CS 578 – Cryptography

Prof. Michael Backes

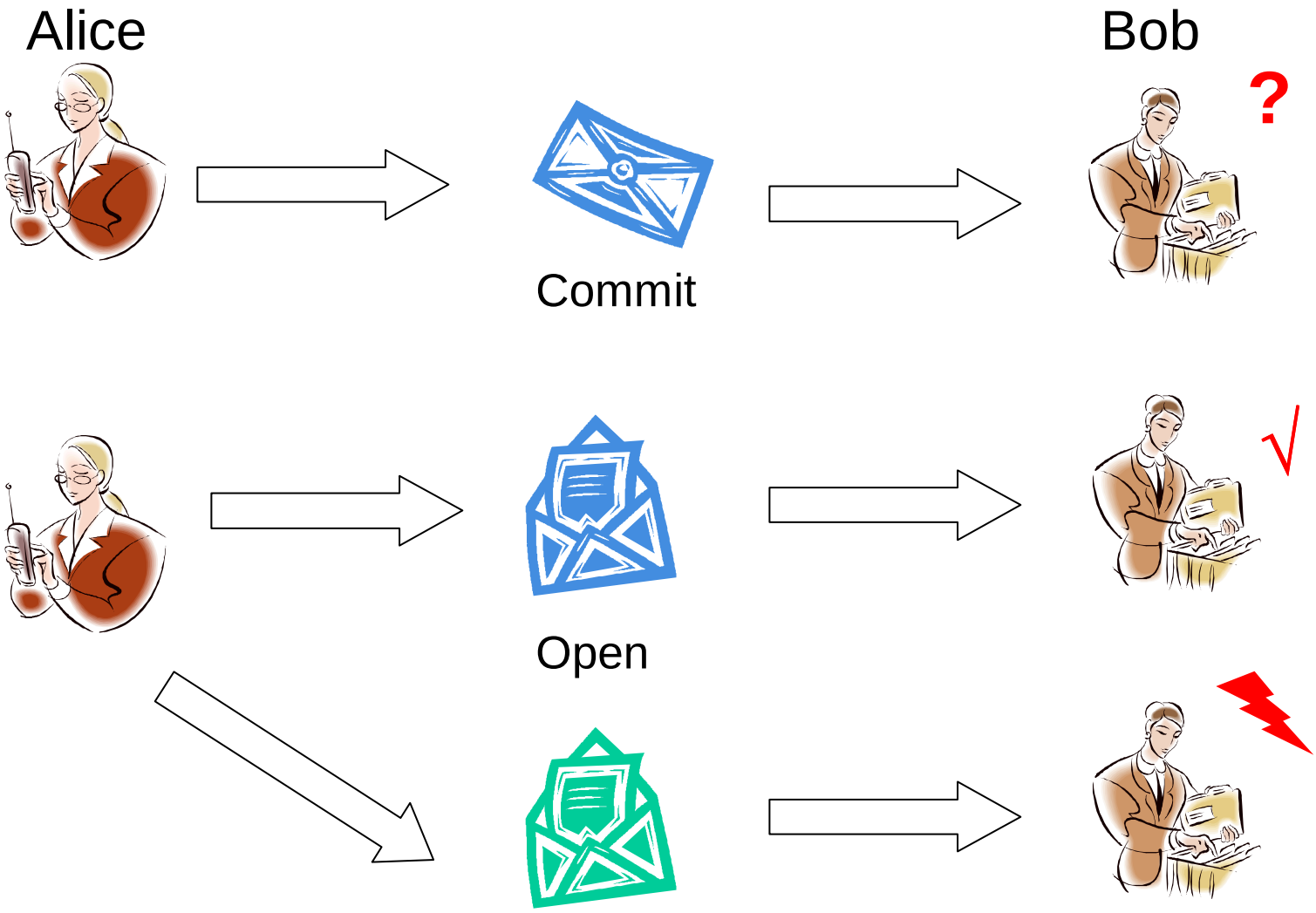
Commitment Schemes

June 30, 2006

Administrative Announcements

- Handouts
  - Lecture notes on authentication methods, SSL, etc.
  - Lecture notes on commitment schemes

Idea of Commitment Schemes



Commitment Schemes

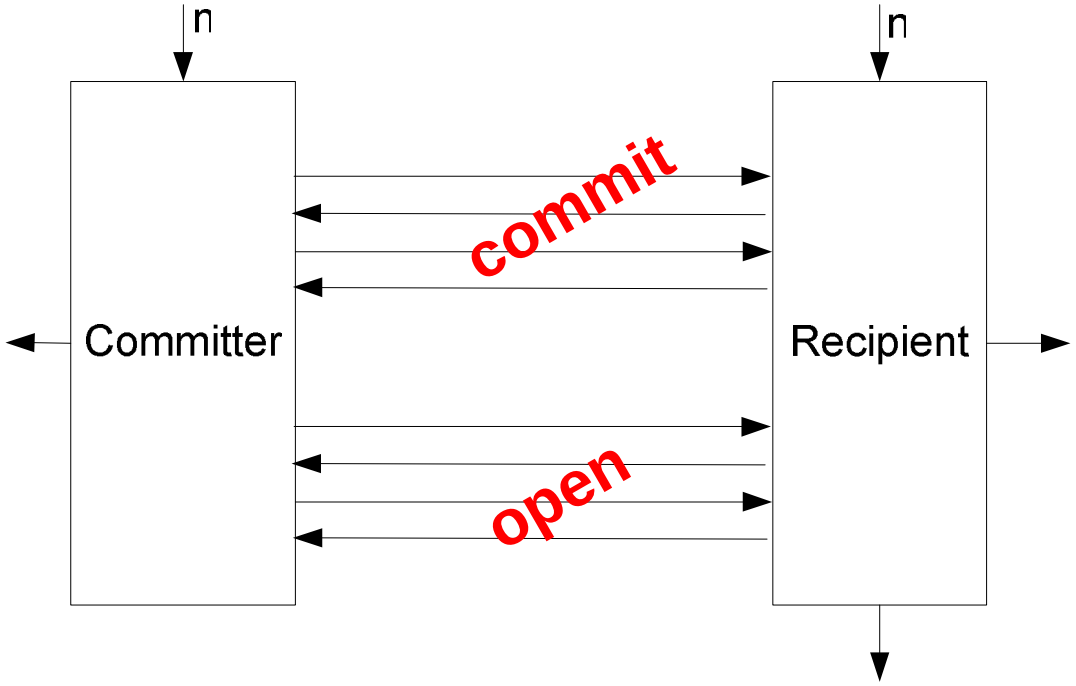
- Definition (Commitment Scheme): A (two-party) commitment scheme consists of two interactive algorithms (commit, open):
  - commit: The committer receives a message m; the recipient obtains no input. Neither committer nor recipient make any output except for a value acc $\in$ {ok, error}.
  - open: The same committer and recipient (maintaining state from the commit phase) take part. No inputs are needed. Recipient either outputs “(accept, m)” for some m or “reject”.

Commitment Schemes

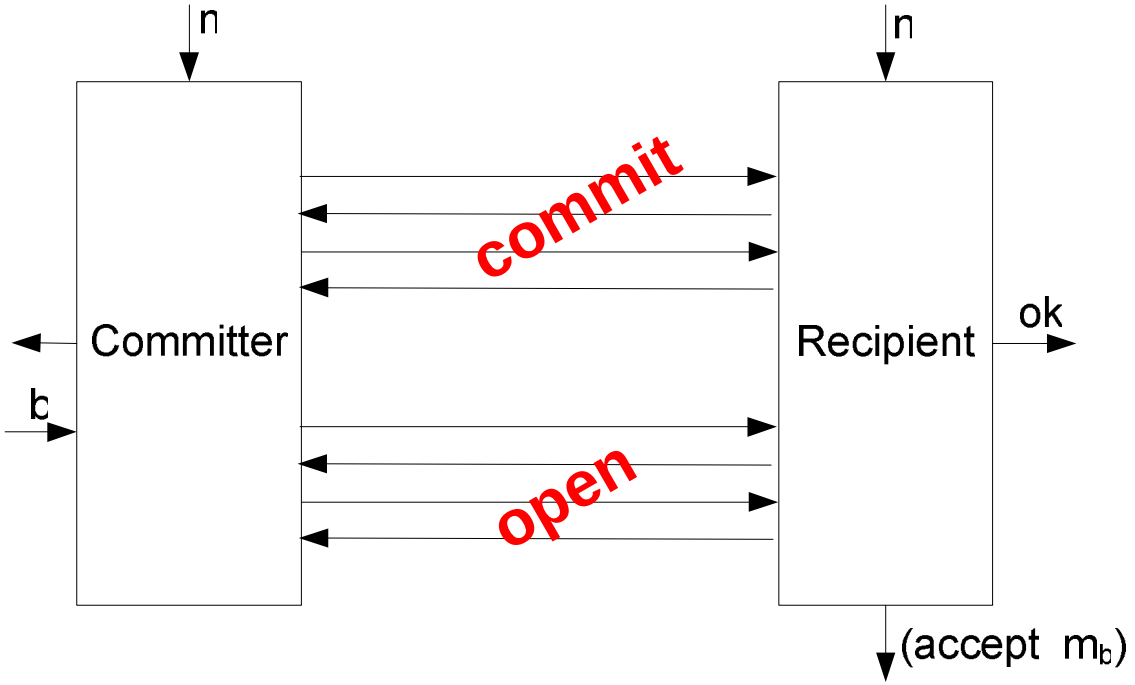
- Properties of a commitment scheme
  - Correctness: If both committer and recipient are honest and run *commit* (on m) and then *open*, then the recipient outputs (accept, m).
  - Binding: Even if the committer is dishonest, he cannot open the commitment in two different ways, i.e., after a successful *commit*, causing the recipient to output (accept, m) or (accept, m') in the *open* protocol.
  - Hiding: The *commit* protocol should not give the recipient any information on m.

Hiding and Binding Definitions

- Let (commit, open) be a commitment scheme.



Binding



- (commit, open) is information-theoretically (computationally) binding if the probability for all (efficient) adversaries is negligible that the challenger outputs (accept, m_0) and (accept, m_1) for b=0 and b=1, respectively, such that $m_0 \neq m_1$.

Interesting Special Cases

- Interesting special cases:
  - Non-interactive commitment schemes: commit is only a single message from committer to recipient
    → Allows for broadcasting the commitment (the message)
  - Publicly verifiable commitment schemes: recipient's result of the open protocol can be inferred from the messages sent.
  - Commitment-schemes with non-interactive opening: as before for the open protocol
- Existing schemes are almost all publicly verifiable and with non-interactive opening

An Impossibility Result

- Theorem: No commitment scheme can be information-theoretically binding and information-theoretically hiding.

- (But information-theoretically binding and computationally hiding is possible, and vice versa)

Information-theoretically Binding Schemes

- Information-theoretically binding schemes constructible from public-key encryption schemes.
- *commit* (on m):
  - Committer generates a pair (sk, pk) := gen(n ; r_1) using randomness r_1, where gen is the key generation algorithm.
  - Committer encrypts m using randomness r_2:
    c := enc(pk, m ; r_2) and outputs
    com:= (pk, c).
- *Open*:
  - Committer sends (m, r_1, r_2).
  - Recipient computes (sk*, pk*) := gen(n ; r_1) and
    c* := enc(pk*, m ; r_2). If (pk*, c*) = com and m in the message space, recipient outputs (accept, m), else reject.

Information-theoretically Binding Schemes

- Theorem: This commitment scheme is information-theoretically binding, and it is computationally hiding if the encryption scheme is CPA-secure.

  [proof on the board]

Back to Number Theory

- Recall lemma: $x \in Z_N$ is invertible in Z_N if and only if gcd(x,N) = 1.
- Denote the of invertible elements in Z_N by Z^*_N
- Define set of quadratic residues modulo N as

$$QR_N := \{x \in Z^*_N \mid \exists\, y \in Z^*_N : y^2 = x \bmod N\}$$

- Lemma: Let N be an arbitrary natural number. Then
  - If y is a root of x mod N, then so is –y.
  - The set QR_N is a subgroup of Z^*_N, i.e., a multiplicative group.
  - If $x_1 \in QR_N$ and $x_2 \notin QR_N$, then $x_1 \cdot x_2 \notin QR_N$.

[proof on the board]

Back to Number Theory

- Now special case $N = pq$ for primes $p \neq q$.
- Lemma: For $N = pq$ for primes $p \neq q$, we have
  - For all $x \in Z^*_N$:

    $$x \in QR_N \Leftrightarrow x \in QR_p \wedge x \in QR_q.$$

  - Every $x \in QR_N$ has exactly 4 square roots.

[proof on the board]

Back to Number Theory

- Definition (Jacobi Symbol). The Jacobi symbol of $x \in Z^*_N$ over N=pq for primes p,q is defined as

$$\left(\frac{x}{N}\right) := \left(\frac{x}{p}\right) \cdot \left(\frac{x}{q}\right)$$

- Define

$$Z_N^{(+1)} := \left\{ x \in Z_N^* \mid \left(\frac{x}{N}\right) = 1 \right\}$$

Back to Number Theory

- Lemma (Jacobi Symbol):
  - For N = pq for primes p ≠ q, we have

$$\left(\frac{x}{N}\right)=1 \Leftrightarrow (x \in QR_p \wedge x \in QR_q) \vee (x \notin QR_p \wedge x \notin QR_q)$$

  - The Jacobi symbol is multiplicative, i.e., for all x,y ∈ Z^*_N

$$\left(\frac{xy}{N}\right) := \left(\frac{x}{N}\right) \cdot \left(\frac{y}{N}\right)$$

  - $Z_N^{(+1)}$ is a multiplicative subgroup of Z^*_N

[proof on the board]

Back to Number Theory

- Now again special case: N = pq for primes $p \neq q$ with $p = 3 \bmod 4$ and $q = 3 \bmod 4$.
- Lemma: For such N, we have
  - -1 is a quadratic non-residue with Jacobi symbol 1, i.e.,

$$-1 \notin QR_N \wedge \left(\frac{-1}{N}\right) = 1$$

  - The non-squares with Jacobi symbol 1 are exactly the negatives of the squares, i.e.,

$$Z_N^{(+1)} \setminus QR_N = -QR_N$$

  - Anybody who knows p and q can compute (all four) square roots of all $x \in QR_N$.

[proof on the board]

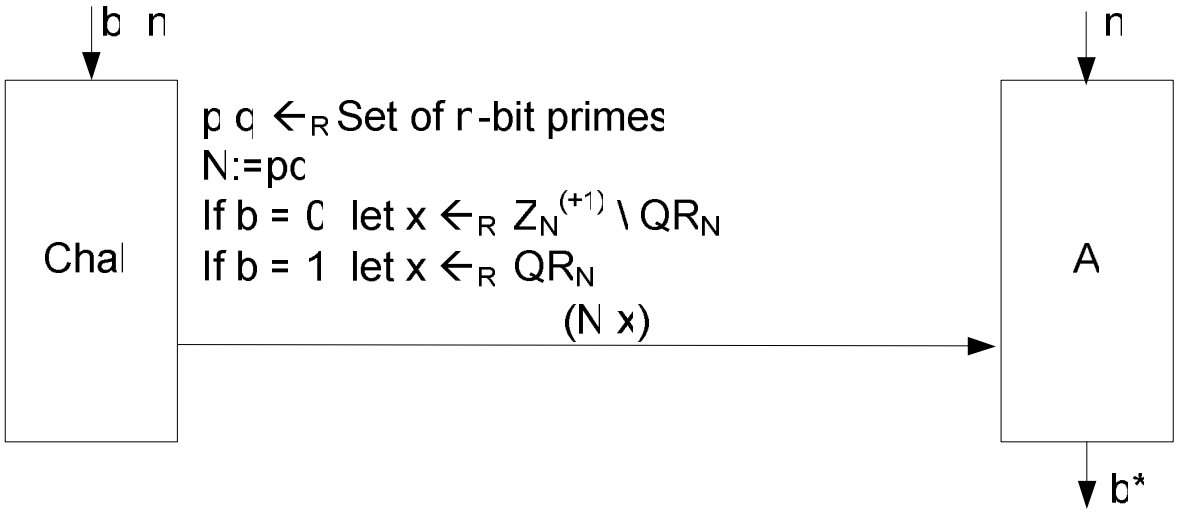
Back to Number Theory

- Lemma: Let N = pq for primes $p \neq q$, but p,q unknown. Then
  - Extracting square roots is infeasible under the factoring assumption
  - Anybody can efficiently choose elements of QR_N randomly and uniformly.
  - Anybody can efficiently compute Jacobi symbols modulo N.

Quadratic Residuosity Assumption

- Quadratic Residuosity Assumption (QRA):
  Given n-bit primes p and q, $p \neq q$, N:=pq, and a random $x \in Z_N^{(+1)}$, no efficient adversary can tell if $x \in QR_N$ or $x \notin QR_N$ when given (N,x).
- Special case 3-QRA
  - Same as QRA but special case p = 3 mod 4 and q = 3 mod 4
  - 3-QRA as hard as QRA by Dirichlet's prime theorem (Approximately half the primes are congruent 3 mod 4. Thus if A won against QRA with prob. P, then A would win against 3-QRA with prob. P/4.)

QRA as a Game



- The advantage of adversary A in breaking QRA is $Adv^{QRA}[A] = |Pr[EXP_A^{QRA}(0)=1] – Pr[EXP_A^{QRA}(1)=1]|$
- QRA Assumption: $Adv^{QRA}[A]$ negligible in n for all efficient A.

Information-theoretically Binding Schemes

- Quadratic residuosity scheme (for single bits)
- *commit* (on m):
  - Committer randomly chooses n-bit primes p,q with p=3 mod 4 and q = 3 mod 4, and sets N:=pq.
    Committer then chooses $y \leftarrow_R Z^*_N$, computes

    $$x := (-1)^m \cdot y^2 \bmod N$$

    and outputs com = (N,x).
- *Open*:
  - Committer sends (m, p, q, y).
  - Recipient checks if p,q primes with p=3 mod 4 and q = 3 mod 4, and if N=pq. Then he checks if $x = (-1)^m \cdot y^2 \bmod N$. If so, he outputs (accept, m), else reject.

The Quadratic Residuosity Scheme

- Theorem: The quadratic residuosity commitment scheme is information-theoretically binding, and it is computationally hiding under the quadratic residuosity assumption.

  [proof on the board]

- Extension to multiple bits easily doable

The Quadratic Residuosity Scheme

- Special properties of the scheme
  - Once N is known, anyone can make commitments with respect to N. The committer can open them all.
  - The commitments are homomorphic: Given two bit commitments x_1 and x_2 with respect to the same N, $x_1 \cdot x_2$ is a commitment to $m_1 \oplus m_2$ where m_i is the content of x_i. (essentially useful for extensions to string commitments)
  - Once N is known, anyone can blind commitments, i.e., transform commitments into a random commitment to the same bit.

    [proof of part a) and c) on the board]