WE THE MILLIONAIRES

A Cryptographic Protocol

Joseph Johnston

December 16, 2018

Prerequisite: An Encryption Scheme

Key Distribution

Our encryption scheme will require a private key K. This key needs to be split between multiple parties (the two millionaires). An encrypted value can only be decrypted if all parties (both millionaires) agree to decrypt it.

There are different ways to distribute a key among multiple parties. Other papers show how.

Homomorphic Encryption

We will need an **additively homomorphic** encryption scheme. This means, for plaintexts $x1, x2$:

$$E(x1 + x2) = E(x1)E(x2)$$

which implies

$$E(x1 - x2) = E(x1)/E(x2)$$

$$E(k * x1) = E(x1)^k$$

for any integer k. We will modify ElGamal Encryption to make it satisfy these properties.

ElGamal Encryption

Choose 2 large primes where $p - 1 = 2q$. Both $\mathbb{Z}_p$ and $\mathbb{Z}_q$ are groups. Choose a generater g of $\mathbb{Z}_q$. All operations will be modulo p.

Private (distributed) key is random $K \in \mathbb{Z}_q$. Public key is (p, g, g^K).

To encrypt plaintext x, choose random $k_x \in \mathbb{Z}_q$ and compute the pair: $E(x) = \left(g^{k_x}, g^x (g^K)^{k_x}\right)$

To decrypt $E(x)$, divide the right by the left raised to private key K, then (if possible) solve the logarithm for x.

$$\left(g^x (g^K)^{k_x}\right) \Big/ \left(g^{k_x}\right)^K = g^x$$

Solving the Logarithm

For our millionaires problem, we will only need to know if an encrypted value is 0 or not. This makes solving the logarithm easy because

$$x = 0 \implies g^x = 1$$
$$x \neq 0 \implies g^x \neq 1$$

So checking for 1 is enough.

In this presentation, we will thus assume it is straightforward to test whether an encrypted value is 0, given the private key.

The Formula

Scenario

Millionaire 1 and Millionaire 2 encode their wealth as bit lists representing the binary numbers $M1$ and $M2$.

$$M1 = (M1_1, \ldots, M1_n)$$
$$M2 = (M2_1, \ldots, M2_n)$$

The protocol will test whether $M1 > M2$ by comparing these bits in encrypted form.

The Boolean Formula

Testing whether $M1 > M2$ will be done by evaluating an (encrypted) boolean formula, which is basically:

$M1$ is greater than $M2$ by the 1st bit.

OR

$M1$ is greater than $M2$ by the 2nd bit.

OR

...

OR

$M1$ is greater than $M2$ by the last bit.

So if the formula is true then Millionaire 1 is richer than Millionaire 2.

... More Precisely

Define the boolean sub-formula

$$
\begin{aligned}
TERM(m) = & \\
& M1_1 = M2_1 \\
& \text{AND } M1_2 = M2_2 \\
& \cdots \\
& \text{AND } M1_{m-1} = M2_{m-1} \\
& \text{AND } M1_m = 1 \\
& \text{AND } M2_m = 0
\end{aligned}
$$

The formula needs to determine if **any** *TERM* is true, thus

$$FORMULA = TERM(1) \text{ OR } TERM(2) \text{ OR } \ldots \text{ OR } TERM(n)$$

Encrypting the Formula

Encrypting Constraints

For each $TERM(m), m = [n]$, we need to encrypt the constraints.

$$
\begin{aligned}
& M1_i = M2_i \\
& \quad \implies S_{m,i} = M1_i - M2_i = 0 \\
& \quad \implies E(S_{m,i}) = E(M1_i)/E(M2_i) = E(0) \\
& M1_m = 1, M2_m = 0 \\
& \quad \implies S_{m,m} = M1_m - M2_m - 1 = 0 \\
& \quad \implies E(S_{m,m}) = E(M1_m)/(E(M2_m)E(1)) = E(0)
\end{aligned}
$$

So $TERM(m)$ is true iff

$$S_{m,i} = 0 \implies E(S_{m,i}) = E(0) \text{ for } i = [m]$$

Testing for $S_{m,i} = 0$

Theorem (sub-case of Schwartz-Zippel Lemma)

Suppose f is a non-zero linear function of v variables over a field $\mathbb{F}$ of size $|\mathbb{F}|$. Then the probability $f(r_1, \ldots, r_v) = 0$ for random $r_1, \ldots, r_v$ is $1/|\mathbb{F}|$.

To test if $S_{m,i} = 0$ for all $i = [m]$, consider the linear function

$$f(t_1, \ldots, t_m) = S_{m,1}t_1 + \cdots + S_{m,m}t_m$$

We use the field $\mathbb{F} = \mathbb{Z}_p$ with $|\mathbb{F}| = p$ because we are using ElGamal encryption. With high probability, $P(r_1, \ldots, r_m) = 0$ for random $r_1, \ldots, r_m$ iff $S_{m,i} = 0$ for all $i = [m]$.

Evaluating E(P)

The two millionaires agree on random input $r_1, \ldots, r_n$. Then for each $m = [n]$ they each evaluate $f(r_1, \ldots, r_m)$ in encrypted form by computing

$$C_m = E(f(r_1, \ldots, r_m)) = E(S_{m,1})^{r_1} E(S_{m,2})^{r_2} \ldots E(S_{m,m})^{r_m}$$

If $f(r_1, \ldots, r_m) = 0$ for some $m = m'$, then we have $C_{m'} = E(f(r_1, \ldots, r_{m'})) = E(0)$. In this case $TERM(m')$ is true.

Testing for Zeros

Testing for E(0)

Suppose C_m encrypts the value V_m. Now the millionaires must check if the list $(C_1, \ldots, C_n) = (E(V_1), \ldots, E(V_n))$ contains **any** $E(0)$, to see if **any** *TERM*s are true.

But they cannot reveal which $C_m = E(0)$, if any, because

...that reveals which $TERM(m)$ is true

...which reveals which of $M1$'s bits is greater than $M2$'s bits

...which reveals approximately $M1 - M2$

...which reveals approximately the other millionaire's wealth.

The Zero Test

Let us reconsider the list as a set instead

$$\{C_1, \ldots, C_n\} = \{E(V_1), \ldots, E(V_n)\}$$

Millionaire 1 multiplies each encrypted value by a secret, random value u_m, by computing

$$\{C_1^{u_1}, \ldots, C_n^{u_n}\} = \{E(u_1 V_1), \ldots, E(u_n V_n)\}$$

Then millionaire 1 randomly shuffles the set and sends it to millionaire 2. Millionaire 2 does the same with the new set. Using secret, random values w_m, millionaire 2 computes

$$\{(C_1^{u_1})^{w_1}, \ldots, (C_n^{u_n})^{w_n}\} = \{E(w_1 u_1 V_1), \ldots, E(w_n u_n V_n)\}$$

Then millionaire 2 randomly shuffles the set and sends it back to millionaire 1.

Finding the Answer

Now both millionaires have the same new set of encrypted values.

If any of the initial encrypted values V_m equal 0, then $E(w_m u_m V_m) = E(w_m u_m * 0) = E(0)$. Thus checking whether the initial list

$$(C_1, \ldots, C_n) = (E(V_1), \ldots, E(V_n))$$

contains $E(0)$ can be done by checking whether the new set

$$\{E(w_1 u_1 V_1), \ldots, E(w_n u_n V_n)\}$$

contains $E(0)$. If both millionaires agree to use the private key for this purpose, it can be done, and the problem is solved.

Example

Encrypt Wealth

Millionaire 1:

$$M1 = 496$$
$$M1 = (M1_1, M1_2, ...M1_L)$$
$$M1 = (1, 1, 1, 1, 1, 0, 0, 0, 0)$$

Millionaire 2:

$$M2 = 368$$
$$M2 = (M2_1, M2_2, ...M2_L)$$
$$M2 = (1, 0, 1, 1, 1, 0, 0, 0, 0)$$

Bits should be encrypted For simplicity kept $0, 1$

Choose Random Numbers

Let $T = 9$ ($2^9 = 512$)

Millionaires randomly choose t_i from $\{0, 1, 2, .., 511\}$

Millionaire 1: $t_{i,1} = \{3, 45, 200, 456, 12, 503, 7, 12, 13\}$

Millionaire 2: $t_{i,2} = \{447, 177, 50, 435, 14, 472, 283, 414, 136\}$

$t_i = t_{i,1} + t_{i,2} \mod 512$

$t_i = \{450, 222, 250, 379, 26, 463, 290, 426, 149\}$

Complex Zero Test

Check if any value is 0, if that is the case, output 0 else 1

Recall:

$t_i = \{450, 222, 250, 379, 26, 463, 290, 426, 149\}$

Millionaire 1: $M1 = (1, 1, 1, 1, 1, 0, 0, 0, 0)$

Millionaire 2: $M2 = (1, 0, 1, 1, 1, 0, 0, 0, 0)$

$$ZM = (M1_1 > M2_1), (M1_1 = M2_1)^{t_1} * (M1_2 > M2_2)^{t_2}, \ldots$$

$$ZM = 1, (1 = 1) * (1 > 0), \ldots$$

$$ZM = 1, 0, \ldots$$

Contains at least one 0, therefore M1>M2

Questions?