How to generate Research Ideas

Ivan Damgård

Does anyone really know?

- Do ideas for problems come “magically”?
- Or can we make them come?
- I don’t know!
- But can offer some “after the fact” thinking that can perhaps help a little bit.
- In particular: What happened in cases where there was success? Is there a pattern?

Example: make the problem easier

Multiparty secure computation:

Players P1…Pn each have input x1…xn

Want to compute function y= f(x1,…,xn) securely. That is,

- all players learn correct value of y, and
- y is the only new info that is leaked

- even if some players behave maliciously

The hard open problem

If we want best possible (information theoretic) security, can we get away with exchanging messages only a constant number of times?

(also known as constant round)

Open for at least 25 years – maybe I'm not going to solve it next week..

Easier Version

Can some of the players get away with minimal exchange of messages, i.e., send 1 message, receive 1 message?

Turns out to be tractable, and the answer is yes.

Example: Generalize

Known result: Privacy amplification.

A and B both have a random bit string X

Adversary Eve has some partial limited information about X.

A and B can talk to each other but Eve can listen to what they say.

Goal: A and B should both output string Y, such that Eve has (almost) no info on Y.

A more general scenario

A has string Xa, B has Xb, and they are correlated (some fixed joint distribution)

Eve has partial info on both strings

Goal: A outputs Ya, B outputs Yb such that (Ya,Yb) has some fixed joint distribution, and Eve has no information.

Turns out to be tractable for certain useful distributions.

The “stash of problems” approach

Keep list of problems you would love to solve. Longer is better. Simple as well as complicated ones.

Follow the literature in your area and make sure you notice each time someone comes up with an interesting new technique or tool.

Now ask: can this tool help to solve a problem on my list?

Notice Yourself!

Are there situations where you are more productive, where you get more ideas?

- on your bike, in the shower, taking a walk,…

Sometimes putting yourself in those situations on purpose can help.

For many of us, “trying very hard” to get ideas tends to be counterproductive!

Group Work

- Groups of 2-3 people from same or related fields
- What is your current favorite problem?
- How did you come up with it?
- Try to come up with a new problem
- If you succeeded, did you use any of the inputs from today? Or something else?