

Saarland University

# CS 578 – Cryptography

Prof. Michael Backes

---

## Commitment Schemes

---

June 30, 2006

---

---

---

---

---

---

---

---

Saarland University

## Administrative Announcements

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

---

---

---

---

---

---

---

---

Saarland University

## Idea of Commitment Schemes

The diagram shows three scenarios of commitment and decommitment:

- Commit:** Alice sends a blue envelope icon labeled "Commit" to Bob. Bob is shown with a red question mark, indicating uncertainty.
- Open:** Alice sends a blue envelope icon labeled "Open" to Bob. Bob is shown with a red checkmark, indicating successful verification.
- Decommit:** Alice sends a green envelope icon to Bob. Bob is shown with a red lightning bolt, indicating a failed or invalid decommitment.

---

---

---

---

---

---

---

---

## 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  $m$ .

---

---

---

---

---

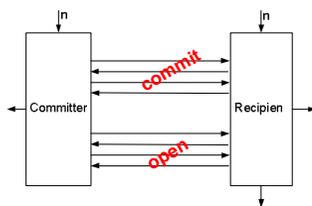
---

---

---

## Hiding and Binding Definitions

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




---

---

---

---

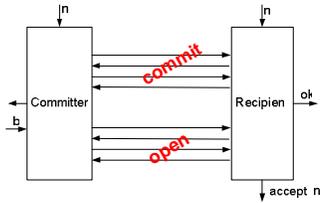
---

---

---

---

## 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  $(sk, pk) := \text{gen}(n; r_1)$  using randomness  $r_1$ , where  $\text{gen}$  is the key generation algorithm.
  - Committer encrypts  $m$  using randomness  $r_2$ :  $c := \text{enc}(pk, m; r_2)$  and outputs  $\text{com} := (pk, c)$ .
- **Open**:
  - Committer sends  $(m, r_1, r_2)$ .
  - Recipient computes  $(sk^*, pk^*) := \text{gen}(n; r_1)$  and  $c^* := \text{enc}(pk^*, m; r_2)$ . If  $(pk^*, c^*) = \text{com}$  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:  $x \in \mathbb{Z}_N$  is invertible in  $\mathbb{Z}_N$  if and only if  $\text{gcd}(x, N) = 1$ .
- Denote the set of invertible elements in  $\mathbb{Z}_N$  by  $\mathbb{Z}_N^*$ .
- Define set of quadratic residues modulo  $N$  as  $\text{QR}_N := \{x \in \mathbb{Z}_N^* \mid \exists y \in \mathbb{Z}_N^*, y^2 = x \pmod N\}$
- **Lemma**: Let  $N$  be an arbitrary natural number. Then
  - If  $y$  is a root of  $x \pmod N$ , then so is  $-y$ .
  - The set  $\text{QR}_N$  is a subgroup of  $\mathbb{Z}_N^*$ , i.e., a multiplicative group.
  - If  $x_1 \in \text{QR}_N$  and  $x_2 \notin \text{QR}_N$ , then  $x_1 \cdot x_2 \notin \text{QR}_N$ .

[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  $x \in \mathbb{Z}_N^*$ :
 
$$x \in \text{QR}_N \Leftrightarrow x \in \text{QR}_p \wedge x \in \text{QR}_q.$$
  - Every  $x \in \text{QR}_N$  has exactly 4 square roots.

[proof on the board]

---

---

---

---

---

---

---

---

## Back to Number Theory

- **Definition (Jacobi Symbol).** The Jacobi symbol of  $x \in \mathbb{Z}_N^*$  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

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

---

---

---

---

---

---

---

---

## Back to Number Theory

- **Lemma (Jacobi Symbol):**

- For  $N = pq$  for primes  $p \neq q$ , we have

$$\left(\frac{x}{N}\right) = 1 \Leftrightarrow (x \in \text{QR}_p \wedge x \in \text{QR}_q) \vee (x \notin \text{QR}_p \wedge x \notin \text{QR}_q)$$

- The Jacobi symbol is multiplicative, i.e., for all  $x, y \in \mathbb{Z}_N^*$

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

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

[proof on the board]

---

---

---

---

---

---

---

---

## Back to Number Theory

- Now again special case:  $N = pq$  for primes  $p \neq q$  with  $p \equiv 3 \pmod{4}$  and  $q \equiv 3 \pmod{4}$ .
- **Lemma:** For such  $N$ , we have
  - $-1 \notin QR_N$  and  $\left(\frac{-1}{N}\right) = 1$
  - The non-squares with Jacobi symbol 1 are exactly the negatives of the squares, i.e.,  $Z_N^{(+)} \setminus QR_N = -QR_N$
  - 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  $x \in Z_N^{(+)}$ , 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  $p \equiv 3 \pmod{4}$  and  $q \equiv 3 \pmod{4}$
  - 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.  $P/4$ .)

---

---

---

---

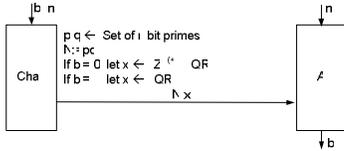
---

---

---

---

## QRA as a Game



- The advantage of adversary  $A$  in breaking QRA is  $\text{Adv}^{\text{QRA}}[A] = |\Pr[\text{EXP}_A^{\text{QRA}}(0)=1] - \Pr[\text{EXP}_A^{\text{QRA}}(1)=1]|$
- QRA Assumption:  $\text{Adv}^{\text{QRA}}[A]$  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  $p \equiv 3 \pmod{4}$  and  $q \equiv 3 \pmod{4}$ , and sets  $N := pq$ . Committer then chooses  $y \leftarrow_{\mathcal{R}} \mathbb{Z}_N^*$ , computes  $x := (-1)^m \cdot y^2 \pmod{N}$  and outputs  $\text{com} = (N, x)$ .
- *Open*:
  - Committer sends  $(m, p, q, y)$ .
  - Recipient checks if  $p, q$  primes with  $p \equiv 3 \pmod{4}$  and  $q \equiv 3 \pmod{4}$ , and if  $N = pq$ . Then he checks if  $x = (-1)^m \cdot y^2 \pmod{N}$ . 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]

---

---

---

---

---

---

---

---