CPSC 467: Cryptography and Security

Michael J. Fischer

Lecture 19a
November 5, 2020

Quadratic Residues

- Modular square roots
- Square roots modulo an odd prime p
- Square roots modulo the product of two odd primes

Feige-Fiat-Shamir Authentication Protocol

Quadratic Residues

Squares and square roots

Recall that an integer r is a *square root* of x modulo n if

$$r^2 \equiv x \pmod{n}.$$

An integer x is a *quadratic residue (or perfect square)* modulo n if it has a square root modulo n.

We explore the properties of the *squaring function* $x \mapsto x^2 \bmod n$ and its “inverse”, $y \mapsto \sqrt{y} \bmod n$.

Generalized inverse

Because the squaring function $x \mapsto x^2 \bmod n$ is not one-to-one or onto, it is not uniquely invertible. Quadratic residues may have multiple square roots, whereas non-residues have none.

We broaden our notion of *inverse* by defining $\sqrt{y} \bmod n$ to be the set of all $x \in \mathbf{Z}_n$ such that $x^2 \equiv y \bmod n$.[1]

Thus, in the case that y is *not* a quadratic residue, $\sqrt{y} \bmod n = \emptyset$ (the empty set).

[1] This same notion of inverse applies to hash functions, which also are not generally one-to-one and are not required to be onto.

A computationally hard problem

The *quadratic residuosity assumption* says that computing $\sqrt{y}$ mod n is computationally hard when n is the product of two distinct large primes.

For such n, the squaring function is believed to be a one-way function.

One-way functions

Cryptography is built on the notion of *one-way function*, that is, a function that is easy to compute but hard to invert.

Can't prove that inversion is hard.

Instead, postulate it to be hard for particular well-studied functions that have no known feasible inversion algorithms.

Some presumed one-way functions and associated hard problems:

$(p, q) \mapsto p \cdot q$	Factoring problem
$x \mapsto g^x \bmod p$	Discrete log problem
$P \mapsto k \times P$	Elliptic curve discrete log problem
$x \mapsto H(x)$	Collision-finding problem
$x \mapsto x^2 \bmod n$	Quadratic residuosity problem

Quadratic residues in $\mathbf{Z}_n^*$

If $r, x \in \mathbf{Z}_n$ and $r^2 \equiv x \pmod{n}$, then

$$r \in \mathbf{Z}_n^* \text{ iff } x \in \mathbf{Z}_n^*.$$

Why? Because

$$\gcd(r, n) = 1 \text{ iff } \gcd(x, n) = 1$$

This follows from the fact that $r^2 = x + un$ for some u, so if p is a prime divisor of n, then

$$p \,|\, r \text{ iff } p \,|\, x.$$

QR_n and QNR_n

Assume from now on that $n = pq$ for p, q large distinct primes and all quadratic residues and square roots are in $\mathbf{Z}_n^*$ unless stated otherwise.

We partition $\mathbf{Z}_n^*$ into two parts.

$$\mathrm{QR}_n = \{x \in \mathbf{Z}_n^* \mid x \text{ is a quadratic residue modulo } n\}.$$
$$\mathrm{QNR}_n = \mathbf{Z}_n^* - \mathrm{QR}_n.$$

QR_n is the *set of quadratic residues* modulo n.

QNR_n is the *set of quadratic non-residues* modulo n.

Quadratic residues in $\mathbf{Z}_{15}^*$

The following table shows all elements of $\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and their squares.

r	$r^2 \bmod 15$
1	1
2	4
4	1
7	4
$8 \quad = -7$	4
$11 \quad = -4$	1
$13 \quad = -2$	4
$14 \quad = -1$	1

Thus, $\mathrm{QR}_{15} = \{1, 4\}$ and $\mathrm{QNR}_{15} = \{2, 7, 8, 11, 13, 14\}$.

Quadratic residues modulo an odd prime p

Fact

For an odd prime p,

- *Every $x \in QR_p$ has exactly two square roots in $\mathbf{Z}_p^*$;*
- *Exactly 1/2 of the elements of $\mathbf{Z}_p^*$ are quadratic residues.*

In other words, if $x \in \mathrm{QR}_p$,

$$|\sqrt{x}| = 2.$$

$$|\mathrm{QR}_p| = \frac{|\mathbf{Z}_p^*|}{2} = \frac{p-1}{2}.$$

Quadratic residues in $\mathbf{Z}_{11}^*$

The following table shows all elements $b \in \mathbf{Z}_{11}^*$ and their squares.

r	$r^2 \bmod 11$
1	1
2	4
3	9
4	5
5	3

r	$-r$	$r^2 \bmod 11$
6	-5	3
7	-4	5
8	-3	9
9	-2	4
10	-1	1

Thus, $\mathrm{QR}_{11} = \{1, 3, 4, 5, 9\}$ and $\mathrm{QNR}_{11} = \{2, 6, 7, 8, 10\}$.

Quadratic residues modulo pq

We now turn to the case where $n = pq$ is the product of two distinct odd primes.

Fact

Let $n = pq$ for p, q distinct odd primes.

- *Every $x \in QR_n$ has exactly four square roots in $\mathbf{Z}_n^*$;*
- *Exactly 1/4 of the elements of $\mathbf{Z}_n^*$ are quadratic residues.*

In other words, if $x \in \mathrm{QR}_n$ then $|\sqrt{x}| = 4$, so

$$|\mathrm{QR}_n| = \frac{|\mathbf{Z}_n^*|}{4} = \frac{(p-1)(q-1)}{4}.$$

Proof sketch

- Let $x \in \mathrm{QR}_n$. Then $x \in \mathrm{QR}_p$ and $x \in \mathrm{QR}_q$.
- There are numbers $r_p \in \mathrm{QR}_p$ and $r_q \in \mathrm{QR}_q$ such that
  - $\sqrt{x} \pmod{p} = \{\pm r_p\}$, and
  - $\sqrt{x} \pmod{q} = \{\pm r_q\}$.
- Each pair (u, v) with $u \in \{\pm r_p\}$ and $v \in \{\pm r_q\}$ can be combined to yield a distinct element $r_{x,y}$ in $\sqrt{x} \pmod{n}$.[2]
- Hence, $|\sqrt{x}| = 4$, and $|\mathrm{QR}_n| = \frac{1}{4}|\mathbf{Z}_n^*|$.

[2] To find $r_{x,y}$ from x and y requires use of the Chinese Remainder theorem (see Appendix).

Feige-Fiat-Shamir Authentication Protocol

Reprise: A simplified one-round FFS protocol

- $n = pq$, where p and q are distinct large primes.
- $v \in \mathrm{QR}_n$. $s \in \sqrt{v^{-1}} \pmod{n}$.
- n and v are public. s is Alice's secret.

FFS protocol:

	Alice		Bob
1.	Choose random $r \in \mathbf{Z}_n^*$.		
	Compute $x = r^2 \bmod n$.	$\xrightarrow{x}$	
2.		$\xleftarrow{b}$	Choose random $b \in \{0, 1\}$.
3.	Compute $y = rs^b \bmod n$.	$\xrightarrow{y}$	Check $x = y^2 v^b \bmod n$.

Properties of FFS protocol

We make three claims for the FFS protocol.

1. [Completeness] When both Alice and Bob are honest, Bob's check always succeeds.
2. [Soundness] If Mallory attempts to impersonate Alice without knowing her secret s, Bob's check will fail with probability at least $1/2$.
3. [Zero knowledge] Anything that Mallory can compute while interacting with Alice in the FFS protocol could also be computed without Alice's involvement. In particular, if Mallory can find Alice's secret s after running the FFS protocol, then he could have found s without ever talking to Alice.

Completeness

We showed in lecture 18 that Bob's check

$$x = y^2 v^r \bmod n.$$

always succeeds when both parties are honest.

Soundness

Theorem

Suppose Mallory doesn't know a square root of v^{-1}. Then Bob's verification will fail with probability at least 1/2.

Proof.

To successfully fool Bob, Mallory must come up with x in step 1 and y in step 3 satisfying $x = y^2 v^b \bmod n$.

Mallory sends x in step 1 before Bob chooses b, so she does not know which value of b to expect.

When Mallory receives b, she responds by sending some value y, which we will call y_b, to Bob.

(continued. . .)

Proof: case 1

Proof (continued).

Case 1: There is at least one $b \in \{0, 1\}$ for which y_b *fails* to satisfy

$$x = y^2 v^b \bmod n.$$

Since $b = 0$ and $b = 1$ each occur with probability $1/2$, this means that Bob's verification will fail with probability at least $1/2$, as desired.

(continued. . .)

Proof: case 2

Proof (continued).

Case 2: y_0 and y_1 both satisfy the verification equation, so $x = y_0^2 \bmod n$ and $x = y_1^2 v \bmod n$.

We can solve these equations for v^{-1} to get

$$v^{-1} \equiv y_1^2 x^{-1} \equiv y_1^2 y_0^{-2} \pmod{n}$$

But then $y_1 y_0^{-1} \bmod n$ is a square root of v^{-1}.

Since Mallory was able to compute both y_1 and y_0, then she was also able to compute a square root of v^{-1}, contradicting the assumption that she doesn't "know" a square root of v^{-1}. □

Successful cheating with probability $1/2$

We remark that it *is* possible for Mallory to cheat with success probability $1/2$.

- She guesses the bit b that Bob will send her in step 2 and generates a pair (x, y).
- If she guesses $b = 0$, then she chooses $x = r^2 \bmod n$ and $y = r \bmod n$, just as Alice would have done.
- If she guesses $b = 1$, then she chooses y arbitrarily and $x = y^2 v \bmod n$.

She proceeds to send x in step 1 and y in step 3.

The pair (x, y) is accepted by Bob if Mallory's guess of b turns out to be correct, which will happen with probability $1/2$.

Zero knowledge

We now consider the case of an honest Alice interacting with a dishonest Mallory pretending to be Bob, or simply a dishonest Bob who wants to capture Alice's secret.

Alice would like assurance that her secret is protected if she follows the protocol, regardless of what Mallory (or Bob) does.

Consider what Mallory knows at the end of the protocol.

Mallory sends $b = 0$

Suppose Mallory sends $b = 0$ in step 2.

Then she ends up with a pair (x, y), where y is a random number and x is its square modulo n.

Neither of these numbers depend in any way on Alice's secret s, so Mallory gets no direct information about s.

It's also of no conceivable use to Mallory in trying to find s by other means, for she can compute such pairs by herself whenever needed without involving Alice.

If having such pairs would allow her find a square root of v^{-1}, then she was already able to compute square roots, contrary to the assumption that finding square roots modulo n is difficult.

Mallory sends $b = 1$

Suppose Mallory sends $b = 1$ in step 2.

Now she ends up with the pair (x, y), where $x = r^2 \bmod n$ and $y = rs \bmod n$.

While y might seem to give information about s, observe that y itself is just a random element of $\mathbf{Z}_n$. This is because r is random, and the mapping $r \to rs \bmod n$ is one-to-one for all $s \in \mathbf{Z}_n^*$. Hence, as r ranges through all possible values, so does $y = rs \bmod n$.

Mallory learns nothing from x that she could not have computed herself knowing y, for $x = y^2 v \bmod n$.

Again, all she ends up with is a random number (y in this case) and a quadratic residue x that she can compute knowing y.

Mallory learns nothing from (x, y)

In both cases, Mallory ends up with information that she could have computed without interacting with Alice.

Hence, if she could have discovered Alice's secret by talking to Alice, then she could have also done so on her own, contradicting the hardness assumption for computing square roots.

This is the sense in which Alice's protocol releases zero knowledge about her secret.

Appendix

Proofs About Quadratic Residues

Proof that $|\sqrt{a}| = 2$ modulo an odd prime p

Let $a \in \mathrm{QR}_p$.

- It must have a square root $b \in \mathbf{Z}_p^*$.
- $(-b)^2 \equiv b^2 \equiv a \pmod{p}$, so $-b \in \sqrt{a}$.
- Moreover, $b \not\equiv -b \pmod{p}$ since $p \nmid 2b$, so $|\sqrt{a}| \geq 2$.
- Now suppose $c \in \sqrt{a}$. Then $c^2 \equiv a \equiv b^2 \pmod{p}$.
- Hence, $p \,|\, c^2 - b^2 = (c - b)(c + b)$.
- Since p is prime, then either $p \,|\, (c - b)$ or $p \,|\, (c + b)$ (or both).
- If $p \,|\, (c - b)$, then $c \equiv b \pmod{p}$.
- If $p \,|\, (c + b)$, then $c \equiv -b \pmod{p}$.
- Hence, $c \equiv \pm b \pmod{p}$, so $\sqrt{a} = \{b, -b\}$, and $|\sqrt{a}| = 2$.

Proof that half the elements of $\mathbf{Z}_p^*$ are in QR_p

- Each $b \in \mathbf{Z}_p^*$ is the square root of exactly one element of QR_p, namely, $b^2 \bmod p$.
- The mapping $b \mapsto b^2 \bmod p$ is a 2-to-1 mapping from $\mathbf{Z}_p^*$ to QR_p.
- Therefore, $|\mathrm{QR}_p| = \frac{1}{2}|\mathbf{Z}_p^*|$ as desired.

Chinese Remainder Theorem

Systems of congruence equations

Theorem (Chinese remainder theorem)

Let $n_1, n_2, \ldots, n_k$ be positive pairwise relatively-prime integers[3]*, let $n = \prod_{i=1}^{k} n_i$, and let $a_i \in \mathbf{Z}_{n_i}$ for $i = 1, \ldots, k$. Consider the system of congruence equations with unknown x:*

$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1) \\ x &\equiv a_2 \ (mod\ n_2) \\ &\vdots \\ x &\equiv a_k \ (mod\ n_k) \end{aligned} \tag{1}$$

(1) has a unique solution $x \in \mathbf{Z}_n$.

[3] This means that $\gcd(n_i, n_j) = 1$ for all $1 \le i < j \le k$.

How to solve congruence equations

To solve for x, let

$$N_i = n/n_i = \underbrace{n_1 n_2 \ldots n_{i-1}} \cdot \underbrace{n_{i+1} \ldots n_k},$$

and compute $M_i = N_i^{-1} \bmod n_i$, for $1 \leq i \leq k$. We compute N_i^{-1} by solving the congruence equation

$$M_i N_i \equiv 1 \pmod{n_i}. \tag{2}$$

The solution to (1) is

$$x = \left(\sum_{i=1}^{k} a_i M_i N_i \right) \bmod n \tag{3}$$

How to find modular inverses

To solve the congruence equation (2), we need to find integers M_i and u such that

$$M_i N_i - 1 = u n_i \tag{4}$$

i.e., n_i divides $M_i N_i - 1$.

Equation (4) has solutions over the integers iff $\gcd(N_i, n_i) = 1$.

Such linear equations over the integers are called *Diophantine equations*. They can be solved using the *Extended Euclidean Algorithm*.

Correctness

Lemma

$$M_j N_j \equiv \begin{cases} 1 \ (mod\ n_i) & if\ j = i; \\ 0 \ (mod\ n_i) & if\ j \neq i. \end{cases}$$

Proof.

$M_i N_i \equiv 1 \pmod{n_i}$ since $M_i = N_i^{-1} \bmod n_i$.
If $j \neq i$, then $M_j N_j \equiv 0 \pmod{n_i}$ since $n_i | N_j$. □

It follows from the lemma and the fact that $n_i \mid n$ that

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \equiv a_i \pmod{n_i} \qquad (5)$$

for all $1 \leq i \leq k$, establishing that (3) is a solution of (1).

Uniqueness

To see that the solution is unique in $\mathbf{Z}_n$, let $\chi : \mathbf{Z}_n \to \mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_k}$ be the mapping

$$x \mapsto (x \bmod n_1, \ldots, x \bmod n_k).$$

χ is a surjection[4] since $\chi(x) = (a_1, \ldots, a_k)$ iff x satisfies (1).

Since also $|\mathbf{Z}_n| = |\mathbf{Z}_{n_1} \times \ldots \times \mathbf{Z}_{n_k}|$, χ is a bijection, and there is only one solution to (1) in $\mathbf{Z}_n$.

[4] A *surjection* is an onto function.

An alternative proof of uniqueness

A less slick but more direct way of seeing uniqueness is to suppose that $x = u$ and $x = v$ are both solutions to (1).

Then $u \equiv v \pmod{n_i}$, so $n_i | (u - v)$ for all i.

By the pairwise relatively prime condition on the n_i, it follows that $n | (u - v)$, so $u \equiv v \pmod{n}$. Hence, the solution is unique in $\mathbf{Z}_n$.