - Alice chooses a random integer *r*, a random sign $s \in \{-1, 1\}$, and compute $x \equiv s \cdot r^2 \pmod{n}$. Alice sends *x* to David.
  - David chooses numbers $a_1, \cdots, a_k$, where a_i equals 0 or 1.
  - Alice computes $y \equiv r s_1^{a_1} s_2^{a_2} \cdots s_k^{a_k} \pmod{n}$ and send it to David
  - David checks $y^2 \equiv \pm x v_1^{a_1} v_2^{a_2} \cdots v_k^{a_k} \pmod{n}$.
  - This procedure is repeated with different *r* and a_i values until David is satisfied that Alice does know the modular square roots (s_i) of his v_i number.


Further references

- Jean-Jacques Quisquater, Louis C. Guillou, Thomas A. Berson. How to Explain Zero-Knowledge Protocols to Your Children. *Advances in Cryptology - CRYPTO '89: Proceedings*, v.435, p.628-631, 1990.
- Austin Mohr, A Survey of Zero-Knowledge Proofs with Applications to Cryptography, 2007