Security (CS4028)

Lecture 8. Zero Knowledge Proof

Chunyan Mu

chunyan.mu@abdn.ac.uk

The School of Natural and Computing Sciences

Schedule

	Week	Lecture 1	Lecture 2	Tutorial
	1	Intro to course & security	Intro to Crypto	-
	2	Symmetric Crypto	Hash	Math for crypto
	3	Asymmetric Crypto-1	Asymmetric Crypto-2	Symmetric Crypto
⇒	4	Signatures	Zero Knowledge Proof	Asymmetric Crypto
	5	Certificates	Authentication	Signature & certificates
	6	Access Control	AC models	Authentication
	7	Information flow	Management	Access control
	8	Protocols	Communications	Concepts & management
	9	Network security	Network security	Protocols and communications
	10	Advanced topics	Advanced topics	Network
	11	Revision		

Lecture 8: Zero knowledge proof

Last lecture

- Signatures

This lecture

After having attended this session, you will be able to:

- understand what is zero knowledge proof
- understand how Feige Fiat Shamir works

Outline

Protocols and interactive proofs

Zero-knowledge proof

Math background: Quadratic residues and square roots

Zero-knowledge protocol: Feige-Fiat-Shamir

Summary

Outline

Protocols and interactive proofs

Zero-knowledge proof

Math background: Quadratic residues and square roots

Zero-knowledge protocol: Feige-Fiat-Shamir

Summary

Protocols: recap

What is a protocol?

- A protocol is a series of steps, involving two (or more) parties, designed to accomplish a task.
- A cryptographic protocol is a protocol that uses cryptography:
  - defining an efficient protocol is usually more important than choosing an algorithm to encrypt a plaintext.
- For example: if you encrypt a message with DES, the receiver has to know the key to decrypt it.

How can you send the key to the receiver safely?

Protocols: an example

Basic symmetric cryptography: Alice, Bob and Eve

1. Alice (sender) and Bob (receiver) choose a cryptographic algorithm;
2. Alice and Bob both agree on a common key K_{AB};
3. Alice encrypts her message (plaintext) using the algorithm and K_{AB};
4. Alice sends the obtained ciphertext to Bob;
5. Bob decrypts the ciphertext using the algorithm and K_{AB}.

Protocols: an example

Problems

- Keys must be shared secretly
- What if a key is: stolen, extorted, discovered?
- Eve can read the messages and even act as a passive or active attacker

Key agreement/exchange

key establishment technique in which a shared secret is derived by two (or more) parties,

- e.g., Diffie-Hellman protocol

Interactive Proof

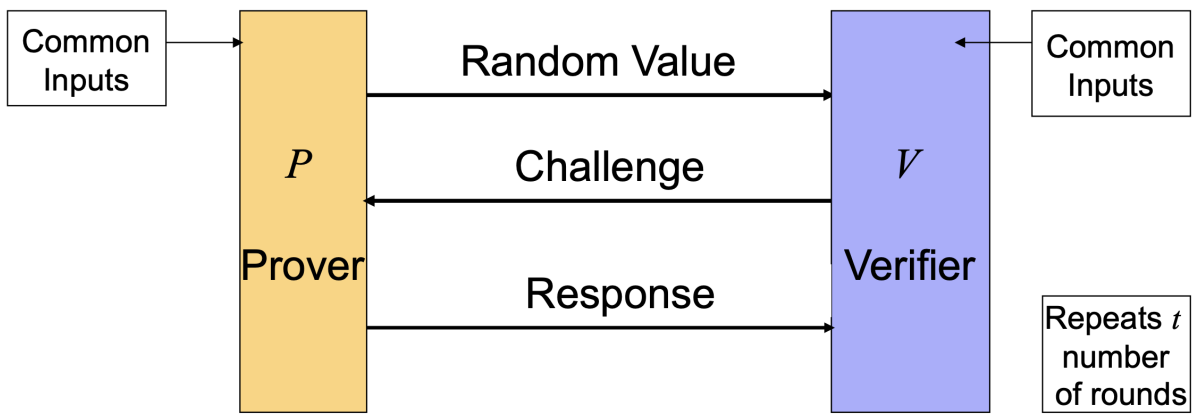
- Two parties (a prover and a verifier) in Zero Knowledge proof are interactive.
  - The prover is to convince the verifier the truth of an assertion, e.g., claimed knowledge of a secret.
  - The verifier either accepts or rejects the proof.
  - Zero knowledge proofs are instances of interactive proof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

Interactive Proof

- 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 Proof

- 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 Proof

- 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 Proof

- 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 Proof

Properties

- **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 not true, no cheating prover can convince the honest verifier that it is true, except with some small probability. Note here, in an interactive proof system, we trust the verifier.

Outline

Protocols and interactive proofs

Zero-knowledge proof

Math background: Quadratic residues and square roots

Zero-knowledge protocol: Feige-Fiat-Shamir

Summary

Zero-knowledge proof

Zero-knowledge proof is a method by which:

- one party (the prover) can prove to another party (the verifier) that a given statement is true,
- without conveying any information apart from the fact that the statement is indeed true.

Zero-knowledge proof

Zero-knowledge proof is a method by which:

- one party (the prover) can prove to another party (the verifier) that a given statement is true,
- without conveying any information apart from the fact that the statement is indeed true.

Ummm...

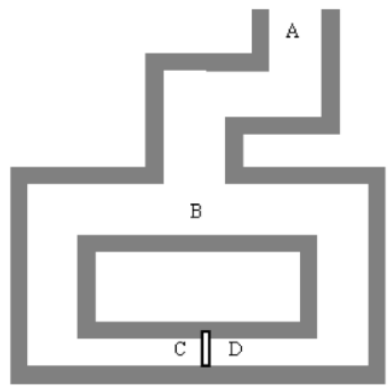
Why do we still pass our passwords over a network? Why do we still hash passwords? Why can't we come up with our own random value, and then prove to everyone that we know the secret?

Zero-knowledge proof: the story

The intuitive ideas of zero-knowledge proofs

J.-J Quisquater and L. Guillou explain ZK with a story about a cave:

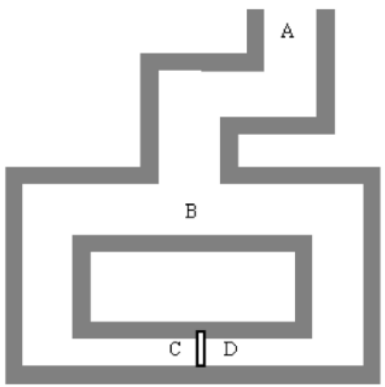
- The cave has a secret
- Peggy (prover) knows the magic words can open the secret door between C and D. To everyone else, both passages lead to dead ends
- Peggy wants to prove her knowledge to Victor (Verifier), but she doesn't want to reveal the magic words
- She will use a zero-knowledge proof protocol



Zero-knowledge proof

The protocol

1. Victor stands at point A
2. Peggy walks all the way into the cave, either to point C or D
3. After Peggy has disappeared into the cave, Victor walks to point B
4. Victor shouts to Peggy, asking her either to:
   - come out of the left passage or
   - come out of the right passage
5. Peggy complies, using the magic words to open the secret door if she has to.
6. Peggy and Victor repeat steps 1. through 5. n times



Zero-knowledge proof

Remark

- if Peggy doesn't know the secret, she can only come out the way she came in, she has $\frac{1}{2}$ of fooling Victor
- after n attempts, she has only $\frac{1}{2^n}$ of fooling Victor

Outline

Protocols and interactive proofs

Zero-knowledge proof

Math background: Quadratic residues and square roots

Zero-knowledge protocol: Feige-Fiat-Shamir

Summary

One-way Functions: recap

- Cryptography is built on the notion of one-way function, that is, a function that is easy to compute but hard to invert.
- Some presumed one-way functions and associated hard problems:

$(p, q) \mapsto p \cdot q$	Factoring problem
$x \mapsto g^x \mod n$	Discrete log problem
$P \mapsto k \times P$	Ellpitic curve discrete log problem
$x \mapsto H(x)$	Collision-finding problem
$x \mapsto x^2 \mod n$	Quadratic residuosity problem

Quadratic residues and square roots

Definition: quadratic residues and square roots

Let $a \in \mathbb{Z}_n$ $(a \neq 0)$. If there is an integer $x \in \mathbb{Z}_n (x \neq 0)$ such that:

$$x^2 \equiv a \pmod{n}$$

then a is said to be a quadratic residue modulo n (or square modulo n, QR_n), and x is called square root of a modulo n. If not, a is said to be a quadratic non-residue modulo n (QNR_n).[a]

[a] Of course, when a is a quadratic non-residue, then there is no square root of a modulo n.

Quadratic residues and square roots

Example: quadratic residues and square roots

For example, $4^2 \equiv 6 \pmod{10}$, so 6 is a quadratic residue modulo 10, and 4 is the square root of 6 modulo 10. The entire set of quadratic residues modulo 10 are given by 1, 4, 5, 6, and 9, since:

$$\begin{aligned} 1^2 &\equiv 1 \pmod{10} & 2^2 &\equiv 4 \pmod{10} \\ 3^2 &\equiv 9 \pmod{10} & 4^2 &\equiv 6 \pmod{10} \\ 5^2 &\equiv 5 \pmod{10} & 6^2 &\equiv 6 \pmod{10} \\ 7^2 &\equiv 9 \pmod{10} & 8^2 &\equiv 4 \pmod{10} \\ 9^2 &\equiv 1 \pmod{10} \end{aligned}$$

making the numbers 2, 3, 7 and 8 the quadratic non-residues (mod 10).

Quadratic residues and square roots

Theorem (optional)

Given an odd prime p, if:

$$r^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

then r is a QR (+) or QNR (-).

Proof. if r is a QR of p then there exists a square x^2 s.t.

$$x^2 \equiv r \pmod{p}$$

so:

$$\begin{aligned} r^{(p-1)/2} &\equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p} \qquad \text{by Fermat's little theorem} \end{aligned}$$

□

Quadratic residues and square roots

Lemma (optional)

For an odd prime p,

- Every $a \in QR_p$ has exactly two square roots in $\mathbb{Z}_p^*$ ($\pm x$)
- Exactly 1/2 of the elements of $\mathbb{Z}_p^*$ are quadratic residues.
- The quadratic residues belong to the residue classes containing the numbers: $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$.

In other words, if $a \in QR_p$:

$$|\sqrt{a}| = 2,\ |QR_p| = |QNR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}.$$

Example: quadratic residues in $\mathbb{Z}_{11}^*$

$QR_{11} = \{1, 3, 4, 5, 9\}$ and $QNR_{11} = \{2, 6, 7, 8, 10\}$

Quadratic residues and square roots

Lemma (optional)

Let $n = pq$ for p, q two distinct odd primes.

- Every $a \in QR_n$ has exactly four square roots in $\mathbb{Z}_n^*$
- Exactly $1/4$ of the elements of $\mathbb{Z}_n^*$ are quadratic residues.

In other words, if $a \in QR_n$ then $|\sqrt{a}| = 4$, so:

$$|QR_n| = \frac{|\mathbb{Z}_n^*|}{4} = \frac{(p-1)(q-1)}{4}.$$

Example: quadratic residues in $\mathbb{Z}_{15}^*$

$QR_{15} = \{1, 4\}$ and $QNR_{15} = \{2, 7, 8, 11, 13, 14\}$

Quadratic residues and square roots

Remark

- The operation of computing square roots modulo n can be performed efficiently when n is prime (using Fermat's little theorem), but is difficult when n is a composite integer whose prime factors are unknown.
- If the factors p and q are known, then the problem of finding a square root can be solved efficiently by first finding square roots of a modulo p and modulo q, and then combining them using the Chinese Remainder Theorem to obtain the square roots of a modulo n.

Outline

Protocols and interactive proofs

Zero-knowledge proof

Math background: Quadratic residues and square roots

Zero-knowledge protocol: Feige-Fiat-Shamir

Summary

Feige-Fiat-Shamir protocol: preparation

The Feige-Fiat-Shamir protocol is based on the difficulty of computing square roots modulo composite numbers.

- Peggy chooses $n = pq$, where p and q are distinct large primes.
- Next she picks a quadratic residue $v \in QR_n$ (which she can easily do by choosing a random element $x \in \mathbb{Z}_n^*$ and letting $v = x^2 \mod n$).
- Finally, she chooses s to be the smallest square root of $v^{-1} \pmod n$. [1] She can do this since she knows the factorisation of n.

She makes n and v public and keeps s private.

[1] Note that if v is a quadratic residue, then so is $v^{-1} \pmod n$

Simplified Feige-Fiat-Shamir

We start from a simplified one-round version.

Identification Scheme

1. Trent (Trusted Arbitrator) chooses a random modulus n which is the product of two large prime numbers.
2. Trent chooses v, where v is a quadratic residue mod n, that is,
   - there exists at least one number x such that $x^2 = v \mod n$ exists
   - and $v^{-1} \mod n$ exists, i.e. $(av = 1 \mod n)$
3. Trent computes the smallest $s \equiv \sqrt{v^{-1}} \mod n$.
4. Trent gives Peggy (Prover) her public key v.
5. Trent gives Peggy her private key s.

Simplified Feige-Fiat-Shamir

Accreditation Scheme

1. Peggy picks a random r less than n
2. Peggy computes $x = r^2 \bmod n$
3. Peggy sends x to Victor (Verifier)
4. Victor sends Peggy a random bit b
5. Answer:
   - If $b = 0$ then Peggy sends Victor r.
   - If $b = 1$ then Peggy sends Victor $y = r \times s \bmod n$
6. Verification:
   - If $b = 0$ then Victor verifies $x = r^2 \bmod n$: Peggy knows $\sqrt{x}$.
   - If $b = 1$ then Victor verifies $x = y^2 \times v \bmod n$: Peggy knows $\sqrt{v^{-1}}$

Simplified Feige-Fiat-Shamir

An example

Let $n = 3 \times 5 = 15$, possible quadratic residues are:

v (public key)	equations	square roots
1	$x^2 = 1 \bmod 15$	$1, 4, 11, 14$
4	$x^2 = 4 \bmod 15$	$2, 7, 8, 13$

we compute the private key:

v	v^{-1}	$\sqrt{v^{-1}}$ (private key)
1	1	1
4	4	2

Simplified Feige-Fiat-Shamir

An example

1. Peggy picks $r = 7$
2. Peggy computes $x = r^2 \bmod n = 7^2 \bmod 15 = 4$
3. Peggy sends $x = 4$ to Victor (Verifier)
4. Victor sends Peggy a random bit b : 0 or 1

Simplified Feige-Fiat-Shamir

An example

5. Answer:
   - If $b = 0$ then Peggy sends Victor $r = 7$.
   - If $b = 1$ then Peggy sends Victor $y = r \times s \bmod n = 7 \times 2 \bmod 15 = 14$
6. Verification:
   - If $b = 0$ then Victor verifies $x = r^2 \bmod n = 7^2 \bmod 15 = 4$
   - If $b = 1$ then Victor verifies $x = y^2 \times v \bmod n = 14^2 \times 4 \bmod 15 = 784 \bmod 15 = 4$
7. Victor accepts the accreditation

Feige-Fiat-Shamir

Identification Scheme

1. Trent chooses a random mod n which is the product of two large prime numbers
2. Trent chooses k different numbers, $v_1, \ldots, v_k$ where v_i is a quadratic residue mod n
3. Trent computes the smallest $s_i = \sqrt{v_i^{-1}} \bmod n$
4. Trent gives Peggy her public keys $v_1, \ldots, v_k$
5. Trent gives Peggy her private keys $s_1, \ldots, s_k$

Feige-Fiat-Shamir

Accreditation Scheme

1. Peggy picks up a random r less than n
2. Peggy computes $x = r^2 \bmod n$
3. Peggy sends x to Victor
4. Victor sends Peggy a random k-bit string: $b_1, \ldots, b_k$
5. Peggy computes $y = r \times (s_1^{b_1} \times s_2^{b_2} \times \cdots \times s_k^{b_k}) \bmod n$
6. Victor verifies that

$$x = y^2 \times (v_1^{b_1} \times v_2^{b_2} \times \cdots \times v_k^{b_k}) \bmod n$$

Feige-Fiat-Shamir

An example

Let $n = 5 \times 7 = 35$, possible quadratic residues are:

v	equations	solutions
1	$x^2 = 1 \bmod 35$	$1, 6, 29, 34$
4	$x^2 = 4 \bmod 35$	$2, 12, 23, 33$
9	$x^2 = 9 \bmod 35$	$3, 17, 18, 32$
11	$x^2 = 11 \bmod 35$	$9, 16, 19, 26$
16	$x^2 = 16 \bmod 35$	$4, 11, 24, 31$
29	$x^2 = 29 \bmod 35$	$8, 13, 22, 27$

Feige-Fiat-Shamir

Computing the quadratic residues

v	v^{-1}	$\sqrt{v^{-1}}$
1	1	1
4	9	3
9	4	2
11	16	4
16	11	9
29	29	8

Feige-Fiat-Shamir

An example

Quadratic residues are: $1, 4, 9, 11, 16, 29,$ assume Peggy's public key $v : 1, 4, 9, 16,$ then corresponding private key $s : 1, 3, 2, 9$.

1. Peggy picks up a random $r = 9$
2. Peggy computes $x = r^2 \bmod n = 81 \bmod 35 = 11$
3. Peggy sends $x = 11$ to Victor
4. Victor sends Peggy a random string: 1001
5. Peggy computes $y = 9 \times (1^1 \times 3^0 \times 2^0 \times 9^1) \bmod 35 = 11$
6. Victor verifies that:

$$\begin{aligned} x &= y^2 \times (v_1^{b_1} \times v_2^{b_2} \times \cdots \times v_k^{b_k}) \bmod n \\ &= (121 \times 1 \times 16) \bmod 35 = 1936 \bmod 35 = 11 \end{aligned}$$

Outline

Protocols and interactive proofs

Zero-knowledge proof

Math background: Quadratic residues and square roots

Zero-knowledge protocol: Feige-Fiat-Shamir

Summary

Summary

This lecture

- Zero knowledge proof
- Feige Fiat Shamir algorithm

Next lecture

- Certificates