

CPSC 367: Cryptography and Security

Michael J. Fischer

Lecture 19
April 4, 2019



Quadratic Residues, Squares, and Square Roots

Modular square roots

Square roots modulo n

Square roots modulo an odd prime p

Square roots modulo the product of two odd primes

Feige-Fiat-Shamir Authentication Protocol

Feige-Fiat-Shamir Authentication Protocol

Quadratic Residues, Squares, and Square Roots

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

Perfect squares over integers and \mathbf{Z}_n^*

Squares and square roots have several other cryptographic applications as well.

A *quadratic residue* is the analog in \mathbf{Z}_n^* of a perfect square over the integers.

In both cases, it is an element for which one or more square roots exist.

For example, 4 is a perfect square over the integers. It has two square roots, 2 and -2 .

Squares and square roots

An integer b is a *square root* of a modulo n if

$$b^2 \equiv a \pmod{n}.$$

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

Quadratic residues in \mathbf{Z}_n^*

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

$$b \in \mathbf{Z}_n^* \text{ iff } a \in \mathbf{Z}_n^*.$$

Why? Because

$$\gcd(b, n) = 1 \text{ iff } \gcd(a, n) = 1$$

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

$$p \mid b \text{ iff } p \mid a.$$

Assume that all quadratic residues and square roots are in \mathbf{Z}_n^* unless stated otherwise.

QR_n and QNR_n

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

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

$$\text{QNR}_n = \mathbf{Z}_n^* - \text{QR}_n.$$

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

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

For $a \in \text{QR}_n$, we sometimes write

$$\sqrt{a} = \{b \in \mathbf{Z}_n^* \mid b^2 \equiv a \pmod{n}\},$$

the *set of square roots* of a 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.

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

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

Quadratic residues modulo an odd prime p

Fact

For an odd prime p ,

- ▶ Every $a \in \text{QR}_p$ 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 $a \in \text{QR}_p$,

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

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

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

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

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

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

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 $a \in \text{QR}_n$ 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 $a \in \text{QR}_n$ then $|\sqrt{a}| = 4$, so

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

Proof sketch

- ▶ Let $a \in \text{QR}_n$. Then $a \in \text{QR}_p$ and $a \in \text{QR}_q$.
- ▶ There are numbers $b_p \in \text{QR}_p$ and $b_q \in \text{QR}_q$ such that
 - ▶ $\sqrt{a} \pmod{p} = \{\pm b_p\}$, and
 - ▶ $\sqrt{a} \pmod{q} = \{\pm b_q\}$.
- ▶ Each pair (x, y) with $x \in \{\pm b_p\}$ and $y \in \{\pm b_q\}$ can be combined to yield a distinct element $b_{x,y}$ in $\sqrt{a} \pmod{n}$.¹
- ▶ Hence, $|\sqrt{a}| = 4$, and $|\text{QR}_n| = \frac{1}{4}|\mathbf{Z}_n^*|$.

¹To find $b_{x,y}$ from x and y requires use of the Chinese Remainder theorem (see [Appendix](#)).

Feige-Fiat-Shamir Authentication Protocol

Feige-Fiat-Shamir protocol: preparation

The Feige-Fiat-Shamir protocol is based on the difficulty of computing square roots modulo composite numbers.

- ▶ Alice chooses $n = pq$, where p and q are distinct large primes.
- ▶ Next she picks a quadratic residue $v \in \text{QR}_n$ (which she can easily do by choosing a random element $u \in \mathbf{Z}_n^*$ and letting $v = u^2 \pmod n$).
- ▶ Finally, she chooses s to be the smallest square root of $v^{-1} \pmod n$.² She can do this since she knows the factorization of n .

She makes n and v public and keeps s private.

²Note that if v is a quadratic residue, then so is $v^{-1} \pmod n$.

A simplified one-round FFS protocol

Here's a simplified one-round version.

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

When both parties are honest, Bob accepts Alice because

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

This holds because

$$y^2 v^b \equiv (rs^b)^2 v^b \equiv r^2 (s^2 v)^b \equiv x (v^{-1} v)^b \equiv x \pmod{n}.$$

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

When both parties are honest, Bob's check

$$x = y^2 v^b \pmod{n}.$$

succeeds because

$$y^2 v^b \equiv (rs^b)^2 v^b \equiv r^2 (s^2 v)^b \equiv x (v^{-1} v)^b \equiv x \pmod{n}.$$

In a little more detail, we consider the two cases separately:

- ▶ $b = 0$: Then $y = r$ and $y^2 \equiv r^2 \equiv x \pmod{n}$.
- ▶ $b = 1$: Then $y \equiv rs \pmod{n}$ and $s^2 \equiv v^{-1} \pmod{n}$, so

$$y^2 v \equiv r^2 s^2 v \equiv r^2 v^{-1} v \equiv r^2 \equiv x \pmod{n}.$$

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

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 a value y_b to Bob.

We consider two cases.

(continued...)

Proof: case 1

Proof (continued).

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

$$x = y^2 v^b \pmod{n}.$$

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 $x = y_0^2 \pmod n$ and $x = y_1^2 v \pmod n$.

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 $y_1 y_0^{-1} \pmod n$ 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 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 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 $r \rightarrow rs \bmod n$ 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 $a \in \text{QR}_p$.

- ▶ 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, $p \mid c^2 - b^2 = (c - b)(c + b)$.
- ▶ Since p is prime, then either $p \mid (c - b)$ or $p \mid (c + b)$ (or both).
- ▶ If $p \mid (c - b)$, then $c \equiv b \pmod{p}$.
- ▶ If $p \mid (c + b)$, 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, $|\text{QR}_p| = \frac{1}{2}|\mathbf{Z}_p^*|$ as desired.

Chinese Remainder Theorem

Systems of congruence equations

Theorem (Chinese remainder theorem)

Let n_1, n_2, \dots, n_k be positive pairwise relatively-prime integers³, let $n = \prod_{i=1}^k n_i$, and let $a_i \in \mathbf{Z}_{n_i}$ for $i = 1, \dots, k$. Consider the system of congruence equations with unknown x :

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

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

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

How to solve congruence equations

To solve for x , let

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

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

$$M_i N_i \equiv 1 \pmod{n_i}. \quad (2)$$

The solution to (1) is

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

How to find modular inverses

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

$$M_i N_i - 1 = u n_i \quad (4)$$

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

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

Proof.

$M_i N_i \equiv 1 \pmod{n_i}$ since $M_i = N_i^{-1} \pmod{n_i}$.

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 $n_i | n$ that

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

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 $\chi : \mathbf{Z}_n \rightarrow \mathbf{Z}_{n_1} \times \dots \times \mathbf{Z}_{n_k}$ be the mapping

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

χ is a surjection⁴ since $\chi(x) = (a_1, \dots, a_k)$ iff x satisfies (1).

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

⁴A *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 .