

Secret Sharing and Zero-knowledge Proofs

Dawn Song
dawnsong@cs.berkeley.edu

1

Review

- Digital signatures
 - What security properties is it designed to provide?
 - One-time signature
 - RSA signature
 - ElGamal signature
- Secret-sharing schemes

2

Secret Sharing

- A trusted authority TA has a secret K
- Wants to split K into n shares S_1, \dots, S_n , distributing to n users U_1, \dots, U_n respectively, s.t.
 - A reconstruction algorithm can be used to efficiently reconstruct K from any t of the n shares
 - Any $t-1$ of the n shares reveal no information about K
- Such a scheme is called an (n, t) threshold secret sharing scheme

3

(n,n) Secret Sharing Scheme

- Suppose the secret K is an integer btw 0 and $M-1$
- (n,n) threshold scheme:
 - Pick S_1, \dots, S_{n-1} uniformly at random btw 0 and $M-1$
 - Set $S_n = K - (S_1 + \dots + S_{n-1}) \bmod M$
- How to reconstruct K ?
- What happens if $n-1$ users get together?

4

(n,t) Threshold Scheme

- Polynomials modulo prime p
 - Polynomials whose coefficients are elements mod p
 - E.g., $f(x) = x^2 + 2x + 4 \bmod 5$
 - Degree- n polynomial $f \bmod p$ is uniquely determined by any $n+1$ distinct pairs (x_i, y_i) s.t. $f(x_i) = y_i$
 - » Lagrange interpolation
- To (n,t) threshold share secret K :
 - Pick a random polynomial $f \bmod p$ of degree $t-1$ s.t. $f(0) = K$
 - Share $s_i = f(i)$ for $i = 1$ to n
 - How to recover K ?
 - How many shares do you need to recover K ?
 - What happens if you have fewer shares than t ?

5

Zero-knowledge Proof

- Alice->Bob: I know the solution to Que 3 in hw 2, but I can't tell you what the solution is
- Bob->Alice: tell me, o.w. I don't believe you
- Alice->Bob: Ok, I'll prove to you that I know the solution in **Zero-knowledge**

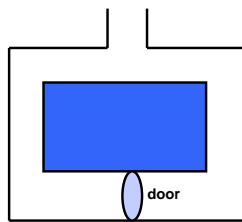
6

Zero-knowledge protocol

- Idea: (interactive) proof btw prover A & verifier B
- At the end of the proof, B is convinced A knows a secret satisfying a fact F
- But B has no information about that secret

7

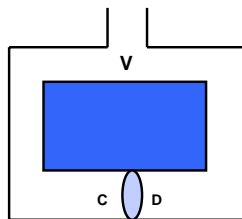
The Zero-knowledge Cave (I)



- Alice wants to prove to Bob that she knows how the magic word to open door
 - Without telling Bob the magic word

8

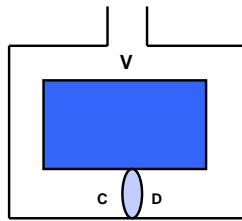
The Zero-knowledge Cave (II)



1. Alice walks to either C or D;
2. Bob stands at V, calling either Left or Right;
3. Alice complies, using her magic word to open door if needed;
4. Alice & Bob repeats steps 1-3 for n times

9

The Zero-knowledge Cave (III)



- What if Alice didn't know the magic word?
- What does Bob learn at the end of the proof?

10

How to prove knowledge of square root

- Finding square root mod $N=pq$ is as hard as factoring
- A knows b s.t. $b^2 \equiv y \pmod{pq}$, & wishes to prove to B that she knows such b .
- $A \rightarrow B$: $s \equiv r^2 \pmod{pq}$ (A picks random r)
- B flips coin
- $B \rightarrow A$: coin flip
- If heads
 - $A \rightarrow B$: $t \equiv r \pmod{pq}$
 - B verifies $t^2 \equiv s \pmod{pq}$
- If tails
 - $B \rightarrow A$: $t \equiv rb \pmod{pq}$
 - A verifies $t^2 \equiv sy \pmod{pq}$
- What if A didn't know the square root?
- What did B learn after the proof?

11

Conclusion

- **Secret-sharing schemes**
 - (n,t) threshold schemes using polynomials
- **Zero-knowledge proofs**
 - Concepts
 - Zero-knowledge proof of square root

12
