Zero Knowledge Proofs
Part II

Class 6

Schneier: Ch 5.1, 5.2, 21, 23.11
Overview

- Zero Knowledge Proofs: Introduction
- Graph Isomorphism
- Zero Knowledge Proofs of Knowledge
  - Discrete Logarithms
  - Zero Knowledge Proofs of Identity
ZK Proofs of Identity

- Authentication relies on what users
  - Have, e.g., password, card, token
  - Are, e.g., fingerprint, retina, ...
- Problem: How can you authenticate without revealing your information
  - Attacker could retrieve user password, card information, retina, fingerprint ...
- Wormhole Attacks
  - Chess Grandmaster Problem
  - The Mafia Fraud
Wormhole Attack

1. Prove identity
2. Alice Id info
3. Prove identity (Alice)

Alice

Bob

Carol
Pretending to be Alice

David
Real Case Study

- Attackers set up a fake automatic teller machine at a shopping mall.
- When a person inserted a bank card, the machine recorded the information.
  - Responded with the message that it could not accept the card.
- The thieves then made counterfeit bank cards and went to legitimate teller machines and withdrew cash.
- How to prevent identity theft?
Zero Knowledge Proof of Identity

- Alice has an identity
- She wants to identify herself to Bob
- She does not want to reveal her identity
- Instead of giving her identity to Bob, she will prove that she knows her identity
Overview

- Zero Knowledge Proofs: Introduction
- Graph Isomorphism
- Zero Knowledge Proofs of Discrete Logarithms
- Zero Knowledge Proofs of Identity
  - Feige-Fiat-Shamir
  - Guillou-Quisquater
  - Schnorr
Guillou-Quisquater: ZK Proof of Identity

Identity J:
\[ H(\text{name, validity, bank #, ...}) \]

Secret (password)
primes p, q & B such that:
\[ J B^v = 1 \mod n \]

2. Pick random \( 1 < r < n-1 \)

3. \( T = r^v \mod n \)

4. Pick random \( 0 < d < v-1 \)

5. \( d \)

6. \( D = rB^d \mod n \)

7. \( T' = D^v J^d \mod n \)

if \( T' = T \) success!
Overview

- Zero Knowledge Proofs: Introduction
- Graph Isomorphism
- Zero Knowledge Proofs of Discrete Logarithms
- Zero Knowledge Proofs of Identity
  - Feige-Fiat-Shamir
  - Guillou-Quisquater
  - Schnorr
Fun Facts About the Paper

- Best known zero knowledge proof of identity
- 1986, authors submitted a US patent application
  - Potential military and commercial application

- Patent office respond with a “secrecy order”
  - Disclosure of this material is dangerous to national security.
  - Otherwise, 2 years imprisonment or $10K fine or both

- Criticism from academic community and press
  - Removed the secrecy order later
Quadratic Residues

- $y$ is called a **quadratic residue** modulo $n$
  - There exists an integer $x$ such that
    - $x^2 = y \mod n$
  - $y$ is QR
- Otherwise, $y$ is called a **quadratic nonresidue** modulo $n$
  - $y$ is QNR
Quadratic Residuosity Problem

- Given $y$, is there $x$ such that $x^2 = y \mod n$
  - $x$ is called the **square root** mod $n$ of $y$
- What if $n = pq$, where $p$ and $q$ are primes?
- Given $y$
  - **Jacobi symbol is 1**
  - Determine if $y$ is a quadratic residue or not
  - Don’t even try to find the root ($x$)
  - If Jacoby symbol of $y$ is $-1$, then $y$ is non-residue
- Without knowing $p$ and $q$ (but only $n$)
  - **This problem is HARD!**
Quadratic Residuosity Problem (cont’d)

- Given $y$, find $x$ such that $x^2 = y \mod n$
  - $x$ is called the square root mod $n$ of $y$
- What if $n = pq$, where $p$ and $q$ are primes?
- Given $y$
  - And $p$ and $q$
  - Problem is easy
- Compute
  - $y_p = y \mod p$
  - $y_q = y \mod q$
  - If $y_p^{(p-1)/2} = 1 \mod p$ and $y_q^{(q-1)/2} = 1 \mod q$
  - Then $y$ is quadratic residue mod $n$
Alice claims that she knows prime factorization of a large number $n$

How can she prove it to Bob

1. Alice generates Random number $Y_1 \ldots Y_k$
2. Computes $X_i$ such that $X_i^2 = Y_i \mod n$
3. Send $Y_1 \ldots Y_k$ and $X_1 \ldots X_k$
4. Bob checks whether $X_i^2 = Y_i \mod n$

No, Alice can cheat.
Alice can generate $X_i$ first then compute $Y_i$.

Should Bob be convinced?
ZKP – Prime Factorization (cont’d)

1. Generates Random number \( Y_1 \ldots Y_k \)

2. Send \( Y_1 \ldots Y_k \) to Alice

3. Computes \( X_i \) such that \( X_i^2 \equiv Y_i \mod n \)

4. Send \( X_1 \ldots X_k \) to Bob

5. Bob checks whether \( X_i^2 \equiv Y_i \mod n \)
   Should Bob be convinced?

Yes, But Bob can cheat
ZKP – Prime Factorization (cont’d)

1. Generate random values $R_1 \ldots R_k$. Compute $Y_1 \ldots Y_k$ such that $R_i^2 = Y_i \mod n$.

2. Send $Y_1 \ldots Y_k$ to Alice.

3. Computes $X_i$ such that $X_i^2 = Y_i \mod n$.

4. Send $X_1 \ldots X_k$ to Bob.

5. Depending on whether $R_i = X_i$ Bob can find out the prime factorization of $n$ (with a very high probability), i.e. prime number $p$ and $q$ such that $n = pq$.

if $R_i \neq X_i$, $\gcd(R_i + X_i, n) = p$ or $q$.
ZKP – Prime Factorization (cont’d)

1. Generates Random number $R_1 ... R_k$ and computes $Y_1 ... Y_k$ such that $R_i^2 = Y_i \mod n$.

2. Send $Y_1 ... Y_k$ to Alice

3. Computes $X_i$ such that $X_i^2 = Y_i \mod n$

4. Send $h(X_1) ... h(X_k)$
   $h$ is a one way function (Hash)

5. Checks whether $h(R_i) = h(X_i)$
Alice claims to know $S$, a square root mod n of $Y$
- $S^2 = Y \mod n$

She wants to prove her knowledge to Bob using ZKP
- She does not want to reveal $S$
- Both $Y$ and $n$ are known to Bob and Alice
ZKP – Quadratic Residue (cont’d)

1. Chooses a random number $R_1$ such that $R_1 \cdot R_2 = S$ and $\gcd(R_1, n) = \gcd(R_2, n) = 1$

2. Computes $X_1 = R_1^2 \mod n$
   $X_2 = R_2^2 \mod n$
   Note: $S^2 = Y = (R_1 \cdot R_2)^2 = X_1 \cdot X_2 \mod n$

3. Send $X_1$ and $X_2$ to Bob

4. Checks whether $X_1 \cdot X_2 = Y$

5. Randomly picks either $X_1$ or $X_2$ and asks Alice to supply a square root of it. Let’s say Bob picked $X_1$

6. Square root mod $n$ of $X_1$?

7. Sends $R_1$

8. Checks whether $X_1 = R_1^2 \mod n$?

Can Alice cheat?

Bob can not ask square root mod $n$ of both $X_1$ and $X_2$. Why?
Alice does not know $S$
Choose a random number $R_1$ and
Computes $X_1 = R_1^2 \mod n$

Finds another value $X_2$ such that,
$X_1 \cdot X_2 = Y$
Note: Finding $R_2$ such that $X_2 = R_2^2 \mod n$ is hard.

Send $X_1$ and $X_2$ to Bob

Square root mod n of $X_1$?

Sends $R_1$

Checks whether $X_1 \cdot X_2 = Y$

Randomly picks either $X_1$ or $X_2$ and asks Alice to supply a square root of it. Let’s say Bob picked $X_1$

Checks whether $X_1 = R_1^2 \mod n$?

But if Bob picks $X_2$, Alice will not be able to deliver $R_2$, 50% chance

Note: Finding $R_2$ such that $X_2 = R_2^2 \mod n$ is hard.
ZKP – Quadratic Residue (cont’d)

- Alice and Bob repeat this protocol $t$ times
  - Probability that Alice is cheating is $\frac{1}{2^t}$
- This protocol is the basic building block of Feige-Fiat-Shamir’s Zero Knowledge Proof of Identification scheme
Feige Fiat Shamir Identification Solution

1. Publishes $n = pq$, where $p$ and $q$ are two large prime numbers (512 bit). Keeps $p$ and $q$ secret.

2. Chooses $k$ random numbers $S_1, \ldots, S_k$ in $\mathbb{Z}_n$. These numbers are her secret (password). $\gcd(S_i, n) = 1$.

3. Computes $I_1, \ldots, I_k$ such that,

$$I_j = \pm \frac{1}{S_j^2} \mod n$$

4. $I = \{I_1, \ldots, I_k\}$

5. Publishes $I_1, \ldots, I_k$

Alice keeps $S_1, \ldots, S_k$ secret.
**FFS Identification Solution (cont’d)**

1. Chooses a random number $R$ and computes $X = \pm R^2 \mod n$

2. $I = \{I_1, \ldots, I_k\}, \ X$

3. Prepare a $k$ bit random Boolean vector $E = E_1 \ldots E_k$, $E_j = 0$ or $1$

4. $E = E_1 \ldots E_k$

5. Computes $Y = R \times \prod_{E_j=1} S_j \mod n$

6. $Y$

7. Checks whether $X' = Y^2 \times \prod_{E_j=1} I_j \mod n = X$

   Note: $I_j = \pm \frac{1}{S_j^2} \mod n$

---

**Alice**

- $S = \{S_1, \ldots, S_k\}$ – Secret (password)
- $I = \{I_1, \ldots, I_k\}$ – Public identity

**Bob**

- $l = \{l_1, \ldots, l_k\}$, $X$
- $Y$
- $S = \{S_1, \ldots, S_k\}$ – Secret (password)
- $I = \{I_1, \ldots, I_k\}$ – Public identity
Example

2. Chooses $S = \{3, 4, 9\}$ as her secret key/password. $k = 3$.

3. 
   
   \[ I_1 = \pm \left( \frac{1}{3} \right)^2 \mod 35 \]
   \[ I_1 = \pm 12^2 \mod 35 \]
   \[ I_1 = 4 \mod 35 = 4 \]
   \[ I_2 = 11 \]
   \[ I_3 = 16 \]
   \[ I = \{4, 11, 16\} \]

4. 
   \[ I = \{4, 11, 16\} \]

5. Publishes $I = \{4, 11, 16\}$

1. Publishes $n = 35 = 5 \times 7$
Example (cont’d)

0. S = {3, 4, 9} - password
    l = {4, 11, 16}

1. Chooses a random number R = 16 and Computes $X = 16^2 \mod 35 = 11$

2. $X = 11$, l = {4, 11, 16}

3. Prepares a 3 bit random Boolean vector $E = 6$ (110)

4. $E = 6$ (110)

5. Computes $Y = R \times \prod_{E_j=1} S_j \mod n$
   
   $(16 \times 3 \times 4 \mod 35)$
   
   $= 17$

6. $Y = 17$

7. Checks whether

   $X' = Y^2 \times \prod_{E_j=1} l_j \mod n$
   
   $= 17^2 \times 4 \times 11 \mod 35$
   
   $= 11$
   
   $== X$
Can Alice Cheat? Guess E

\[ S = \{3, 4, 9\} \text{— password} \]
\[ I = \{4, 11, 16\} \]
\[ E = 2 = (010) \text{— Correct guess} \]

1. Computes X for any Random \( Y = 7 \)
\[
X = Y^2 \times \prod_{E_j=1} \frac{I_j \mod n}{\prod_{E_j=1}}
\]
\[
= 7^2 \times 11 \mod 35
\]
\[
= 14
\]

2. \( X = 14, I = \{4, 11, 16\} \)

3. Prepares a 3 bit random Boolean vector \( E = 2 = (010) \)

4. \( E = 2 \ (010) \)

5. \( Y = 7 \)

6. Bob

7. Checks whether
\[
X' = Y^2 \times \prod_{E_j=1} \frac{I_j \mod n}{\prod_{E_j=1}}
\]
\[
= 7^2 \times 11 \mod 35
\]
\[
= 14
\]
\[
== X
\]

Alice

Bob
Can Alice Cheat? Guess E (cont’d)

- If she can correctly guess E of step 4
  - Can compute the X for any random Y for step 7 before the start of the protocol.
  - Does not need to know secret keys
- Probability of correct guess is $2^{-k}$ (since, $|E|=k$)
- Bob repeats the protocol $t$ times
  - Probability of cheating is $2^{-kt}$
Real World Use

- Smart Card issuer generates $S = \{S_1, \ldots, S_k\}$ and $I = \{I_1, \ldots, I_k\}$ using a large composite $n = pq$
- Keeps $p$ and $q$ secret
- Publishes $n$ and $I = \{I_1, \ldots, I_k\}$
- Embeds $S = \{S_1, \ldots, S_k\}$ and other information into the card
A microprocessor with limited computational power is embedded on the card

No one can read $S = \{S_1, \ldots, S_k\}$ directly

Only microprocessor can access them for computation

Card is built using tamper proof technology