Zero-Knowledge Proofs

Slides from a Talk

by Eric Postpischil

Zero-Knowledge Proofs

Goals

Alice wants to prove to Bob that she knows an identifying number *X*.

Bob should not be able to figure out *X*.

Dave observes all communications between Alice and Bob but should not be able to fake the proof to Bob.

Application

Alice is your smart card. Bob is your bank's computer. Dave is a merchant's terminal.

You put Alice into Dave at the store, and Alice proves to Bob that she is your smart card.

Bob authorizes the transaction, telling Dave your purchase is approved and bank will pay.

Dishonest Dave can't forge card later even if Dave records all messages.

Definitions

In this talk, “number” means non-negative integer: 0, 1, 2, 3,…

“Iff” stands for “if and only if.”

A number *f* is a factor of *n* iff *n* is an integer multiple of *f*.

A number *p* is a prime number iff *p* has exactly two factors (which must be 1 and *p*).

The remainder when *m* is divided by *n* is written *m* % *n*.

We will pick a number *n* and from then on consider any number *m* to be the same number as *m* % *n*.

- Sometimes I will still write *m* % *n* when it is important that *m* itself not be used (to hide information).

Open the Bank Account

Alice chooses two very large prime numbers, *p* and *q*.

Alice multiplies *p* and *q* to make *n*.

Alice picks a very large number *X*. *X* represents Alice's password for the bank account.

(*X* is smaller than *n*, so *X* equals *X* % *n*.)

Alice calculates X^2 % *n*.

Alice tells Bob (the bank's computer) *n* and X^2 % *n*.

After the account is open, Alice can go shopping.

Zero-Knowledge Proofs

Premises

If n is the product of two very large prime numbers, p and q, it is believed to be very difficult to find p or q if you only know n.

- This has not been proven, but many smart people have tried and failed to find fast ways to find p and q from n.

If you know $X^2 \% n$ and n but not p or q, finding X is about as difficult as finding p or q. Therefore, telling somebody $X^2 \% n$ does not reveal X.

- This can be proven because the ability to find X can be used to find p and q.

“Very large” means numbers with several hundred digits. At this size, computers can do all the arithmetic for zero-knowledge proofs very quickly. But we have no way for computers to find p and q in less than many years.

Alice Proves She Knows *X*

Alice's personal identification number is *X*. Bob doesn't know *X* but has been told $X^2 \% n$.

1. Alice makes up a random number *R* and sends Bob the number $X^2R^2 \% n$.

2. Bob randomly sends one of two messages:

- "Send me *R*."
- "Send me $XR \% n$."

3. Since Alice knows both *X* and *R*, she can easily satisfy both of these requests.

4. Bob checks Alice's answer (see next page):

- If Bob asked for *R*, Bob squares it and multiplies by X^2 to check that it matches the $X^2R^2 \% n$ Alice sent in the first message.
- If Bob asked for $XR \% n$, Bob squares it to check that it matches the $X^2R^2 \% n$ Alice sent in the first message.

Bob Checks Alice's Answer

1. Bob asks for R.

- Alice sends $X^2R^2 \% n$.
- Bob sends "Send me R."
- Alice sends R.
- Bob squares R to make R^2.
- Bob multiplies by $X^2 \% n$ and takes remainder to find $X^2R^2 \% n$.

2. Bob asks for $XR \% n$.

- Alice sends $X^2R^2 \% n$.
- Bob sends "Send me $XR \% n$."
- Alice sends $XR \% n$.
- Bob squares $XR \% n$ and takes the remainder to find $X^2R^2 \% n$.

Why Bob Believes Alice Knows *X*

Bob requests either *R* or *XR* % *n*. Since Alice has both answers, she can always give whichever one is requested. Later, we will show this proves she knows *X*.

Dave might know one answer (as we will consider later) but not both. If Dave pretends to be Alice and tries to fool Bob, there is a 50-50 chance Dave will be caught.

Bob can repeat the procedure, requiring different values of *R* each time. If Bob repeats the procedure 30 times, there is only one chance in 2^{30} (1,073,741,824) that Dave would pass all 30 times.

So Bob is convinced the other party knows both *R* and *XR* % *n*, and, as we will see, this convinces Bob the other party knows *X*.

Dave Cannot Fool Bob

Dave can try to fool Bob in two ways:

- Dave can make up a random number P and send P^2.
- Dave can make up a random number R and send X^2R^2. (Dave knows X^2 from listening to Alice and Bob previously.)

In the first case, Dave is pretending that P^2 is X^2R^2.

- If Bob asks for XR % n, Dave can send P, and it will pass Bob's test.
- But if Bob asks for R, Dave is caught. Dave has no way to calculate an R that matches.

In the second case, Dave really sends X^2R^2.

- If Bob asks for R, Dave can send R.
- If Bob asks for XR % n, Dave is caught.

Dave Does Not Learn

Dave could tap Alice and Bob's communications and learn both R and X^2R^2 for many values of R and also both XR % n and X^2R^2 for many other values of R.

But a pair R and X^2R^2 does not give any new information, since R is just a random number and X^2R^2 is public information, so anybody can make up pairs R and X^2R^2.

The pair XR % n and X^2R^2 contains XR % n, but, since nobody but Alice knows R, this cannot be used to find X.

XR % n without R contains no information about the value of X.

- This is because any value of XR could be the result of any possible value of X with some value of R.

Finding *X* from *R* and *XR* % *n*

Knowing *R* and *XR* % *n* proves you know *X*.

Write two equations:

$$n = 1 \cdot n + 0 \cdot R.$$
$$R = 0 \cdot n + 1 \cdot R.$$

Repeat this algorithm:

- Divide the bottom two numbers on the left sides (*n* and *R* to start) and take only the integer part of the quotient.
- Multiply the entire bottom equation by the quotient.
- Subtract from the equation above.
- Write the resulting new equation below.
- Stop when the left side is 1.
- Take the coefficient of *R* in the last equation and call it *m*.
- *X* is *mXR* % *n*.

Example

n is 143. *R* is 28. *XR* % *n* is 17. What is *X*?

$$143 = 1 \cdot 143 + 0 \cdot 28$$
$$28 = 0 \cdot 143 + 1 \cdot 28 \quad \text{floor}(143/28) = 5$$
$$3 = 1 \cdot 143 + -5 \cdot 28 \quad \text{floor}(28/3) = 9$$
$$1 = 9 \cdot 143 + 46 \cdot 28$$

m is 46.

mXR is 46·17, which is 782.

Find *mXR* % *n*: 782 divided by 143 is 5 with a remainder of 67.

X is 67.

Check:

$$XR = 67 \cdot 28 = 1876.$$

$$XR \,\%\, n = 1876 \,\%\, 143 = 17.$$

Summary

Alice proves she knows *X* indirectly by proving she knows both a random number *R* and its product with *X*, *XR*.

Only somebody who knows *X* can always provide both *R* and *XR* on demand.

Bob tests Alice's claim by randomly checking one of *R* or *XR*, never both.

Revealing *R* or *XR* but not both reveals no information about *X*.

A lucky forger can pass Bob's tests. The probability of this can be made as low as the chance of guessing *X*.