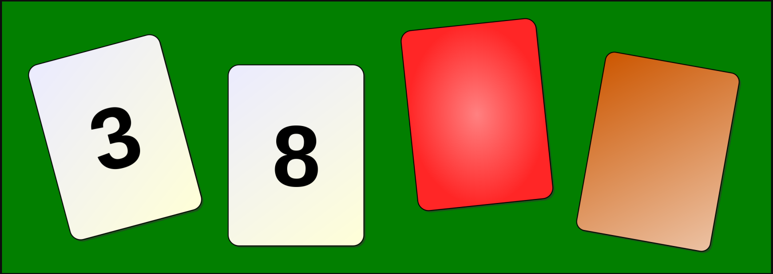
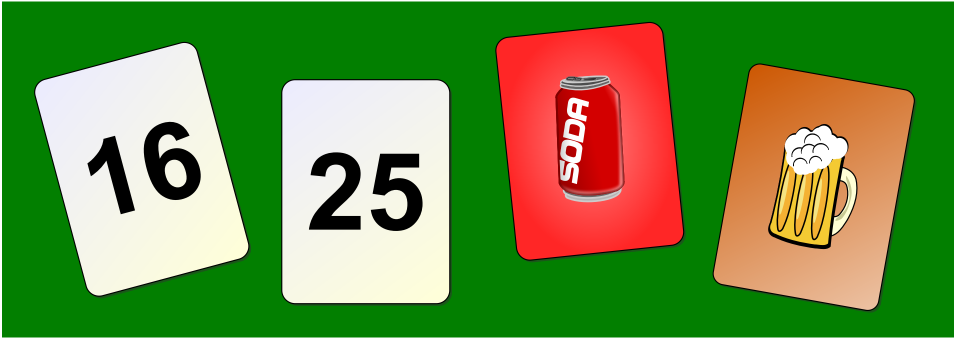
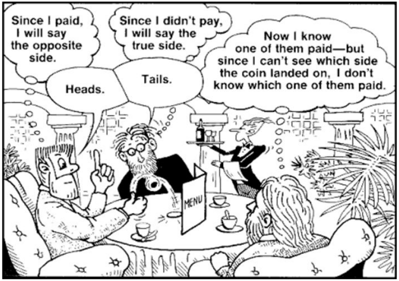

3
8

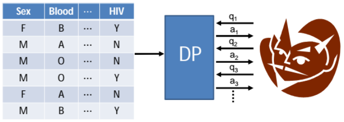

16
25
SODA

OPTIONAL

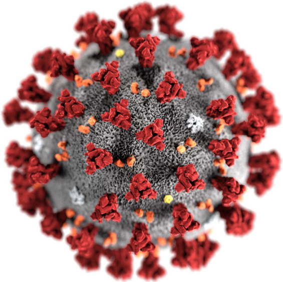
DC (Dining Cryptographers) nets [Chaum 1988]


Since I paid, I will say the opposite side.
Since I didn't pay, I will say the true side.
Now I know one of them paid—but since I can't see which side the coin landed on, I don't know which one of them paid.
Heads.
Tails.
MENU

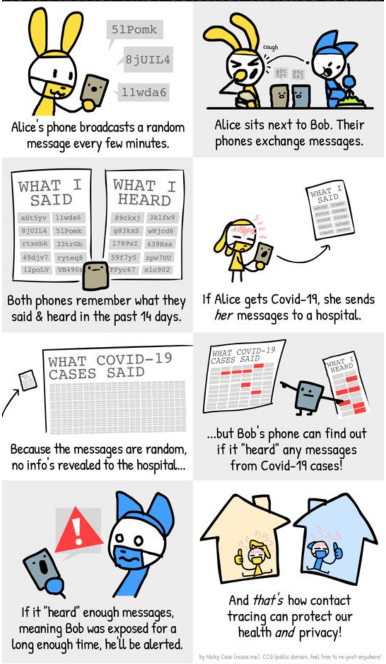
AVERAGE SALARY = ?
A
B
C



Sex	Blood	···	HIV
F	B	···	Y
M	A	···	N
M	O	···	N
M	O	···	Y
F	A	···	N
M	B	···	Y



HOW PRIVACY-FIRST CONTACT TRACING WORKS



Alice's phone broadcasts a random message every few minutes.

Alice sits next to Bob. Their phones exchange messages.

Both phones remember what they said & heard in the past 14 days.

If Alice gets Covid-19, she sends *her* messages to a hospital.

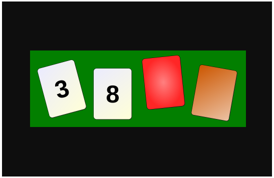
Because the messages are random, no info's revealed to the hospital...

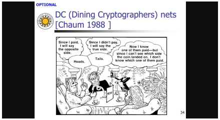
...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!

If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.

And *that's* how contact tracing can protect our health *and* privacy!

by Nicky Case (ncase.me). CC0/public domain. feel free to re-post anywhere!

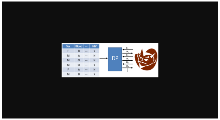




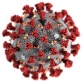
OPTIONAL

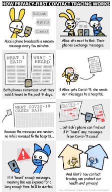
DC (Dining Cryptographers) nets [Chaum 1988]

Since I paid, I will say the opposite side.
Since I didn't pay, I will say the true side.
Now I know one of them paid—but since I can't see which side the coin landed on, I don't know which one of them paid.
Heads.
Tails.
MENU



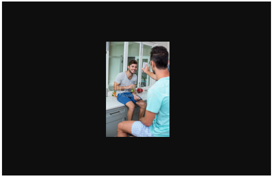
Sex	Blood	···	HIV
F	B	···	Y
M	A	···	N
M	O	···	N
M	O	···	Y
F	A	···	N
M	B	···	Y





HOW PRIVACY-FIRST CONTACT TRACING WORKS

51Pomk
8jUIL4
11wda6
Alice's phone broadcasts a random message every few minutes.
Alice sits next to Bob. Their phones exchange messages.
WHAT I SAID
WHAT I HEARD
Both phones remember what they said & heard in the past 14 days.
If Alice gets Covid-19, she sends her messages to a hospital.
WHAT COVID-19 CASES SAID
Because the messages are random, no info's revealed to the hospital...
...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!
If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.
And that's how contact tracing can protect our health and privacy!



Papers created during this process

- Op ed that started it
- This got a few people to write an expository version.
- I was allowed to sign the math version.
- We have written a letter Wash state legislature.
- I've worked on some psychological guidelines for apps.

Lecture notes:

- If a card is “brown” then it is “even.”
  - Which cards should be checked?
  - This is much harder than it should be
- If you are “drinking,” you are over “21.”
  - Trivial to check
  - We engage our internal Private Knowledge curcuit!
  - We worry about who knows what!
  - Called privacy.

- DC:
  - Story: Crypto people can’t accept money from the NSA or they will no longer be trusted. The waiter says, “Someone anonymously paid your bill.” They are worried it is the NSA. But it might be one of them. How can they check?
  - Easy: Just ask! Breaks anonymity
  - Cool protocol: At the end of the day, everyone knows if NSA paid, but not who the anonymous payer is if NSA didn’t pay.
- Computing an Average
  - Useful in statistics: Computing say an average of numbers. We can do this without knowing any of the values.
  - Can compute regressions
  - Example: Each person has an Alexa device. We want to compute a better machine learning model. We don’t want to ship the information from the Alexa to Amazon. We can still compute the regression without moving the data around. Further, no ones Alexa device learns anything about anyone elses except the regression coefficient.
- Differential privacy
  - Same idea–but with a slightly trusted database.
  - We want to protect all the knowledge we can except for stuff that has to do with the real world. So the sample is private, the “population estimates” are public

- Coronavirus picture:
  - What does this mean for a COVID App?
  - We want to know who has talked to whom, so we can inform them if one of them is infected
  - How can this be done privately? Or more accurately, as privately as possible?
  - When I get informed that I'm was exposed, what do I know? It has to have come from someone I was close to fairly recently. (Or if you are a formant(sp)
- trace description
  - see harvard paper and crypto paper
- flashing green
  - See psyc paper.