Lecture 10

Public Key Cryptography: Encryption + Signatures

Identification

- Public key cryptography can be also used for IDENTIFICATION
- Identification is an interactive protocol whereby one party: "prover" (who claims to be, say, Alice) convinces the other party: "verifier" (Bob) that she is indeed Alice
- Identification can be accomplished with public key digital signatures
- However, signatures reveal information...
- Also, signatures are "transferable", i.e., anyone can verify them
Fiat-Shamir Identification Scheme

• In Fiat-Shamir, prover has an RSA modulus \( n = pq \) (factorization is secret).

• Factors themselves are not used in the protocol.

• Unlike RSA, a trusted center can generate a global \( n \), used by everyone, as long as nobody knows its factorization. Trusted center can "forget" the factorization after computing \( n \).

Fiat-Shamir Identification Scheme

• Secret Key: Prover (P) chooses a random value 
  \( 1 < S < n \) (to serve as the key)
  such that \( \gcd(S,n) = 1 \)

• Public Key: P computes \( I = S^2 \mod n \), publishes \((I,n)\) as his public key.

• Purpose of the protocol: P has to convince verifier (V) that he knows the secret \( S \) corresponding to the public key \((I,n)\),
  - i.e., to prove that he knows a square root of \( I \mod n \), without revealing \( S \) or any portion thereof.
Fiat-Shamir Identification Scheme

V wants to authenticate identity of P, who claims to have a public key I. Thus, V asks P to convince him that P knows the secret key S corresponding to I.

1. P chooses at random $1 < R < n$ and computes:
   $X = R^2 \mod n$

2. P sends $X$ to V

3. V randomly requests from P one of two things (0 or 1):
   (a) $R$
   or
   (b) $RS \mod n$

4. P sends requested information
Fiat-Shamir ZK Identification Scheme

5. V checks the correct answer:
   a) \( R^2 \equiv X \pmod{n} \)
      or
   b) \( (R*S)^2 \equiv X*I \pmod{n} \)

6. If verification fails, V concludes that P does not know S.

7. Protocol is repeated t (usually 20, 30, or \( \log n \)) times, and, if each one succeeds, V concludes that P is the claimed party.

What if Prover knows the challenge ahead of time: Case 0

\( n, I \) (doesn’t know S)

- Pick random \( R \);
- Set \( x = R^2 \pmod{n} \)

\( I, x \) \quad \text{query} = 0

\( R \) \quad \text{Check that:} \quad R^2 = x \pmod{n}
What if Prover knows the challenge ahead of time: Case 1

\[ n, I \text{ (doesn’t know } S) \]

pick random \( R \);
set \( x = R^2 \times I \mod n \)

\[ I, x = R^2 \times I \]

query = 1

Check that:

\[ R \times I \mod n \]

\[ (R \times I)^2 = x \times I \mod n \]

(Instead of: \( R \times S \mod n \))

Fiat-Shamir Identification Scheme

**CLAIM:** Protocol does not reveal ANY information about \( S \) or
Protocol is **ZERO-KNOWLEDGE**

Proof: We show that no information on \( S \) is revealed:

- Clearly, when \( P \) sends \( X \) or \( R \), he does not reveal any information on \( S \).

- When \( P \) sends \( RS \mod n \):
  - \( RS \mod n \) is random, since \( R \) is random and \( \gcd(S, n) = 1 \).
  - If adversary can compute any information on \( S \) from
    
    \[ I, n, X \text{ and } RS \mod n \]
    
    he can also compute the same information on \( S \) from \( I \) and \( n \), since he can choose a random \( T = R’S \mod n \) and compute:
    
    \[ X’ = T^2 I^{-1} = (R’)^2 S^2 I^{-1} = (R’)^2 \]
Security

Clearly, if P knows S, then V is convinced of his identity.

If P does not know S, he can either:

1. know R, but not RS mod n. Since he is choosing R, he cannot multiply it by the unknown value S or
2. choose RS mod n, and thus can answer the second question: RS mod n. But, in this case, he cannot answer the first question R, since he needs to divide by the unknown S.

In any case, adversary cannot answer both questions, since otherwise he can compute S as the ratio between the two answers.

But, we assumed that computing S is hard, equivalent to factoring n.

Since P does not know in advance (when choosing R or RS mod n) which question that V will ask, he cannot foresee the required choice. He can succeed in guessing V’s question with probability 1/2 for each question.

The probability that V fails to catch P in all runs is thus: $2^{-t}$ (e.g., 1 in 1,000,000,000 for $t=20$)
How to explain ZK to your children

The Protocol:

1) V asks someone he trusts to check that the door is locked on both sides.

2) P goes into the maze past point B (heading either right or left)

3) V looks into the cave (while standing at point A)

4) V randomly picks right or left

5) V shouts (very loudly!) for P to come out from the picked direction

6) If P doesn’t come out from the picked direction, V knows that P is a liar and protocol terminates

REPEAT (2)-(6) n TIMES