Crypto connections
… and dividing a pie

Rump Session of the
Workshop on T&P of SMPC
(May 08, 2014 – Aarhus, Denmark)

Luís Brandão

(University of Lisbon and Carnegie Mellon University)

ay 5 to 9, 2014
arhus University
Denmark

Workshop:

THEORY & PRACTICE of SECURE MULTIPARTY COMPUTATION

- Multiparty Computation is a cryptographic technique that lets you do amazing things
- The workshop brings together people from both theory and practice of the field
- The workshop is open to anyone interested

Sign up at www.cfem.au.dk or scan the QR code

Visiting Aarhus

The other day, after intensive lectures on secure computation, some of us got together for dinner.

(can you guess the common ingredient?)

After many potatoes, some of us still wanted to try dessert.

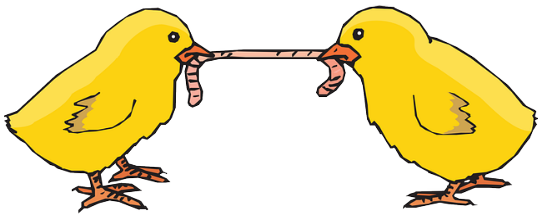
But money was scarce … as many of us had lost while betting on the winner of the Eurovision contest.

Eurovision
SONG CONTEST
COPENHAGEN 2014

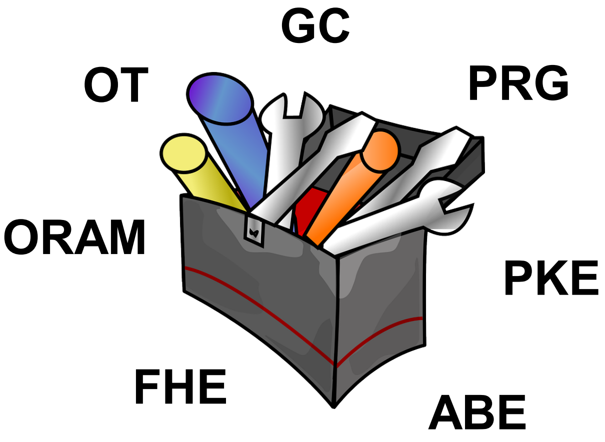
The problem

So Alice and Bob joined efforts and were able to gather enough donut-shaped Krones to buy an apple pie.

But now there was a problem! How to divide the pie in equal parts, namely when both were really hungry?

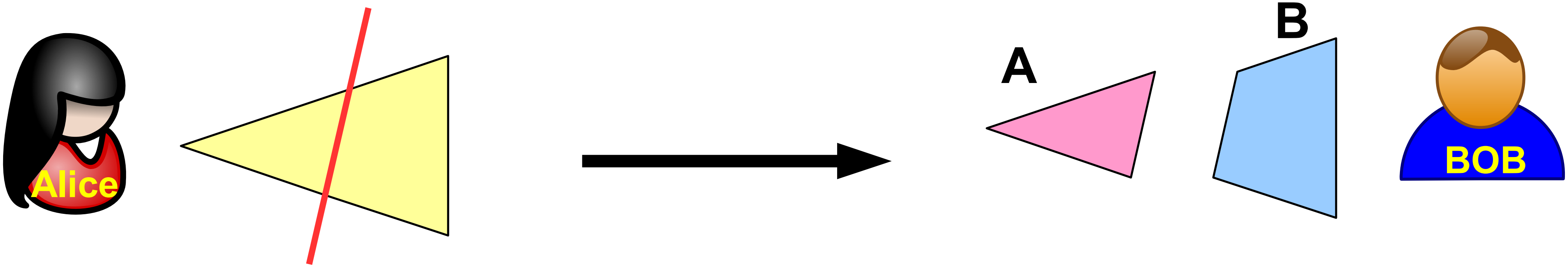


We had to use a secure protocol!



Two-party pie cut-and-choose

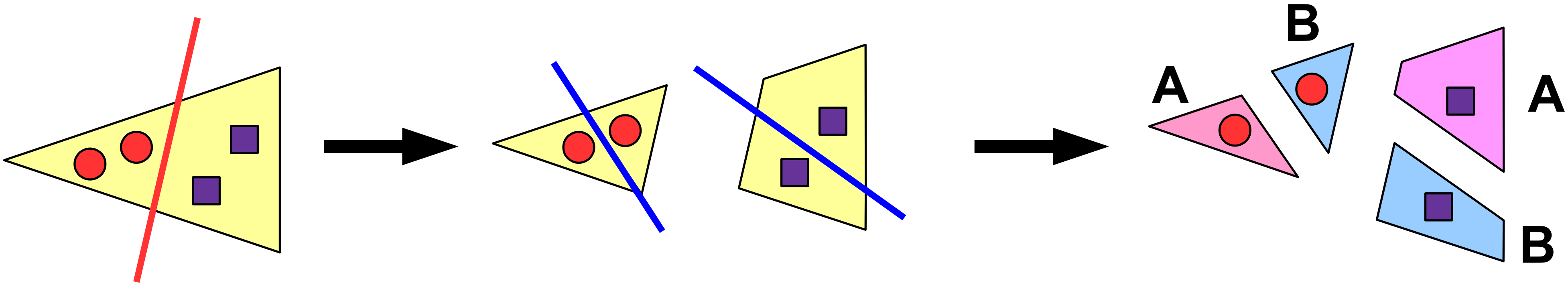
At first sight, this looked easy!



Step 1: Alice cuts

Step 2: Bob chooses

But upon closer inspection, Bob wanted a cherry and a blueberry. So he asks for one extra step in each of the two parts.



Step 1:
Alice cuts

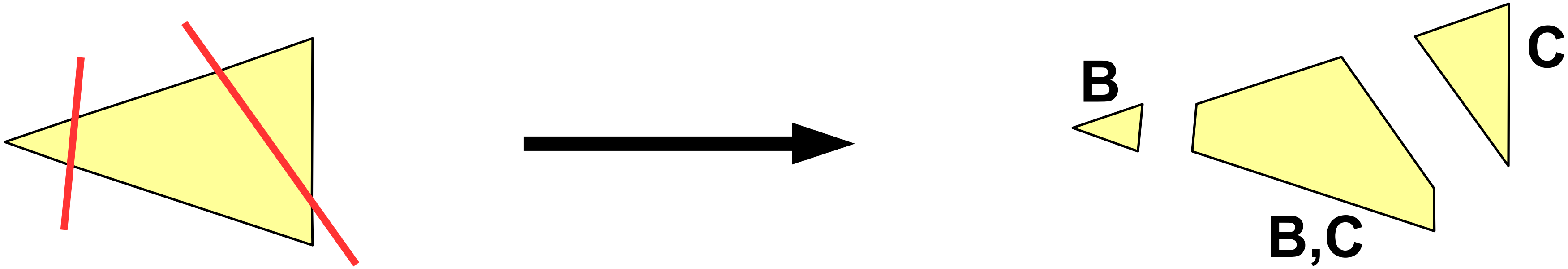
Step 2: Bob cuts
each part

Step 3: Alice chooses one
sub-part from each cut.

It could get more complicated (if the pie was more complex) ... but they were satisfied.

Three-party pie cut-and-choose

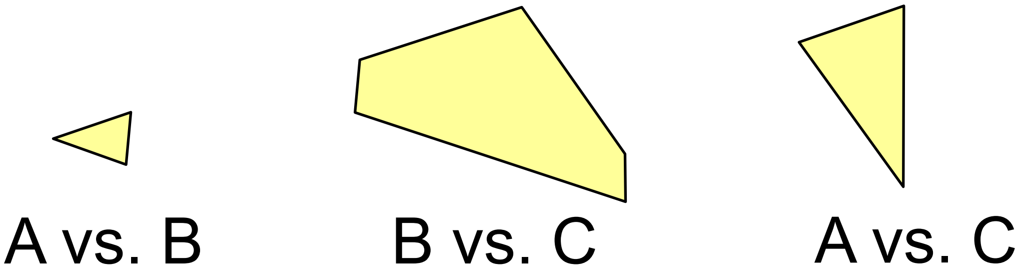
With all this complication, Cai also got hungry and asked for a piece of the pie! They all agreed to restart the division (without looking at the toppings, to simplify).



Step 1: Alice cuts in three

Step 2: each of Bob and Cai choose two parts

Step 3: each part is sub-divided by the two interested parties



The pie was tasty, and A, B, C felt lucky for being in a dinner with other secure-computation researchers!

The key insight:

It's quite useful and nice to bring together secure-computation researchers!

Thanks for organizing the workshop!

(and offering student stipends)

This motivates a further research question:

What about even more networking?
How to scale-up, from a linear number of workshops to a quadratic number of crypto connections?

Use case 1: Alice, a Ph.D. student researching Crypto, is traveling abroad and would not mind taking the chance to visit a crypto group in the area. She feels awkward to invite herself to stop by, but would be glad to do so for crypto-groups that advertise their willingness to receive visitors.

Use case 2: Bob is a under-graduate crypto-newbie student (still learning the basics and never attended a conference), but already knows that crypto is the topic of his future research. While planning his future, Bob would like to know where are the crypto-groups around the world, even those not currently advertising specific open positions for students.

Basic idea: a crypto-group directory

Create an online easy-to-browse directory, listing crypto-groups that are potentially available to be visited.

Each crypto-group would send basic info:

- Country, city, institution, website URL, contact info
- Main crypto-research topics, # crypto-researchers
- Willingness for which type of visits:
  - attending a seminar, or presenting a seminar;
  - informal meeting with the students;
  - discussing ongoing research;
  - couch-surfing, ...

Could propose to maintain this list at the IACR website and/or at another specific webpage.

Thank you for your attention!

Feedback is welcomed!

Presented at the rump Session of the *Workshop on Theory and Practice of Secure Multi-Party Computation*
(May 08, 2014 – Aarhus, Denmark)

**https colon slash slash
cryptoconnections dot wordpress dot com**

This was a non-technical rump-session talk, intended for entertainment. Some characters (Alice, Bob and Cai) in the story are fictitious, or their names have been changed to protect their privacy. Some aspects of the story were based on social conversations, but some resemblances are purely coincidental. Clipart images (e.g., from clker dot com and openclipart dot org) were obtained under the expectation of being available for free reuse.

Minor updates on June 05, 2014