Christmas Lectures 2008

Zero-knowledge games

Security is very important on the internet. You often need to prove to another person that you know something but without letting them know what the information actually is (because they could just copy and use it). For example, you might need to convince an online music shop that you know your password for their website without sending them the password itself.

These are called 'zero-knowledge' methods, because you can get an answer without ever finding out anything new about the important information. Here we provide two zero-knowledge games you can try with your friends at home or school. The first is one way of finding out if two people agree on a decision without either of them revealing what they actually decided! The second lets you work out the total of all your ages, without everyone finding out how old anyone else is.

THE DECISION GAME

Let's suppose that you and a friend have to make a 'yes' or 'no' joint decision, but you don't want the other person to know what you thought. For example, you both need to decide whether to go on holiday together, and you don't want to hurt their feelings if you don't want to go but they do. How do you know if you agree or not without knowing what both your answers are? By playing the decision game, that's how!

The Royal Institution of Great Britain
Microsoft Research
FIVE

What to do

A set of three 'Yes' cards and two 'No' cards are shown below. Print the page with them on and cut out the cards (or draw your own). Now, follow the steps below.

1. Each of the two people needing to make a decision takes one 'Yes' and one 'No' card, with the third 'Yes' left over.
2. Say the question out loud so that you both know exactly what you're answering.
3. The first person puts their decision cards face down on the table, with their decision **on top**.
4. Now place the spare 'Yes' card face down on top of the pile.
5. The second person puts their decision cards face down on top of the pile, with their decision as the one **underneath**.
6. Next, the pile of cards is 'cut' (split at a random place and the top cards put on the bottom). Cut the deck as many times as you like until you are both sure that your cards are secret. Now neither person has seen the other's cards or the order they were put on the pile.
7. Turn the pile over and spread out the cards in a line, face up so you can both see them.
8. If all three of the 'Yes' cards are next to each other, then you both decided 'Yes'. Because the pile was cut, the cards wrap around and it is still a yes result even if the 'Yes' cards are on the edges. If the three 'Yes' cards are separated by 'No' cards then one or the other, or both of you, decided 'No'. The beauty of the decision game is that the players never know who said 'No', so no one has to feel embarrassed or hurt!

					Result
NO	NO	YES	YES	YES	Yes
YES	YES	NO	NO	YES	Yes
YES	NO	YES	NO	YES	No

Christmas Lectures 2008

Zero-knowledge games

NO

NO

YES

YES

YES

Zero-knowledge games

SECRET AGES

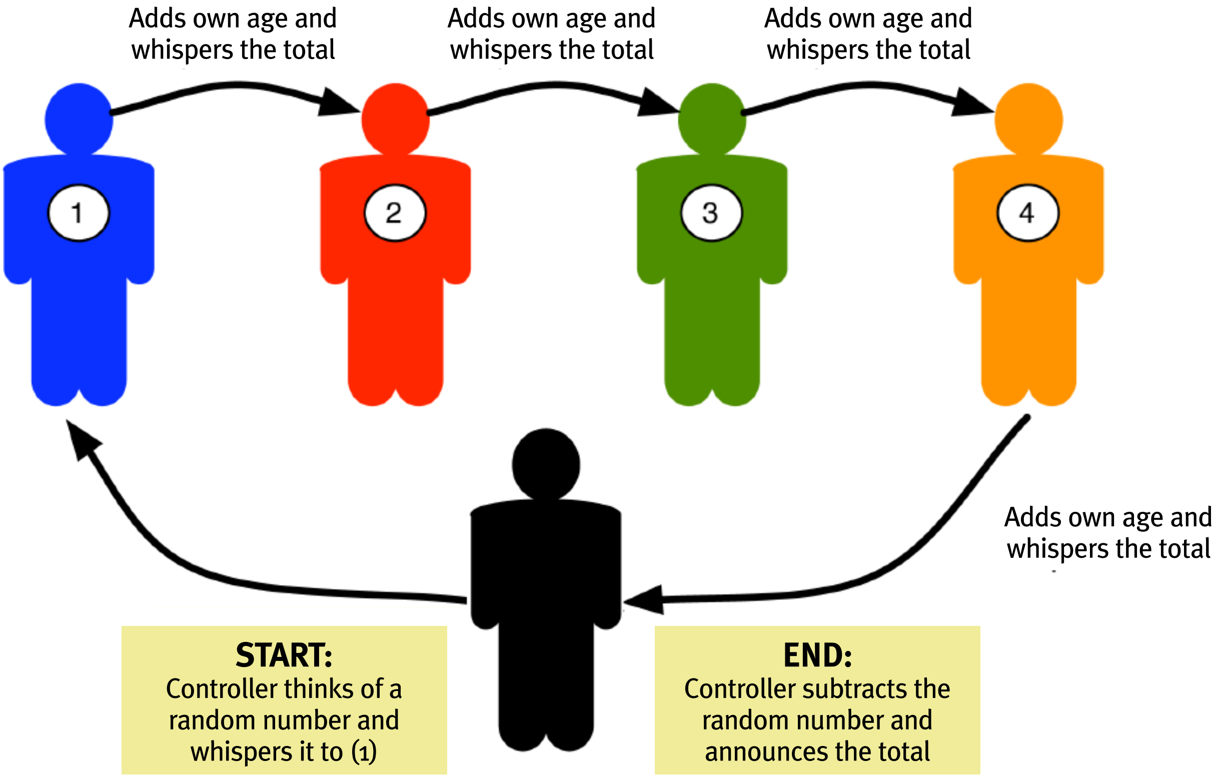
This is a zero-knowledge game for adding up people's ages without them ever finding out what anyone else's age actually is. You just need to find out the total for everyone. We use age, but the game works with any number that individuals might want to keep secret. Instead of ages, you could try this with the number of pairs of shoes you own or how many biscuits you've eaten today.

You can do this with any number of your friends, but this example involves four people.

What to do

1. The four people with secret ages stand side by side in a line facing the fifth person, the 'controller' (your teacher or another friend).
2. The controller thinks of a number between 1 and 100 and whispers it in the ear of the first person in the line.
3. The first person adds their age to the number, then whispers the total to the second person.
4. The second person adds their age and whispers the total to the third person, who then does the same to the fourth.
5. The fourth person whispers the grand total to the controller. The controller then takes away the original number and announces to everyone what the grand total is.

Zero-knowledge games


Adds own age and whispers the total
Adds own age and whispers the total
Adds own age and whispers the total
1
2
3
4
Adds own age and whispers the total

START:
Controller thinks of a random number and whispers it to (1)

END:
Controller subtracts the random number and announces the total

In this way, important information has been found out about the whole group without anyone having to reveal their secret!

This zero-knowledge method is not very *secure*. It is possible for people to cheat and work out some of the supposedly secret information. How do you think this could happen? Which people could get together after the game has finished and work out secret information about the other players?

Zero-knowledge games

SECRET AGES – ADVANCED

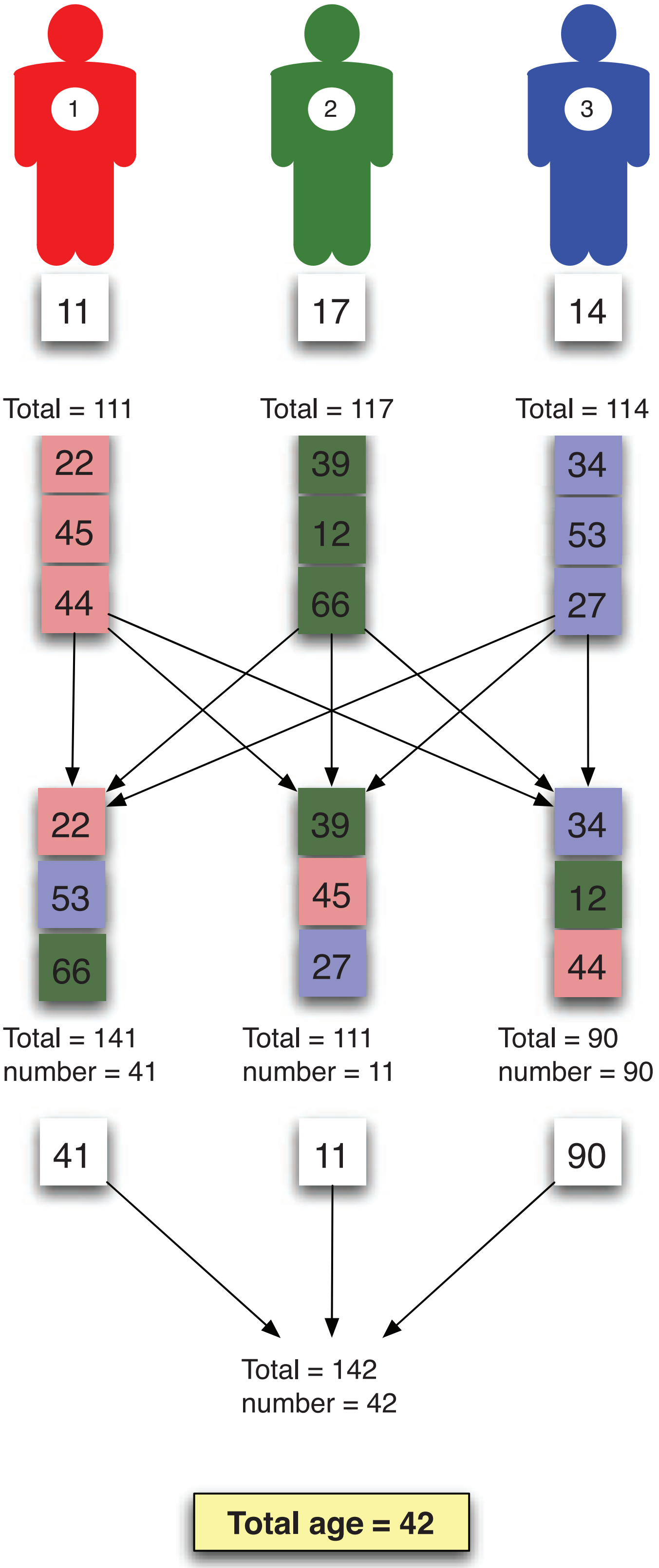
If you’ve worked out how to cheat at the zero-knowledge system, can you design a more secure system? The method shown in the diagram below is a little more complicated, but it is secure against cheats. Try it out with your friends!

- You need three friends who don’t know each other’s ages, and a calculator.
- Each player adds their age to 100, then divides the total into three random numbers (for example, age 11, 111 = 22 + 45 + 44).
- The random numbers are ‘shares’, which each player writes down onto three pieces of paper.
- Each player keeps one share for themselves and gives the other two players one of the other shares.
- Each player ends up with three shares, which, using the calculator, they re-total then divide by 100. They then keep the two digits after the decimal point. (If there’s only one digit after the decimal point put a zero after it, for example 0.9 gives you 90).
- All players reveal the resulting number to the others.
- The players add the three numbers together and divide by 100 as before (adding a zero if necessary).
- The two digits after the decimal point give you the sum of all three people’s ages.

Diagram based on ‘How to keep secrets safe’, *Scientific American*, August 2008.

Christmas Lectures 2008

Zero-knowledge games



	1	2	3
Secret age =	11	17	14
	Total = 111	Total = 117	Total = 114
	22	39	34
	45	12	53
	44	66	27

Choose any 3 numbers that add up to 100 + your age. Write these 'shares' onto 3 pieces of paper.

Keep one of these shares yourself, and give the rest to the two other players.

1	2	3
22	39	34
53	45	12
66	27	44

Total = 141
number = 41
	Total = 111
	number = 11
		Total = 90
		number = 90

41	11	90

Find the total of these three shares, and take the two digits following the decimal point after dividing by 100

Add up these numbers and take the two digits following the decimal point after diving by 100 again (this part is not secret – everyone can check). This is the total of the secret ages of the 3 people!

Total = 142
number = 42

Total age = 42