CSE 539: Applied Cryptography Week 10: Basic Crypto - Review

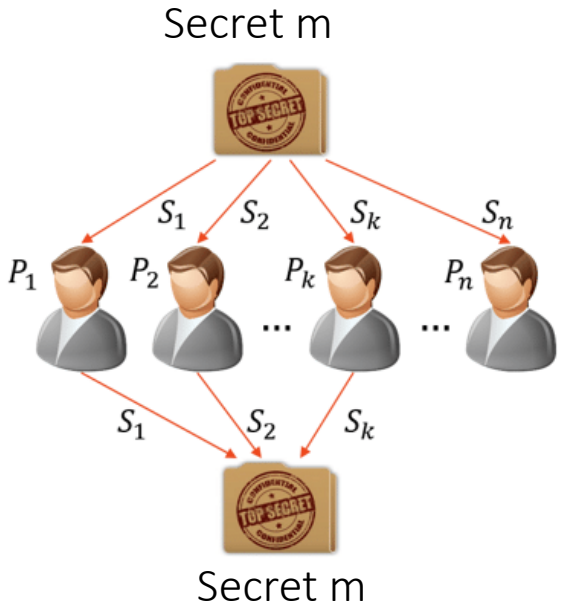
Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap15.pdf

Secret Sharing

- m – Secret to be shared
- P – Set of participants

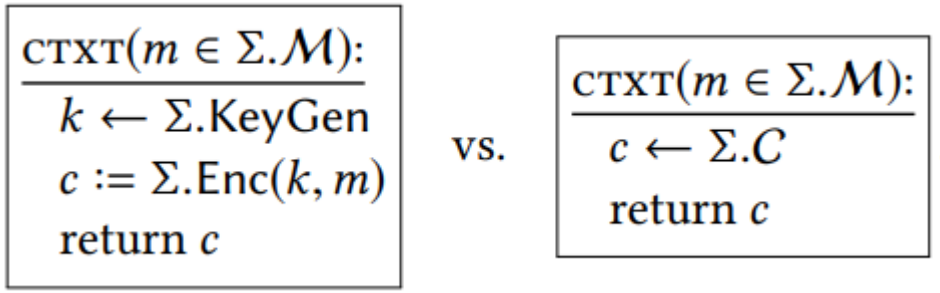
=> A qualified subsets of can reconstruct m



- Formally, secret sharing scheme allows share a secret m among n parties such that for a fixed number t < n, the following conditions are satisfied.
  - If < t parties get together, then they get no additional information about the secret.
  - If > t parties get together, then they can correctly reconstruct the secret

Provable Security

- "Real-vs-Random" Style of Security Definition



CPA: secure if Adversary chooses plaintext

- Cares about m ---> c direction

CCA: secure if Adversary gets all of Dec(ctxt)

- Cares about c ---> m direction

Pseudorandom Generator

- A PRG is a function $\mathbf{G}: \{0,1\}^{\lambda} \to \{0,1\}^{\lambda+\ell}$
- Security:

Let $G : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda+\ell}$ *be a deterministic function with* $\ell > 0$. *We say that* G *is a* ***secure pseudorandom generator (PRG)*** *if* $\mathcal{L}^{G}_{\text{prg-real}} \approx \mathcal{L}^{G}_{\text{prg-rand}}$, *where:*

$\mathcal{L}^{G}_{\text{prg-real}}$

QUERY():
$s \leftarrow \{0,1\}^{\lambda}$
return $G(s)$

$\mathcal{L}^{G}_{\text{prg-rand}}$

QUERY():
$r \leftarrow \{0,1\}^{\lambda+\ell}$
return r

PRG/PRF/PRP

- A PRG is a function $\mathbf{G}: \{0,1\}^{\lambda} \rightarrow \{0,1\}^{\lambda+\ell}$
- A PRF is a function $\mathrm{F}: \{0,1\}^{\lambda} \times \{0,1\}^{in} \rightarrow \{0,1\}^{out}$
- A PRP is a function $\mathrm{F}: \{0,1\}^{\lambda} \times \{0,1\}^{blen} \rightarrow \{0,1\}^{blen}$

Message Authentication Code (MAC)

- A MAC is like a signature that can be added to a piece of data, which certifies that someone who knows the secret key attests to this particular data

- A MAC scheme is a secure MAC if the adversary knows valid MACs corresponding to various messages, she cannot produce a valid MAC for a different message.

Hash Function

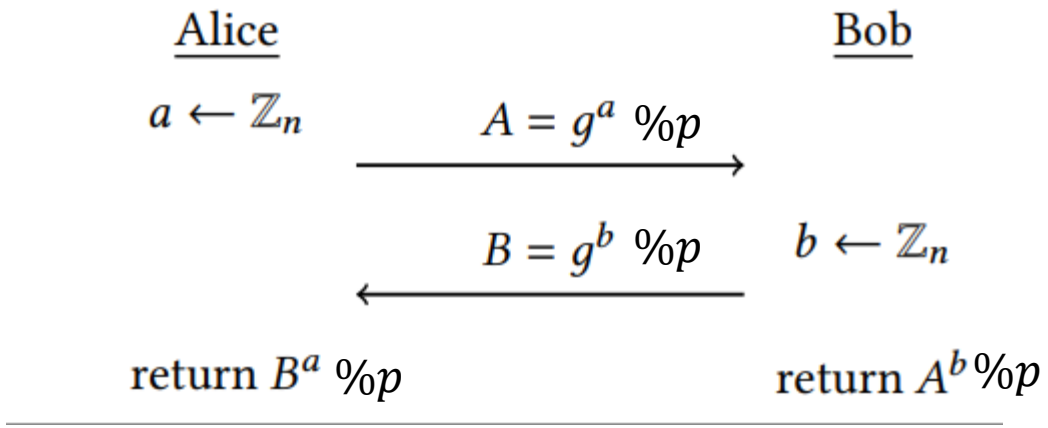
- A hash function maps a message of an arbitrary length to a n-bit output

$$\boldsymbol{H}: \{\mathbf{0},\mathbf{1}\}^* \rightarrow \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}$$

- Collision resistance:
  - It should be hard to compute any collision x ≠ x’ such that H(x) = H(x’)

- Second-preimage resistance (weak collision resistant):
  - Given x, it should be hard to compute any collision involving x. In other words, it should be hard to compute x’ ≠ x such that H(x) = H(x’)

DHKE



Definition 14.2 (Discrete Log) *The **discrete logarithm problem** is: given $X \in \langle g \rangle$, determine a number x such that $g^x = X$. Here the exponentiation is with respect to the multiplication operation in $\mathbb{G} = \langle g \rangle$.*

Public Key