Oblivious Transfer and Zero Knowledge Proofs

CS355 October 18, 2016

Oblivious Transfer

- **Concept**: A sender sends information to a receiver, but remains unaware of what the receiver actually received.
  - Example: a noisy communications channel as in a bad cell phone connection or unstable data connection

- Oblivious Transfer applies the process of finding square roots modulo n (as we did using Chinese Remainder Theorem) in the Rabin-Blum Coin Flipping Protocol.

- Oblivious Transfer protocols are also used in electronic contract signing, secure multiparty communications, or retrieval of sensitive information.

Oblivious Transfer: Rabin Blum Coin Tossing

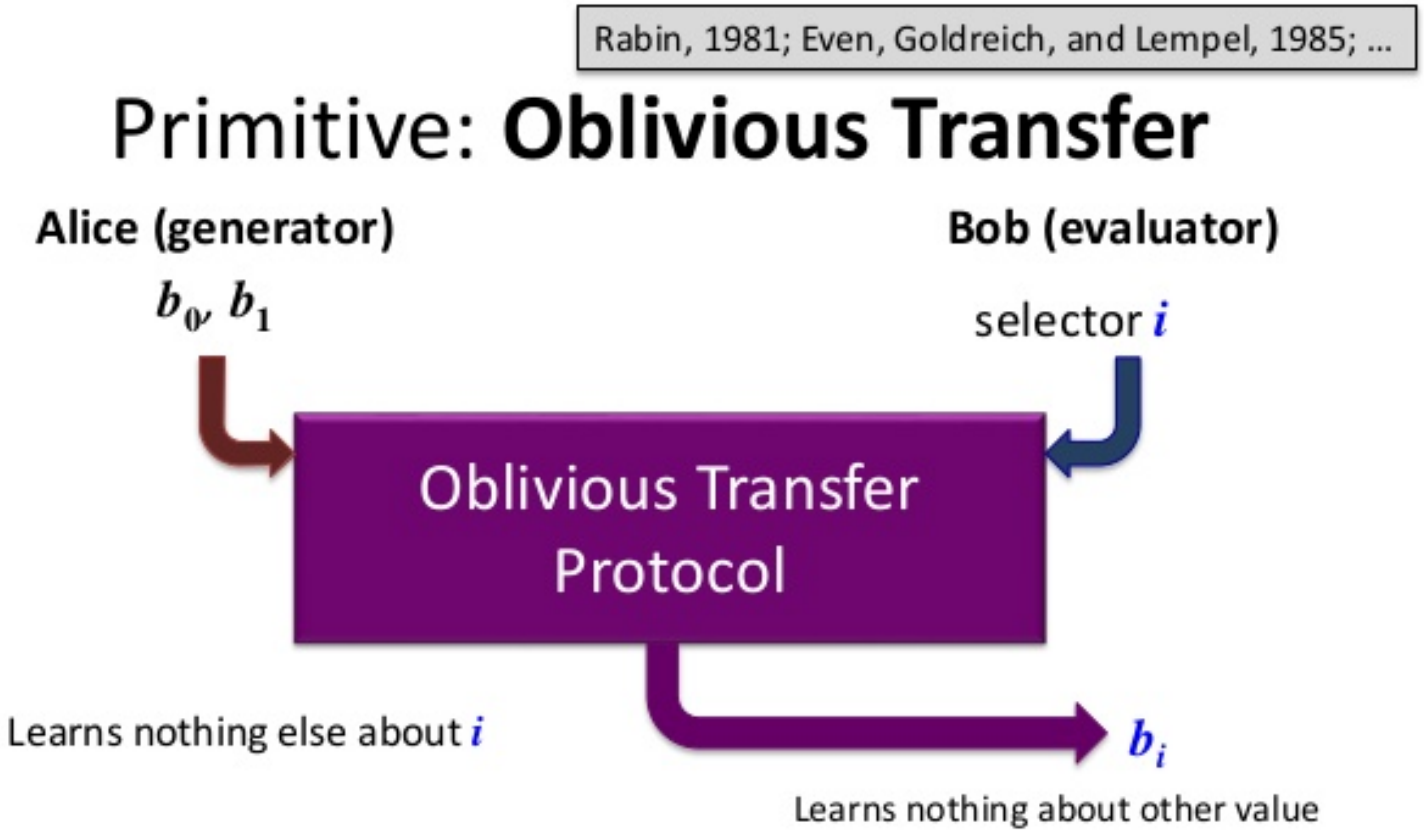
- Alice reveals a secret to Bob with probability 0.5
  - For example, she could put the secret in a hat with one other piece of nonsense information. Bob picks from the hat once Alice leaves and has a 0.5 chance of picking each of the two pieces of information
  - Alice doesn't know whether or not Bob actually got the secret.
  - If Alice must know, OT does not work.

- Bob tells Alice whether he got the secret.

- Bob wins the coin toss if he got the secret, but loses if he did not.

Oblivious Transfer: Rabin Blum Coin Tossing

- Alice generates two bits, $b_0\ and\ b_1$, and gives them to the OT machine. One bit represents her secret.
- Alice learns nothing else about the OT process or Bob's selection.
- Bob uses a selector, i, to pick a bit from the OT machine.
- Bob has a 0.5 probability of randomly learning Alice's secret, but learns nothing else about the process or the other value(s)



Graphic Credit: Dr. David Evans, University of Virginia

Oblivious Transfer: Rabin Blum Coin Tossing

- Alice's secret is the factorization of n, which is the product of two large prime numbers, $n = pq$ where $p \equiv q \equiv 3(mod\ 4)$.

1. Alice sends n to Bob.
2. Bob picks a random x in $\sqrt{n} < x < n$ where $\gcd(x, n) = 1$. He computes $a = x^2\ (mod\ n)$ and sends a to Alice.
3. Alice computes the four solutions to $x^2 \equiv a\ (mod\ n)$, which she can do because she knows p and q.
4. If Bob receives x or $n - x$, he learns nothing. If he receives y or $n - y$, he can factor n by computing $\gcd(x + y, n) = p\ or\ q$

Oblivious Transfer: Activity

- lice's secret is the factorization of n, which is the product of two large prime numbers, $n = pq$ where $p \equiv q \equiv 3(mod\ 4)$.

1. Alice sends n to Bob.
2. Bob picks a random x in $\sqrt{n} < x < n$ where $\gcd(x, n) = 1$. He computes $a = x^2\ (mod\ n)$ and sends a to Alice.
3. Alice computes the four solutions to $x^2 \equiv a\ (mod\ n)$, which she can do because she knows p and q.
4. Bob receives x or $n - x$, he learns nothing. If he receives y or $n - y$, he can factor n by computing $\gcd(x + y, n) = p\ or\ q$

Oblivious Transfer: Theory and Proof

- Why can Bob factor n if he gets y or $n - y$?

  - **Theorem** If $n = pq$ is the product of two distinct primes, and if $x^2 = y^2 \ (mod\ n)$, but $x \not\equiv \pm y \ (mod\ n)$, then $\gcd(x + y, n) = p \ or \ q$.

  - **Proof** We are given that n divides $(x + y)(x - y)$ but not $(x + y)$ or $(x - y)$ individually. As a result, either p or q must divide $(x + y)$ and the other must divide $(x - y)$.

Oblivious Transfer: Secret File Example

- Black = Original Protocol ; Red = Modified for this example

1. Alice enciphers a secret file using AES with a secret key, K, and gives the enciphered file to Bob
2. Alice chooses two large primes $p \equiv q \equiv 3(mod\ 4)$, sets $n = pq$, and chooses $0 < e < n\ with \gcd\big(e, (p-1)(q-1)\big) = 1$. This sets up an RSA public key cipher with public keys n and e. Alice enciphers K as $C = K^e\ (mod\ n)$. Alice gives Bob C and e.
3. Alice sends n to Bob.
4. Bob picks a random x in $\sqrt{n} < x < n$ where $\gcd(x, n) = 1$.
5. Alice computes the four solutions to $x^2 \equiv a\ (mod\ n)$, which she can do because she knows p and q.
6. If Bob learns the factorization of $n = pq$ in Step 4, then Bob finds d with $ed \equiv 1\big(mod\ (p-1)(q-1)\big)$ by extended Euclidean Algorithm. He finds $K = C^d\ (mod\ n)$, and deciphers the file using K as the AES key.

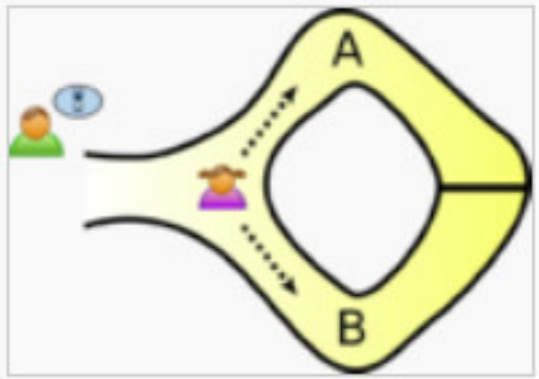
Zero Knowledge Proof

- **Concept**: A party wants to prove to a second party that she knows a secret without revealing to the second party what the secret is
  - Related to Oblivious Transfer.
  - Example: Alice wants to convince Bob that he knows the factors of $n = pq$ without telling him the factors.

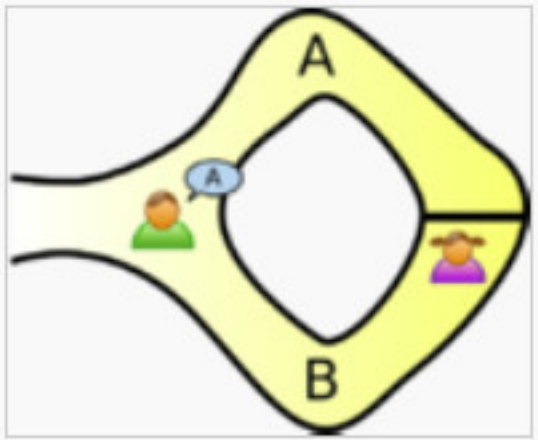
- Alice (the prover) convinces Bob (the verifier) that she knows the prime factorization of a large composite number n, but does not give Bob any hint which would help him find the factors of n. Bob learns nothing about the factorization of n during the protocol that he could not have deduced on his own without Alice's help..

- **How it works, in brief**: Bob gives Alice some quadratic residues modulo n and Alice replies with their square roots. The difficulty with this simple approach is that when Alice replies to Bob with a square root, there is a 50% chance that she will reveal the factorization of n to Bob, as in the oblivious transfer protocol.

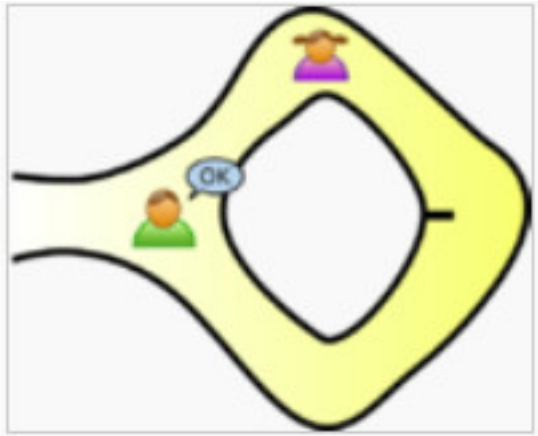
Zero Knowledge Proof: Graphical Example



Peggy randomly takes either path A or B, while Victor waits outside



Victor chooses an exit path



Peggy reliably appears at the exit Victor names

Zero Knowledge Proof: A good protocol

1. Alice chooses a in $\sqrt{n} < a < n$ and computes $b = a^2 \ (mod\ n)$.
2. At the same time, Bob chooses c in $\sqrt{n} < c < n$ and computes $d = c^2 \ (mod\ n)$.
3. Alice sends b to Bob and Bob sends d to Alice.
4. Alice receives d and solves $x^2 \equiv bd \ (mod\ n)$. This is possible because bd is a quadratic residue and she can compute its square root because she knows all the factors of n. Let x_1 be one solution of the congruence.
5. At the same time, Bob tosses a fair coin and gets either Heads or Tails (each with a probability of 0.5). Bob sends H or T to Alice.

Zero Knowledge Proof: A good protocol(cont.)

6. If Alice receives H, she sends a to Bob. If Alice receives T, she sends x_1 to Bob.
7. If Bob sent H to Alice, then he receives a from Alice and checks that $a^2 \equiv b \ (mod\ n)$. If Bob sent T to Alice, then he receives x_1 from Alice and checks that $x_1^2 \equiv bd \ (mod\ n)$.

- Alice and Bob repeat these steps many (20 or 30) times.
- If the check in step 7 is always OK, then Bob accepts that Alice knows the factorization of n.
- If Alice ever fails the test (even once!), then Bob concludes that Alice is lying.

Zero Knowledge Proof: Questions

- Why does this protocol work?

- Why does Bob not learn the factors of n?

Zero Knowledge Proof: Activity

In groups of three, consider the ZKP protocol. Bob wants Alice to prove that she can log into a server. Alice would like to be able to log into the server repeatedly with Bob observing, but doesn't want to share with Bob the secret she uses to log into the server. Create a potential solution using ports on the server as the authentication mechanism.

In your protocol, what is absolutely key to Bob's inability to learn the protocol from his observation?

Diagram your answer and include equations where appropriate. Be prepared to describe your answers to the class.

The activity will last for 20 minutes – no Internet use.