Plan of Talk

- **Zero Knowledge proofs**
- **Ali baba's cave story.**
- **Zero knowledge proof based on discrete logarithms.**
- **DSA-Digital Signature Algorithm of NIST**

Advanced Cryptographic Concepts

There are many esoteric protocols in cryptography which facilitate wide varieties of modern day network security applications.

Some of the important concepts:

- Zero Knowledge Protocols
- Threshold Cryptography
- Oblivious Transfer
- Anonymous Protocols

Here we discuss briefly Zero-Knowledge protocols.

Zero Knowledge proofs
Interactive proof (IP) Systems

- Is an interactive proof by a party (Prover) to a an another party (Verifier) that a mathematical statement is true, without revealing anything more than what is conveyed in the interaction.
- Usually the Prover holds some secret protected by a hard problem (a problem in NP) and describe a mathematical statement involving the secret which otherwise could not have been made without the secret.
- Protocols which use such proofs are known as Zero Knowledge protocols.

Zero Knowledge Protocols

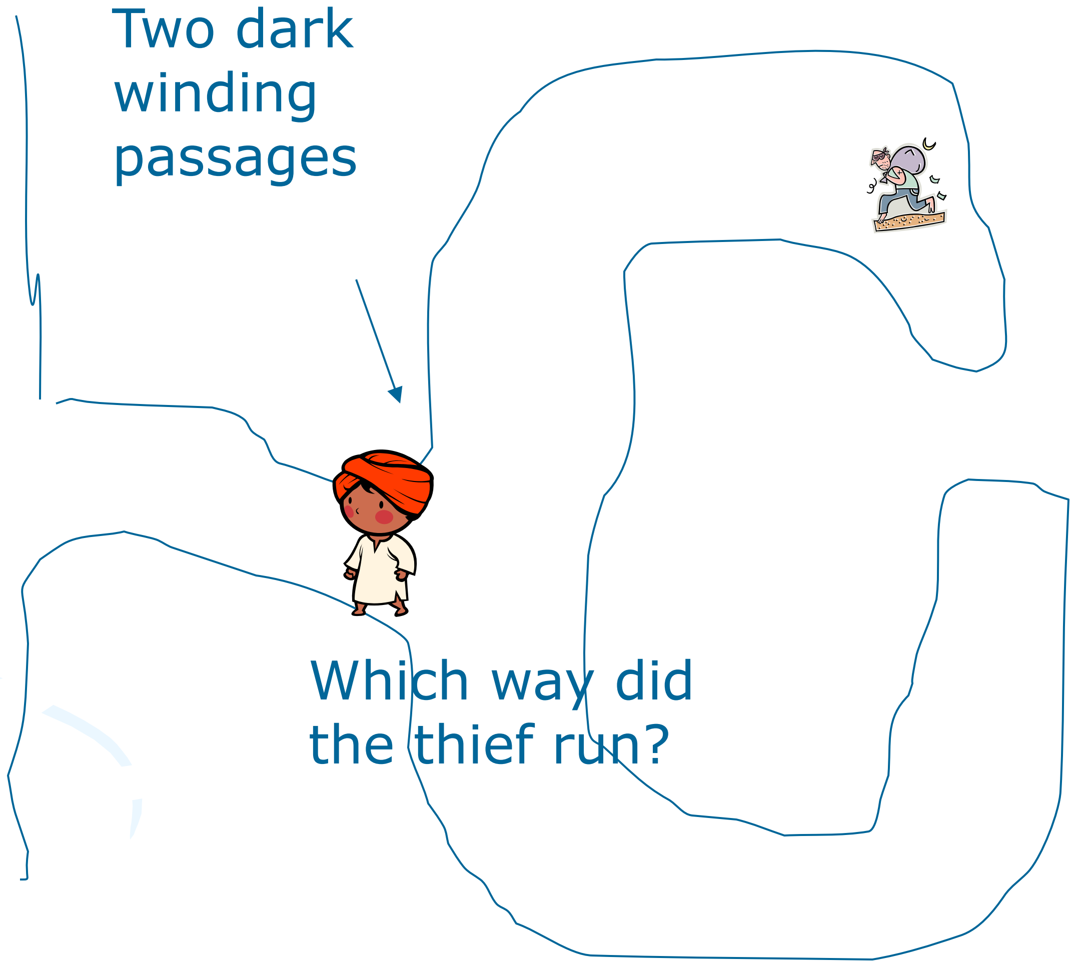
- Two party interactive game where Alice (called the prover) proves to Bob (called the verifier) that a predicate of statement holds true without letting Bob learn the method of Alice's proof.
- The game uses **Interactive proof (IP) System**.
- Sometimes it is called as "**proof in the dark**".
- Verifier after been convinced the validity of the what is being proved cannot have learned the knowledge possessed by the prover.
- Any third party watching the game learns nothing.

Zero Knowledge Protocols

General Ideas:

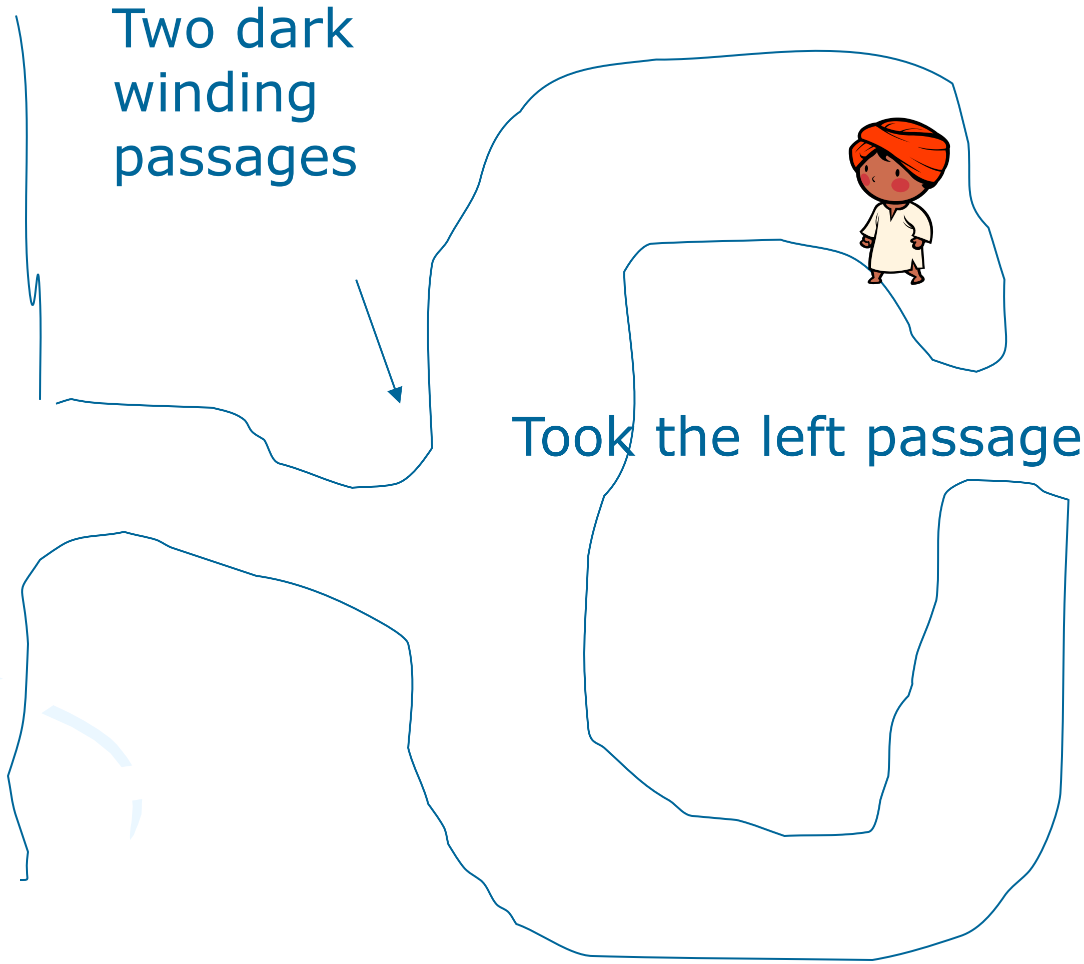
- The prover has certain knowledge (protected by some one-way function and an hard problem).
- The verifier is ignorant of this knowledge.
- The prover uses his knowledge to convince the verifier that he holds that knowledge.
- The information leaked while proving is **zero**.

Ali baba's cave story



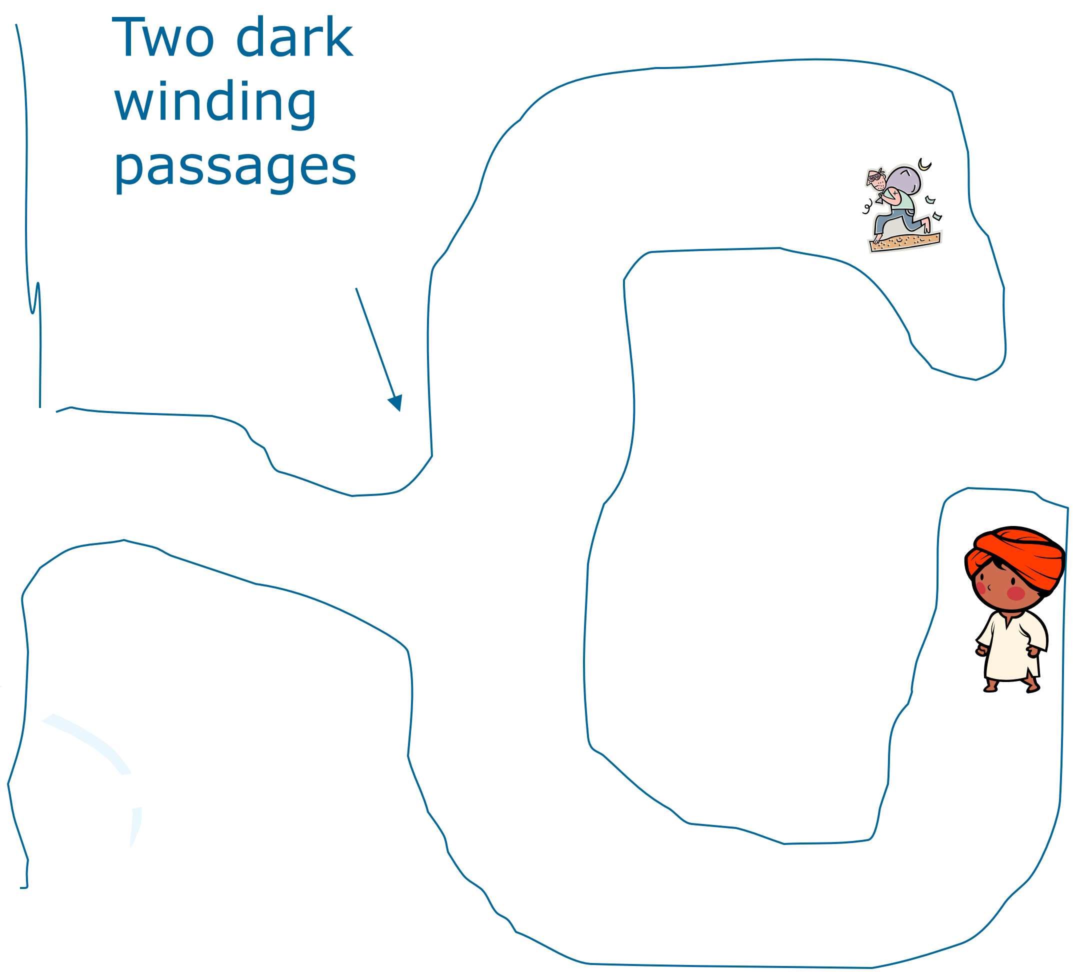
Read the article on this topic by Quisquarter et.al on the internet

First day he misses him



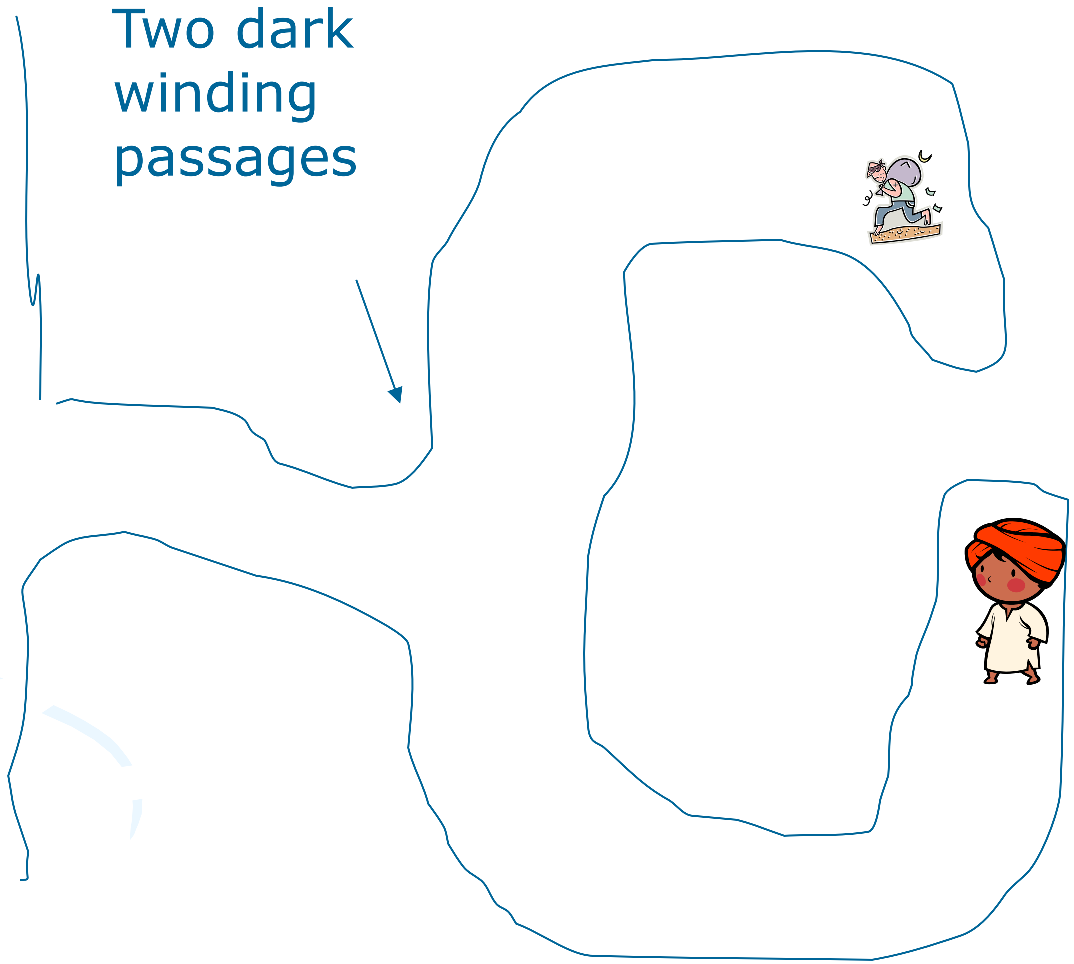
Read the article on this topic by Quisquarter et.al on the internet

Next day he misses him too



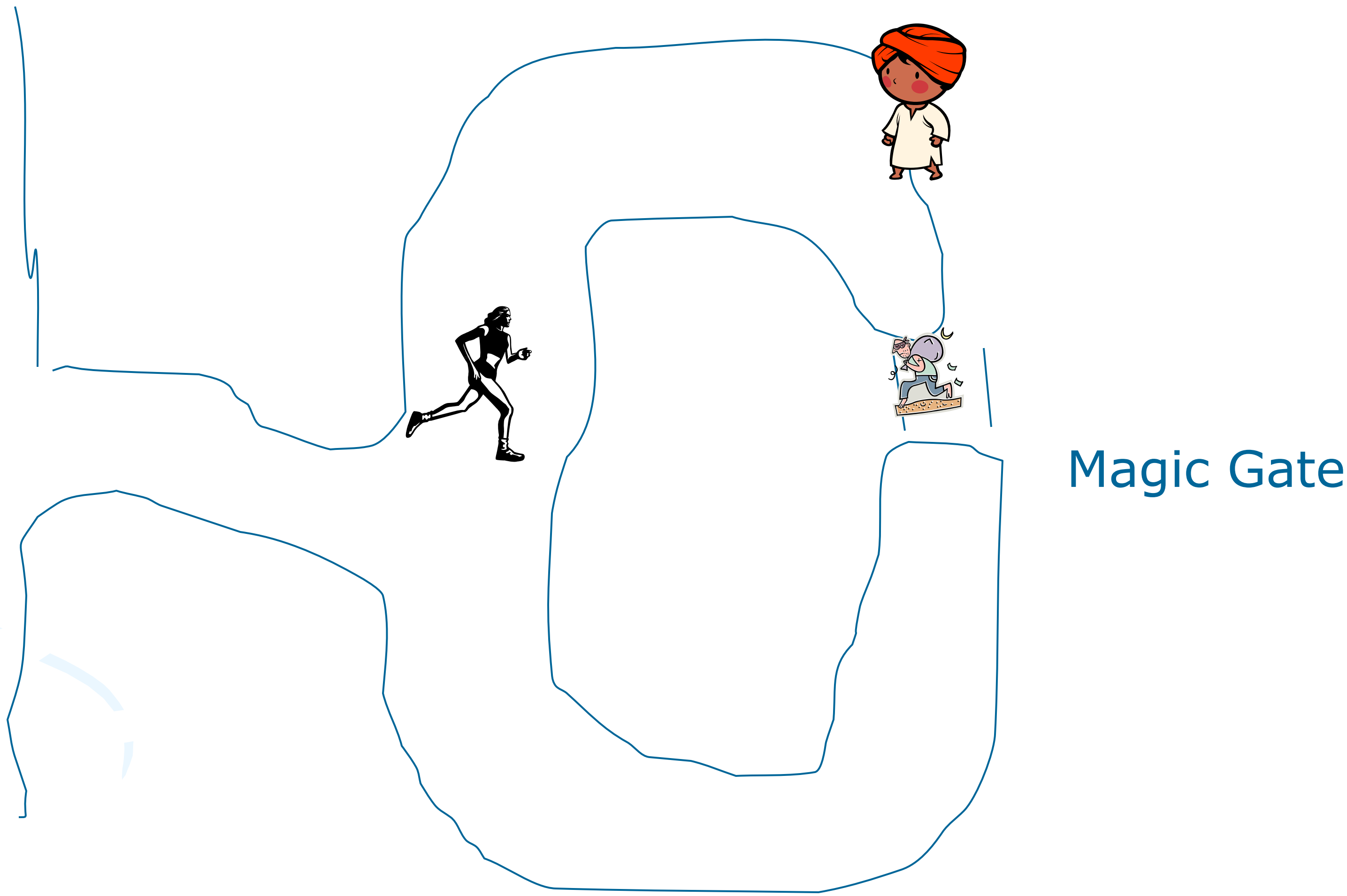
Read the article on this topic by Quisquarter et.al on the internet

Was thief lucky for 40 times



Read the article on this topic by Quisquarter et.al on the internet

Ali Baba learns the secret



Read the article on this topic by Quisquarter et.al on the internet

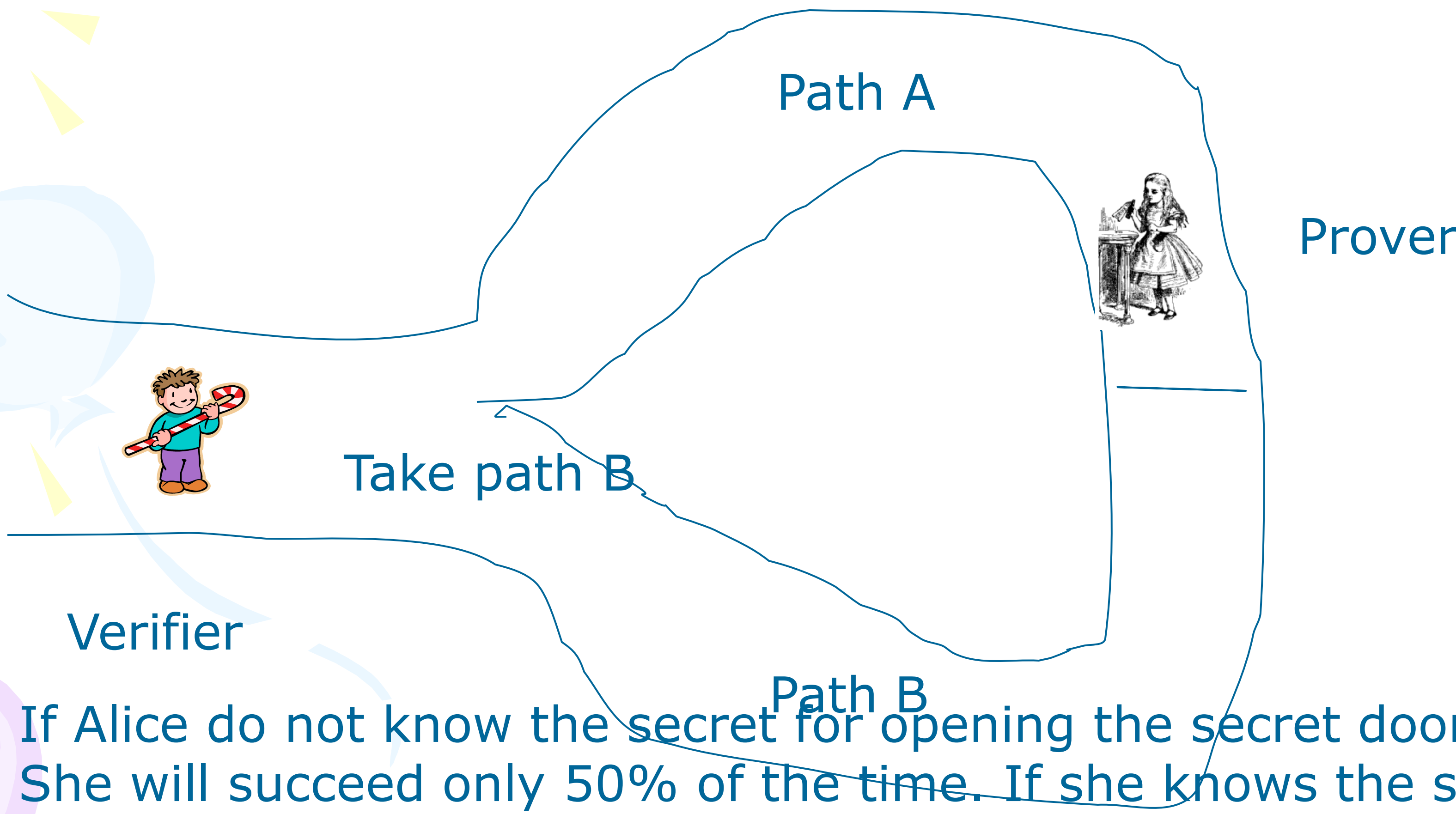
Modern version

- Manuscript to modern times-one of descendent of Ali broke the code.
- Sold the story to a tv network –
- Jealous reporter
- Court judgement- a proof obtained by one person cannot be transferred to others.

Cont.

- Tests in parallel-
- Jealous reporter’s tale is a case of a prior agreement.
- A single test with million passages.

A protocol



If Alice do not know the secret for opening the secret door, She will succeed only 50% of the time. If she knows the secret She will succeed always. Repeating the above steps increases the confidence of the verifier

Nature of Zero Knowledge protocols

- Alice holds some secret and a corresponding public protected by some hard problem.
- At the end of the protocol Bob is convinced that Alice holds the secret.
- Alice(Prover) Bob (Verifier)
- Repeat the following m times
- {
- Computes **Commit** ---------------→
- <----------------- **Challenge**
- **Response** -------→ Bob verifies **Response**
- reject if verification fails
- }
- Bob accepts

Simple Scheme

- Let p be a prime and g be a generator of Z_p
- Let A's Secret be a, $1 \le a < p$ and its public parameter is $y = g^a$.
- A will prove this to B that A knows this secret `a' by announcing a witness g^r, where r is a random number.
- B's Challenge is a random c, $1 \le c < p$
- A's response is $u = r + c\,a$.
- B can verify that $g^u = g^r y^c$

$y = g^a$: public information of A

Choose random r

Witness g^r

g^r →

Challenge c

←

Challenge
c = random

$U = r + ac$ →

U

Response

Mod (p-1)

Verification
Accept if
$g^{\mathbf{u}} = g^r y^{\mathbf{c}}$ **Mod p**

Operations on Integer Ring

Operations in Finite Field

Schnorr's Identification Protocol

- COMMON PARAMETERS
- P, q: two primes, q divides (p-1) ($q \mid (p-1)$;
- Size of p = 1024 bits, size of q = 160 bits;
- g: An Element of order q, i.e $g^q = 1 \bmod p$;
- y: $y = g^{-a} \pmod{p}$;
- Alice's Public Key Material (p,q,g,y), certified by Certificate Authority
- Alice's Private Key information: $a < q$;
- After the protocol Bob is certain that Alice knows some a in Z_q
- with a property $y = g^{-a} \pmod{p}$;

Schnorr's Identification Protocol. Contd.

- Repeat the following steps m times
- Alice picks k in Z^q computes **Commit** ← g^k (mod p)
- Alice Sends **Commit** to Bob
- Bob picks **Challenge** and Sends it to Alice
- Alice Computes **Response** ← k + a * **challenge** (mod q) and Sends **Response** to Bob
- Bob checks if Commit = $g^{\textbf{Response}} y^{\textbf{Challenge}}$ (mod p);
- he rejects and abort if the checking shows error

- Bob accepts the fact that Alice knows a such that $y = g^{-a}$ (mod p);
-

Verification Equation

- The verification equation:
- Commit = $g^{\textbf{Response}}\ y^{\textbf{Challenge}}$ (mod p);

- RHS:=$g^{(k + a * \textbf{challenge})} * g^{\textbf{(-a*Challenge)}}$
- = g^{k}
- = Commit = LHS

Summary

- Zero Knowledge proofs
- Schnor’s ZKN protocol