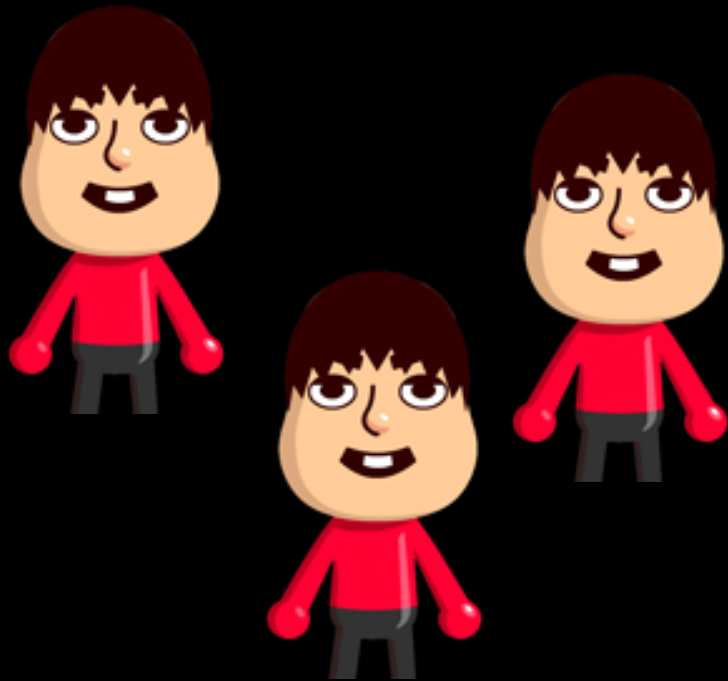


15-396

Science of teh Interwebs

Identity and Privacy 2

Lecture 6 (September 15, 2011)



Average Salary

50k



62k



How can these guys calculate their average salary without telling each other what their salaries are?

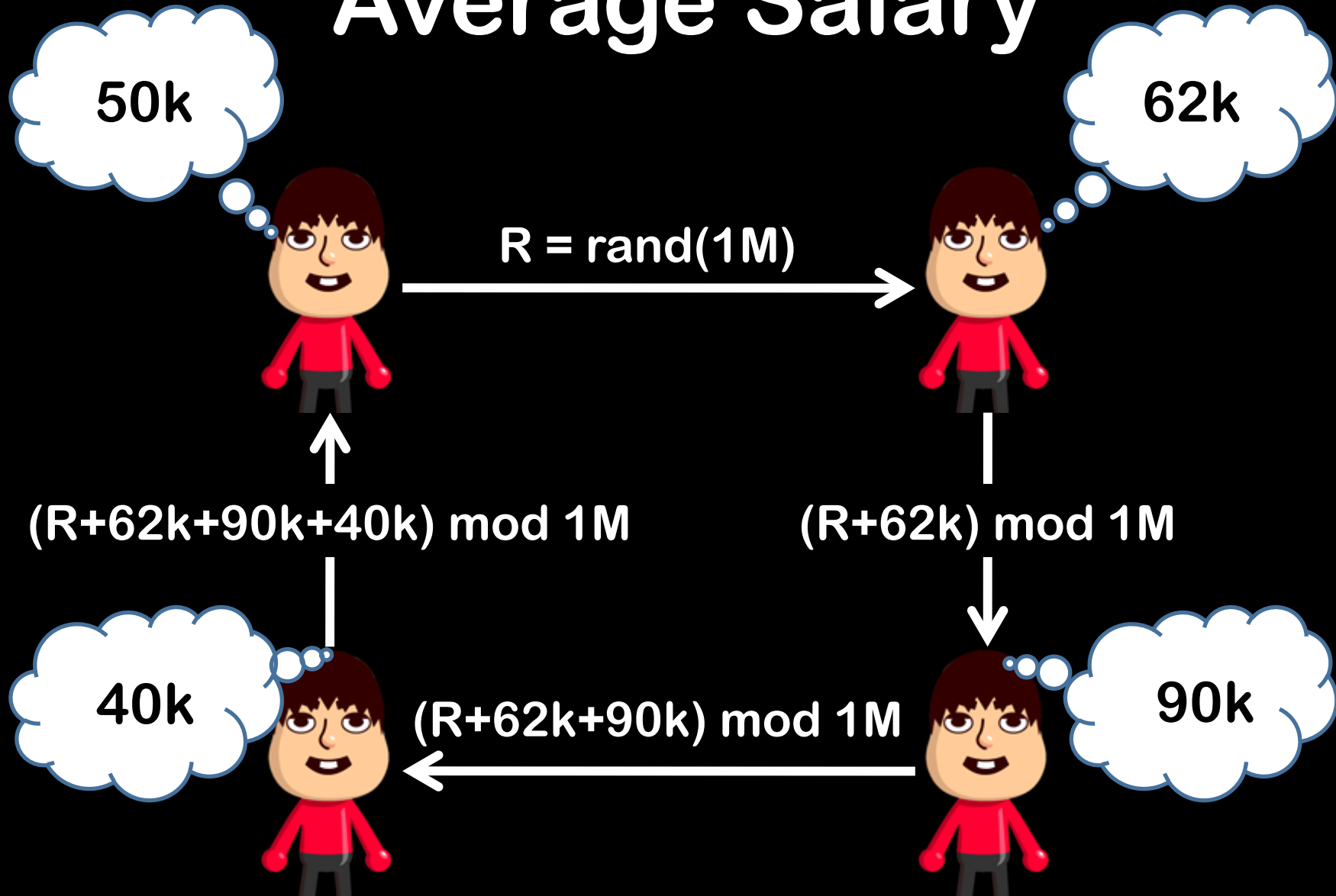
40k



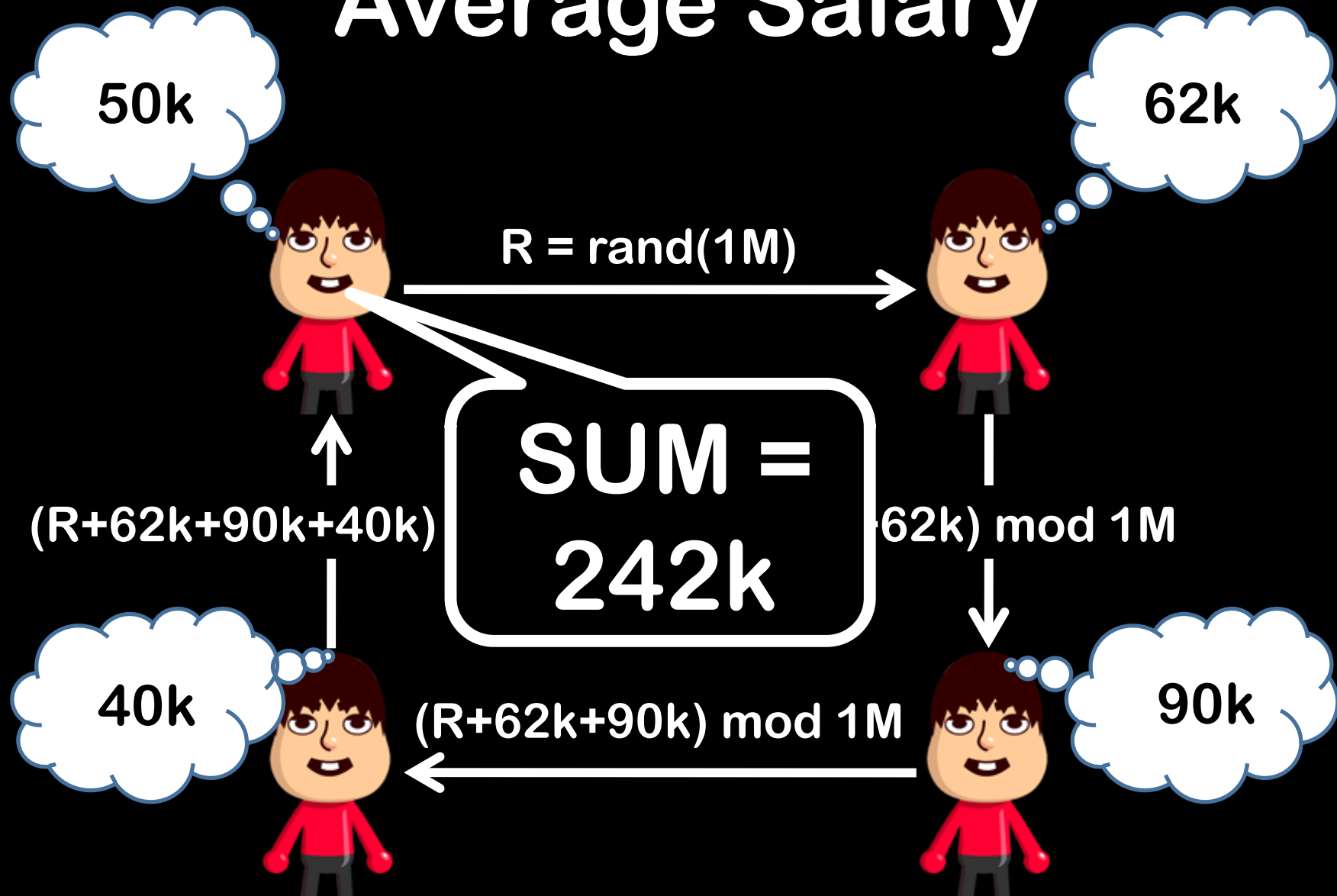
90k



Average Salary



Average Salary

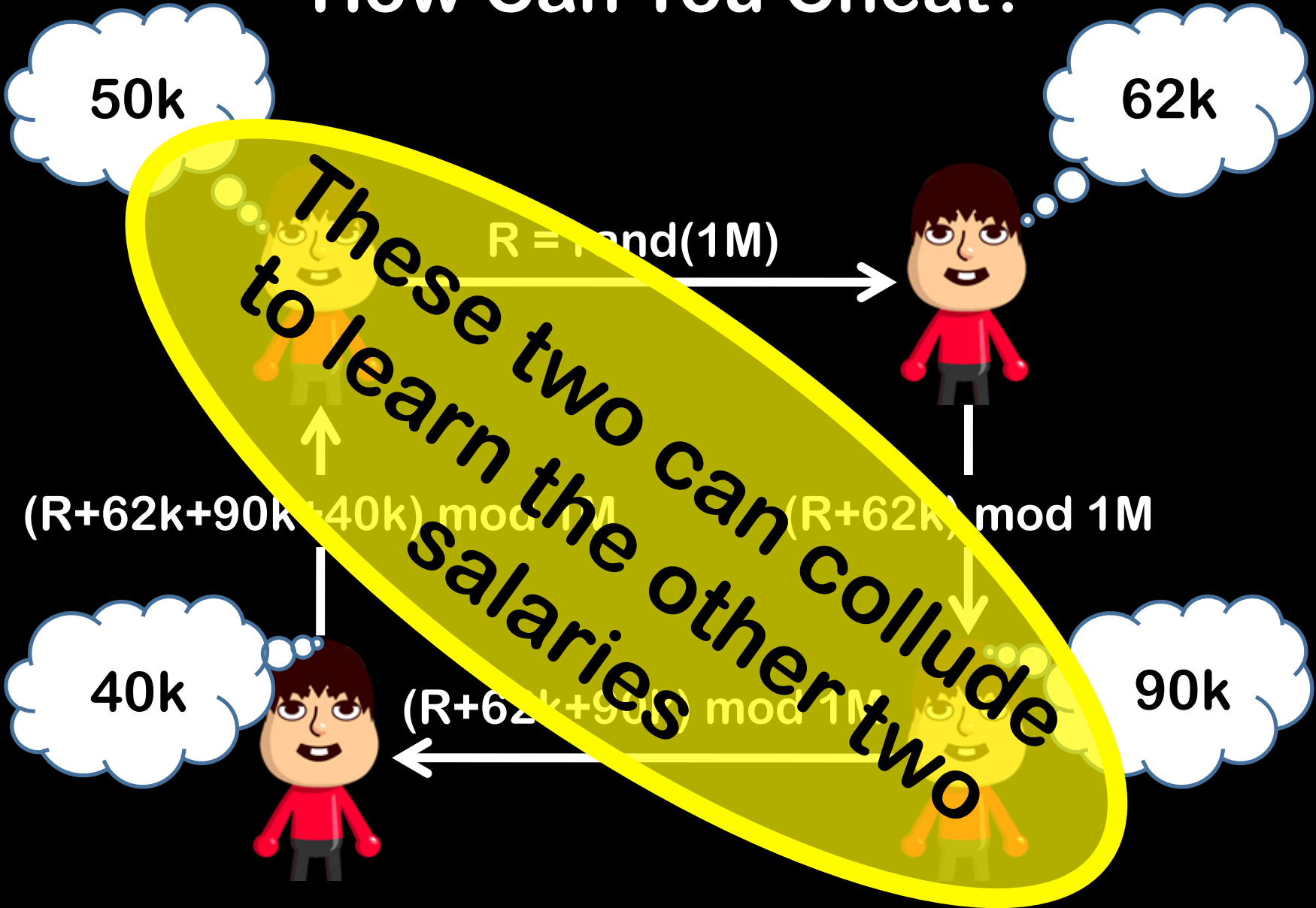


How many messages required
with N participants?

$O(N)$

The guarantee is that (as long as all parties follow the protocol) nobody learns anything other than what can be learned from the sum of the secret salaries

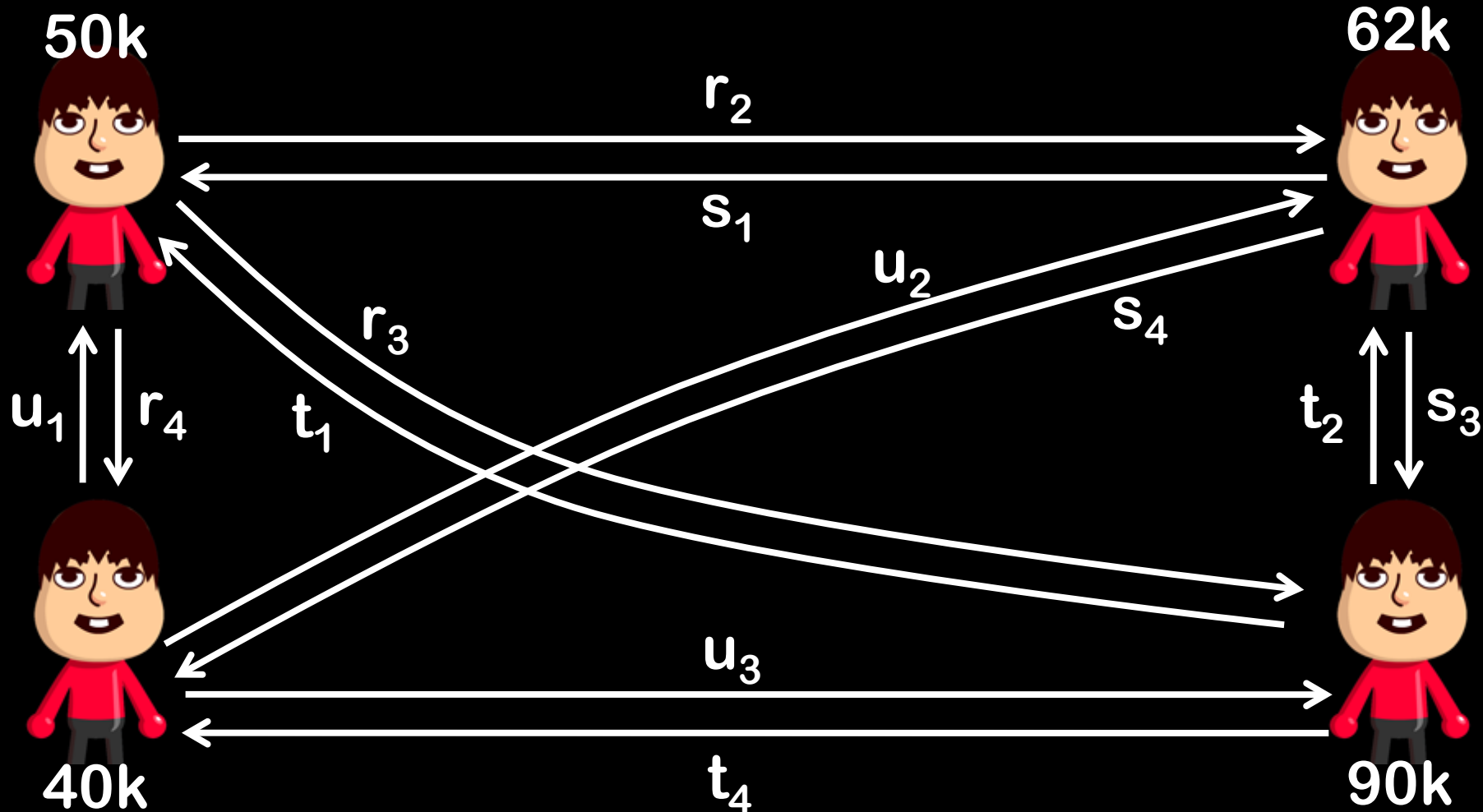
How Can You Cheat?



A More Secure Protocol

Pick random r_1, r_2, r_3 (mod 1M)
Set $r_1+r_2+r_3+r_4 = 50k$ (mod 1M)

Pick random s_1, s_2, s_3 (mod 1M)
Set $s_1+s_2+s_3+s_4 = 62k$ (mod 1M)



Pick random u_1, u_2, u_3 (mod 1M)
Set $u_1+u_2+u_3+u_4 = 40k$ (mod 1M)

Pick random t_1, t_2, t_3 (mod 1M)
Set $t_1+t_2+t_3+t_4 = 90k$ (mod 1M)

Pick random $r_1, r_2, r_3 \pmod{1M}$
Set $r_1+r_2+r_3+r_4 = 50k \pmod{1M}$

50k



$$r_1+s_1+t_1+u_1 \pmod{1M}$$



Pick random $s_1, s_2, s_3 \pmod{1M}$
Set $s_1+s_2+s_3+s_4 = 62k \pmod{1M}$

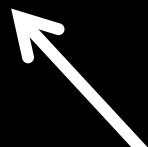
62k



$$r_2+s_2+t_2+u_2 \pmod{1M}$$



+



$$r_4+s_4+t_4+u_4 \pmod{1M}$$



40k

Pick random $u_1, u_2, u_3 \pmod{1M}$
Set $u_1+u_2+u_3+u_4 = 40k \pmod{1M}$

$$r_3+s_3+t_3+u_3 \pmod{1M}$$



90k

Pick random $t_1, t_2, t_3 \pmod{1M}$
Set $t_1+t_2+t_3+t_4 = 90k \pmod{1M}$

How many messages required
with N participants?

$O(N^2)$

**How do you do anonymous
communication?**

Anonymous Communication

$(0, \dots, 0, M_1, 0, \dots, 0)$



$(0, M_2, 0, \dots, 0)$



The sum equals:

$(0, \dots, M_1, \dots, M_2, \dots, M_3, \dots, M_4, \dots, 0)$



$(0, 0, \dots, M_4, \dots, 0)$



$(M_3, 0, \dots, 0)$

**How do you identify
yourself to a Website?**

Reuse of Passwords

27% of username/passwords on
espgame.org matched username/
passwords from either Yahoo! or
Hotmail

Untrusted Terminal

How do you know the cluster machine is not running a key logger?



http://205.188.226.153/sohal201/myspace.com

Help

myspace.com
a place for friends

The Web MySpace Search Help | SignUp

You Must Be Logged-In to do That!

MySpace is FREE, But Feature

<http://123.456.789.012/sohal201/myspace.com>

Your session has expired. Please re-login.

Member Login

E-Mail :

Password :

Forgot your password?

Remember Me

Your session has expired!

Your session has expired. Please re-login.

Member Login

E-Mail :

Password :

Forgot your password?

Remember Me

Not a MySpace Member? Join FREE!

After You Sign Up You Can:

- Create Free Profiles on MySpace
- Upload Pictures & Write Blogs
- Use MySpace Mail & Instant Messenger

[About](#) | [FAQ](#) | [Terms](#) | [Privacy](#) | [Safety Tips](#) | [Contact MySpace](#) | [Promote!](#) | [Advertise](#) | [MySpace International](#)

©2003-2006 MySpace.com. All Rights Reserved.

Here's How SiteKey Works

By passing back and forth secret information that only you and Bank of America know, you can feel even more secure with your Online Banking experience. We recognize you and you recognize us.



1 Enter your Online ID.

2 Click **Sign In using my SiteKey**.

Your SiteKey Image and Message:



cute dog

3 **If we recognize your computer:**
We will show you your secret SiteKey. If you are vision-impaired, you can recognize your SiteKey by its specific name and message.

What was your high school mascot?

* Answer:

4 **If we don't recognize your computer:**
We will ask you one of your secret SiteKey Confirmation Questions.
After you answer your question correctly, we will show you your SiteKey.

Passcode:

5 Once you view your valid SiteKey, you can then safely enter your Passcode and continue onto your Online Banking account.

Biometrics

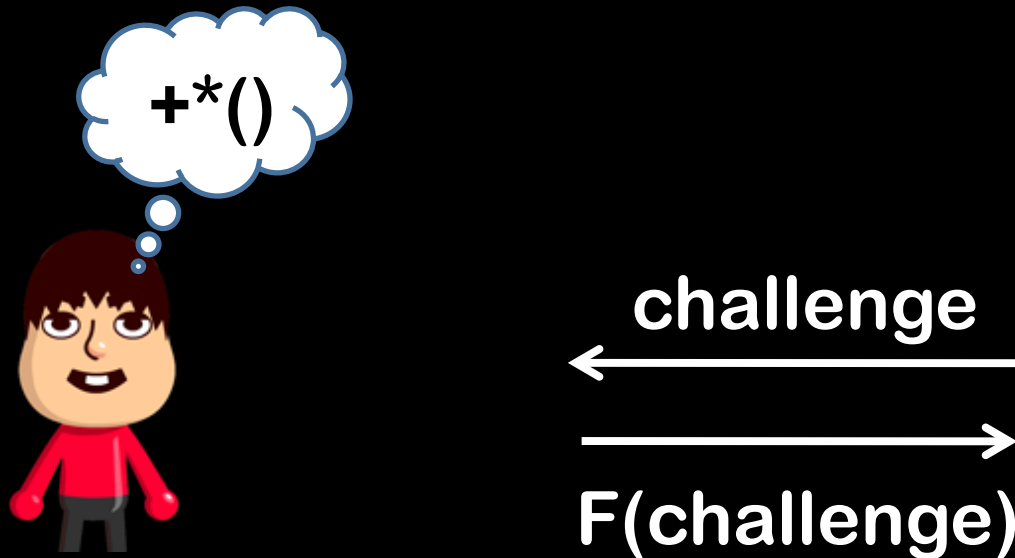
Expensive

Nobody knows how secure they really are

Not revocable

Every time you touch something, you
leave your fingerprint there

Research Question: Human Doable Challenge-Response System



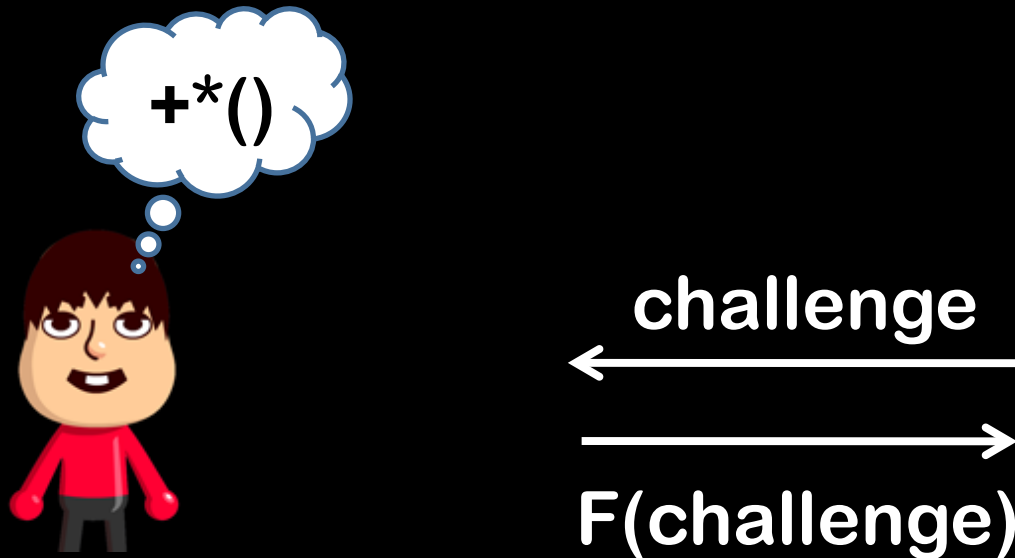
If somebody sees N pairs $(Y, F(Y))$, they still cannot compute $F(X)$ for some X they haven't seen

Failed Example

$$F(X) = 3X + 2X^2$$

After you see $(X, F(X))$ for two different values of X , you can learn the secret function

Research Question: Human Doable Challenge-Response System



If somebody sees N pairs $(Y, F(Y))$, they still cannot compute $F(X)$ for some X they haven't seen

g2g

ttyl