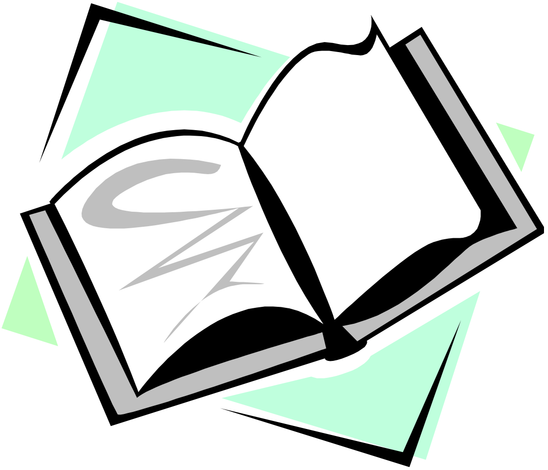
Cryptography
CS 555

Topic 20: Other Public Key Encryption Schemes

Outline and Readings

- Outline
  - Quadratic Residue
  - Rabin encryption
  - Goldwasser-Micali
  - Commutative encryption
  - Homomorphic encryption



- Readings:
  - Katz and Lindell: Chapter 11

Review: Quadratic Residues Modulo A Prime

- Definition: a is a quadratic residue modulo p if it has a square root, i.e., $\exists$ b $\in Z_p^*$ such that $b^2 \equiv a \bmod p$,
  - We write this as $a \in QR_p$
- Exactly half of elements in Z_p^* are in QR_p
  - let g be generator, $a=g^j$ is a quadratic residue iff. j is even.
- Each QR modulo p has two square roots in Z_p^*
- Legendre symbol indicates QR

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{if } \; p \mid a \\ 1, \text{if } \; a \in QR_p \\ -1, \text{if } \; a \in \overline{QR}_p \end{cases} \qquad \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$

Quadratic Residues Modulo a Composite n

Definition: a is a quadratic residue modulo n ($a \in QR_n$) if $\exists\, b \in Z_n^*$ such that $b^2 \equiv a \bmod n$, otherwise when $a \neq 0$, a is a quadratic nonresidue

Fact: $a \in QR_n$, where $n=pq$, iff. $a \in QR_p$ and $a \in QR_q$

- The "only if" direction: $b^2 \equiv a \bmod n$, then $b^2 \equiv a \bmod p$ and $b^2 \equiv a \bmod q$
- The "if" direction: If $b^2 \equiv a \bmod p$ and $c^2 \equiv a \bmod q$, then the four solutions to the four equation sets
    1. $x \equiv b \bmod p$ and $x \equiv c \bmod q$
    2. $x \equiv b \bmod p$ and $x \equiv -c \bmod q$
    3. $x \equiv -b \bmod p$ and $x \equiv c \bmod q$
    4. $x \equiv -b \bmod p$ and $x \equiv -c \bmod q$

  satisfies $x^2 \equiv a \bmod n$

For example

- Fact: if n=pq, then $x^2 \equiv 1 \pmod{n}$ has four solutions that are <n.
  - $x^2 \equiv 1 \pmod{n}$ if and only if
    both $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$
  - Two trivial solutions: 1 and n-1
    - 1 is solution to $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$
    - n-1 is solution to $x \equiv -1 \pmod{p}$ and $x \equiv -1 \pmod{q}$
  - Two other solutions
    - solution to $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{q}$
    - solution to $x \equiv -1 \pmod{p}$ and $x \equiv 1 \pmod{q}$
  - E.g., $n=3\times5=15$, then $x^2 \equiv 1 \pmod{15}$ has the following solutions: 1, 4, 11, 14

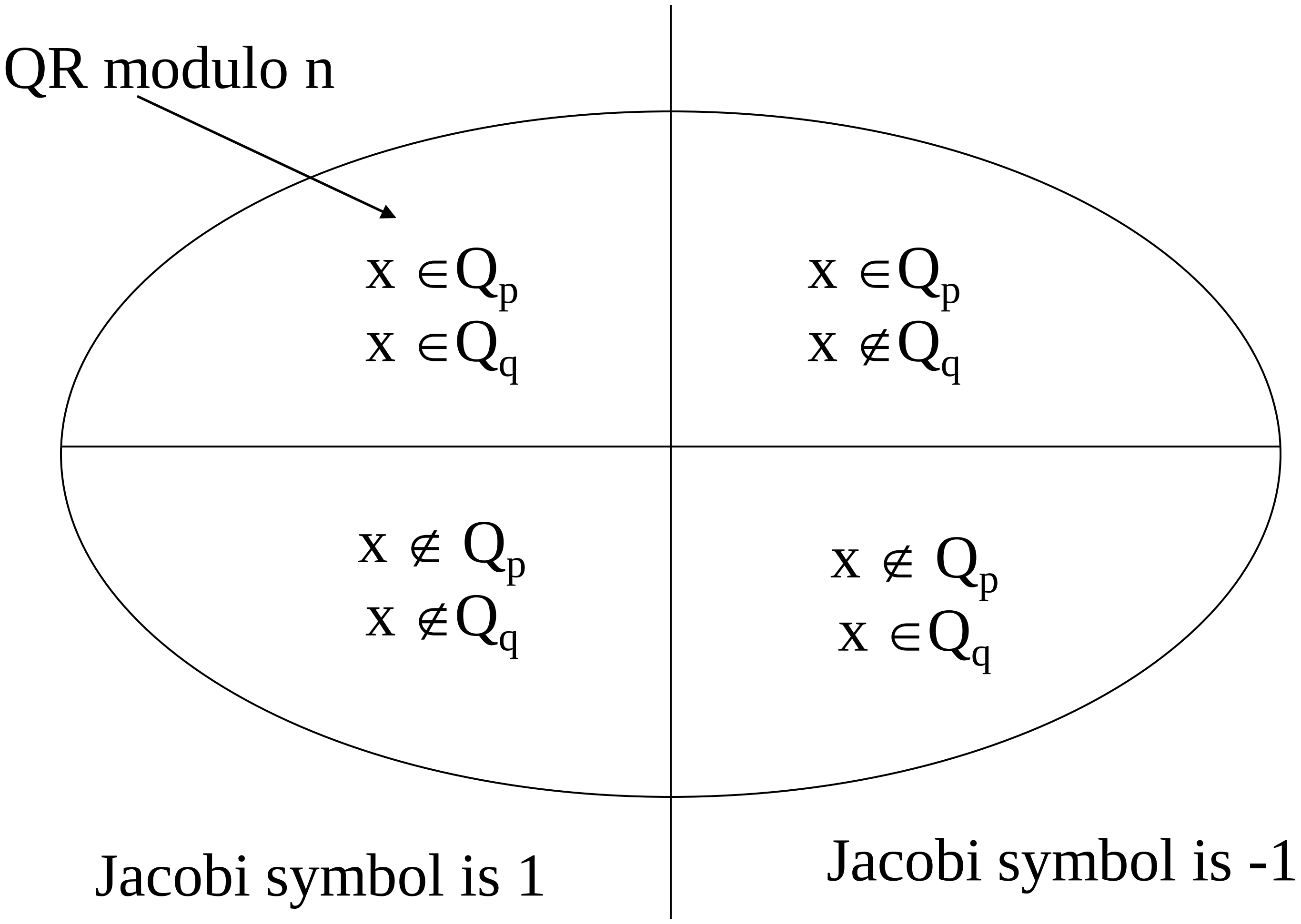
Quadratic Residues Modulo a Composite

- $|QR_n| = |QR_p| \bullet |QR_q| = (p-1)(q-1)/4$
- $|\overline{QR_n}| = 3(p-1)(q-1)/4$
- Jacobi symbol does not tell whether a number a is a QR

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

- when it is -1, then either $a \in Q_p \wedge a \notin Q_q$ or $a \notin Q_p \wedge a \in Q_q$, then a is not QR
- when it is 1, then either $a \in Q_p \wedge a \in Q_q$ or $a \notin Q_p \wedge a \notin Q_q$
  - A is QR for the former case, but not the latter case
- it is widely believed that determining QR modulo n is equivalent to factoring n, no proof is known
  - without factoring, one can guess correctly with prob. ½ for those with Jacobi symbol 1

Integers in Z_n*



The Rabin Encryption Scheme

- Motivation: The security of RSA encryption depends on the difficulty of computing the e'th root modulo n, i.e., given C, it is difficult to find M s.t. $M^e=C \bmod n$.
- It is not known that RSA encryption is as difficult as factoring.
- The Rabin encryption scheme is provably "secure" if factoring is hard
- Idea: rather than using an odd prime as e, uses 2
  - $f(x)=x^2 \bmod n$
  - this is not a special case of RSA as this function is not 1-to-1.

The Rabin Encryption Scheme

- Public key: n
- Privacy key: p, q s.t. n=pq
- Encryption: compute $c=m^2 \bmod n$
- Decryption: compute the square roots of c.
  - how many are there?
- Fact:
  - when $p \equiv q \equiv 3 \pmod 4$, deterministic algorithms exist to compute the square roots
    - When $p \equiv 3 \pmod 4$, $a^{(p+1)/4}$ is square root of a because
      $(a^{(p+1)/4})^2 = a^{(p+1)/2} = a^{(p-1)/2}\, a = a$
  - otherwise, efficient randomized algorithms exist to compute the square roots

Computing Square Roots is as hard as Factoring

- Given an algorithm A that can compute one square root of a number a modulo n,

- One can use A to factor n as follows
  - randomly pick x, compute $z = x^2 \bmod n$
  - ask A to compute the square root of z, A returns y
  - if y=x or y=n–x, then try again, otherwise, compute gcd(x+y,n) gives us a prime factor of n
  - as A has no way to tell which x we've picked, with prob. ½, A returns a square root that allows us to factor n

Pragmatic Considerations for the Rabin Encryption Scheme

- Normally, one picks $p \equiv q \equiv 3 \pmod 4$
- Textbook Rabin insecure, because it is deterministic
- Redundancy is used to ensure that only one square root is a legitimate message
- Encryption very fast, only one exponentiation
- Decryption comparable to RSA decryption

The Goldwasser-Micali Probablistic Encryption Scheme

- First provably semantically secure public key encryption scheme, security based on the hardness of determining whether a number x is a QR modulo n, when the factoring of n is unknown and the Jacobi symbol $\left(\frac{x}{n}\right)$ is 1

- Encryption is bit by bit
- For each bit in the plaintext, the ciphertext is one number in Z_n*, expansion factor is 1024 when using 1024 moduli

The Goldwasser-Micali Probablistic Encryption Scheme

- Key generation
  - randomly choose two large equal-size prime number p and q, pick a random integer y such that

$$\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1$$

  - public key is (n=pq, y)
  - private key is (p,q)
  - Property of y: y is not QR, but has Jacobi symbol 1
- Encryption
  - to encrypt one bit b, pick a random x in Z_n^*, and let $C=x^2y^b$
  - that is, $C=x^2$ when b=0, and $C=x^2y$ when b=1

The Goldwasser-Micali Probablistic Encryption Scheme

- Consider the Jacobi symbol of the ciphertext C

$$\left(\frac{x^2}{n}\right)=\left(\frac{x^2}{p}\right)\left(\frac{x^2}{q}\right)=1\bullet 1=1 \qquad \left(\frac{yx^2}{n}\right)=\left(\frac{yx^2}{p}\right)\left(\frac{yx^2}{q}\right)=-1\bullet -1=1$$

- Consider whether the ciphertext C is QR modulo n
  - C is QR iff. the plaintext bit b is 0
- Decryption:
  - knowing p and q s.t. n=pq, one can determine whether x is QR modulo n and thus retrieves the plaintext (how?)

Cost of Semantic Security in Public Key Encryption

- In order to have semantic security, some expansion is necessary
  - i.e., the ciphertext must be larger than its corresponding plaintext (why?)
  - the Goldwasser-Micali encryption scheme generate ciphertexts of size 1024m
  - suppose that all plaintexts have size m, what is the minimal size of ciphertexts to have an adequate level of security (e.g., takes 2^t to break the semantic security)?

Commutative Encryption

Definition: an encryption scheme is commutative if
$E_{K1}[E_{K2}[M]] = E_{K2}[E_{K1}[M]]$

- Given an encryption scheme that is commutative, then $D_{K1}[D_{K2}[E_{K1}[E_{K2}[M]] = M$
- That is, if message is encrypted twice, the order does not matter.
- Most symmetric encryption scheme (such as DES and AES) are not commutative

Examples of Commutative Encryption Schemes

- Private key: Pohlig-Hellman Exponentiation Cipher with the same modulus p
  - encryption key is e, decryption key is d, where ed≡1 (mod (p-1))
  - $E_{e1}[M] = M^{e1}$ mod p and $D_{d1}[C]= C^{d1}$ mod p
  - $E_{e1}[E_{e2}[M]] = M^{e1e2} = E_{e1}[E_{e2}[M]]$ (mod p)

The SRA Mental Poker Protocol

- How do two parties play poker without a trusted third party?
  - Need to deal each one a hand of card, and after placing bet, be able to show hand.
  - Setup: Alice and Bob agree on using M_1, M_2, …, M_{52} to denote the 52 cards.

- Any ideas?

The SRA Mental Poker Protocol

- Alice encrypts M_1, M_2, …, M_{52} using her key, then randomly permute them and send the ciphertexts to Bob
- Bob picks 5 ciphertexts as Alice’s hand and sends them to Alice
- Alice decrypts them to get his hand
- Bob picks 5 other ciphertexts as his hand, encrypts them using his key, and sends them to Alice
- Alice decrypts the 5 ciphertexts and sends to Bob
- Bob decrypts what Alice sends and gets his hand
- Both Alice and Bob reveals their key pairs to the other party and verify that the other party was not cheating. (Why need this step?)

Homomorphic Encryption

- Encryptions that allow computations on the ciphertexts
  - $E_k[m_1] \bullet E_k[m_2] = E_k[m_1 \circ m_2]$
- Applications
  - E-voting: everyone encrypts votes as 1 or 0, aggregate all ciphertexts before decrypting; no individual vote is revealed.
    - Requires additive homomorphic encryption: $\circ$ is +
  - Secure cloud computing.
    - Requires full homomorphic encryption, i.e., homomorphic properties for both + and $\times$

Homomorphic Properties of Some Encryption Schemes

- Multiplicative homomorphic encryption
  - Unpadded RSA: $m_1^e \times m_2^e = (m_1 \times m_2)^e$
  - El Gamal: Given public key $(g, h=g^a)$, ciphertexts $(g^{r1},h^{r1}m_1)$ and $(g^{r2},h^{r2}m_2)$, multiple both components $(g^{r1+r2},h^{r1+r2}m_1m_2)$
- Additive homomorphic encryption schemes
  - Paillier cryptosystem (will explore in HW problem)
- Fully homomorphic encryption also exist
  - Significantly slower than other PK encryption

Coming Attractions …

- Digital Signatures

- Reading: Katz & Lindell: Chapter 12.1 to 12.5