Trustworthy and Secure Future Internet

An Implementation of Secure Two-Party Computation for Smartphones with Application to Privacy-Preserving

Gianpiero Costantino

and

Fabio Martinelli - Paolo Santi - Dario Amoruso

IIT - National Research Council - Pisa, Italy *Master Degree Student*

Paris | 17/07/2012

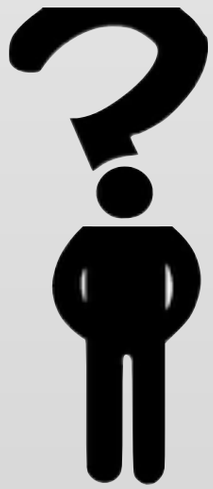
e-mail : gianpiero.costantino@iit.cnr.it

Overview

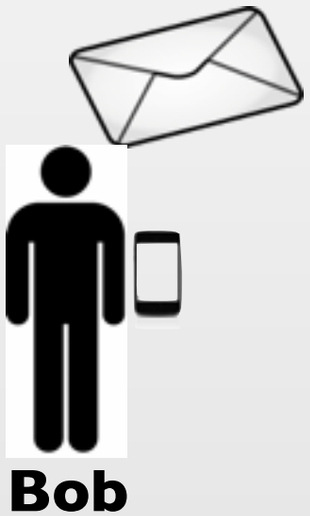
- Opportunist Networks
  - Interest Cast model.
- FairPlay Project
  - FairPlay for smartphone *(MobileFairPlay)*.
  - MobileFairPlay App.
- Time Evaluation
  - for compiling.
  - and running our secure function.
- Conclusions and Future Work

Opportunist Networks

- Opportunist networks are characterised by the presence of mobile devices, like:
  - ***Personal Digital Assistants (PDAs);***
  - ***SmartPhones;***
- Devices are not directly connected each other, as, for example, it happens within MANETs:
  - ***Store - Carry*** *and* ***Forward****;*



Opportunist Networks .2



Bob

Store

Forward

Carol

Alice

Interest - Cast

- Users share messages about topics in which they have same interest, like:
  - Books;
  - Cars;

- However, people would not disclose the “amount” of interest for a topic *(Do I know you?)*:
  - Books? I like...
  - Cars? I do not like...

Interest - Cast .2

- A user can express his/her “amount” of interest for a topic with a score between 1 and 100;
- Alice and Bob share their messages whether the following condition if verified:

$$| i_t - j_t | \leq \lambda$$

where:

- i is the degree of Alice’s interest;
- j is the degree of Bob’s interest;
- λ bounds the interest similarity;
- t is a selected topic.

Interest - Cast .3

- To verify the previous condition:
  - Alice must know j;
  - Bob must know i;

Privacy Issue

- Alice would not disclose i;
- Bob would not disclose j;

FairPlay Project

- FairPlay is a framework for secure two-party computation that allows users to write and run secure function;
- Alice and Bob would run:

$$f(x,y)$$

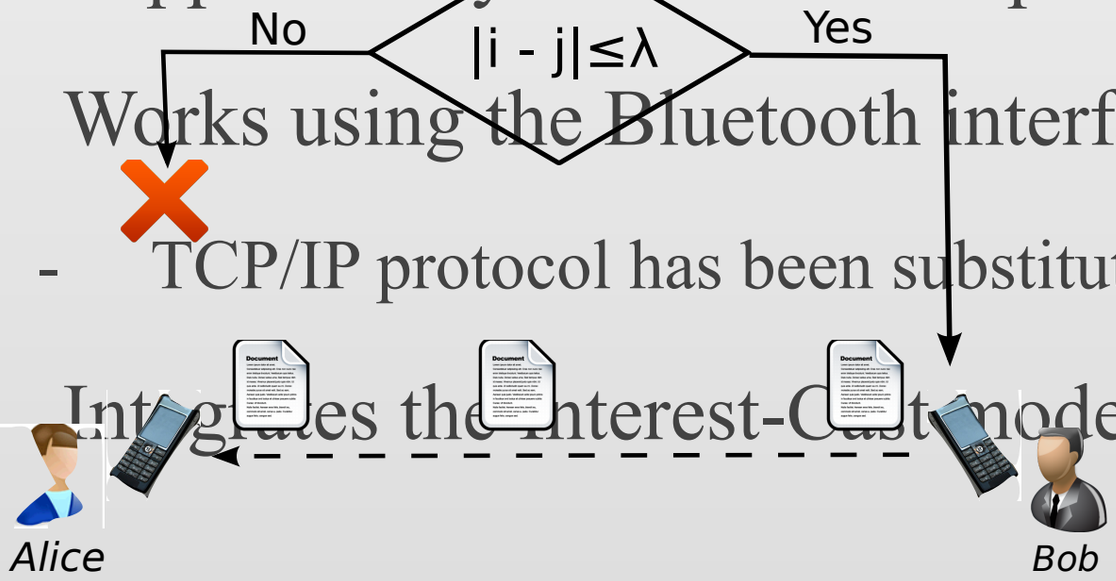
- By using FairPlay, Alice and Bob know the result of the function without disclosing out their input.
- No Trusted Third Party (TTP) is needed.

FairPlay Project .2

- Boolean circuits are obtained by compiling a function written with a high-level language *(SFDL)*;
- The compiled files are run by the participants of the secure function;
- Alice and Bob exchange their garbled circuits;
- At the end of all interactions, they know the result. of the function.

Mobile FairPlay

- "Thought" for Opportunist Networks;
  - Supports only Android Smartphones
  - Works using the Bluetooth interface
    - TCP/IP protocol has been substituted
  - Integrates the Interest-Cast model;



Mobile FairPlay .2

- In our application a user can:

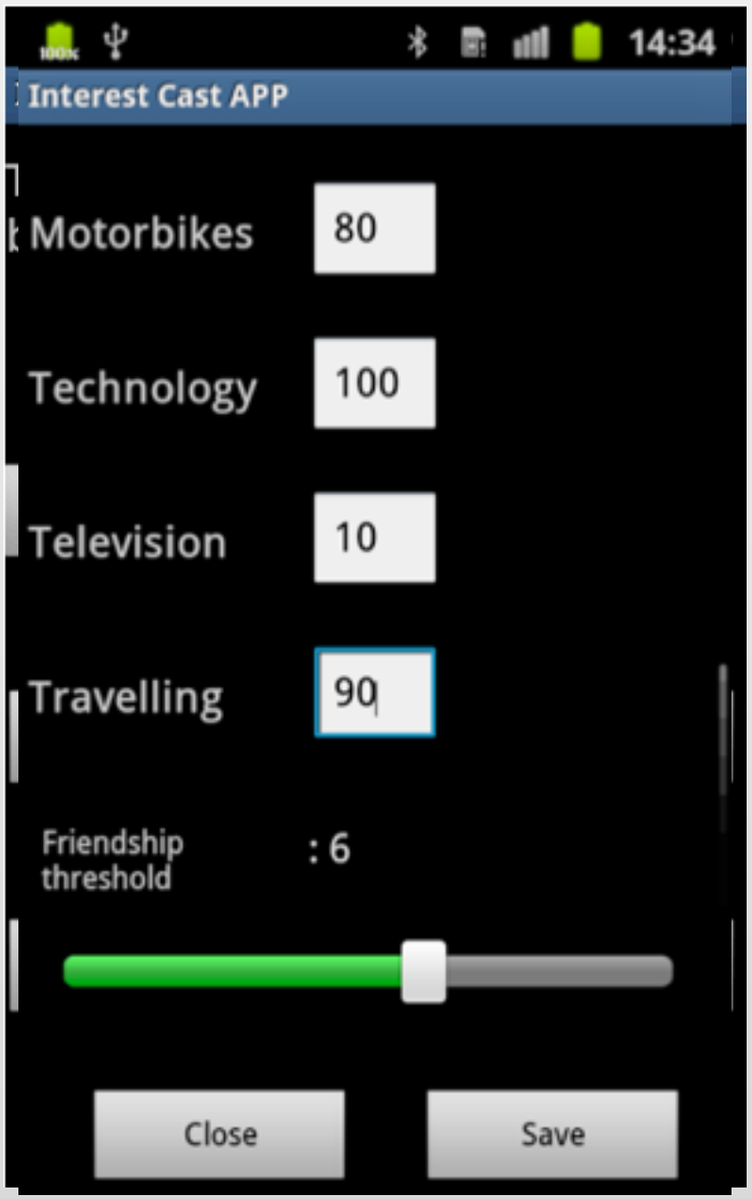
  I. Set up his own profile regarding different topics;

  II. Start a new connection with another user to run the interest-cast secure function;

  III. Wait for incoming connection;

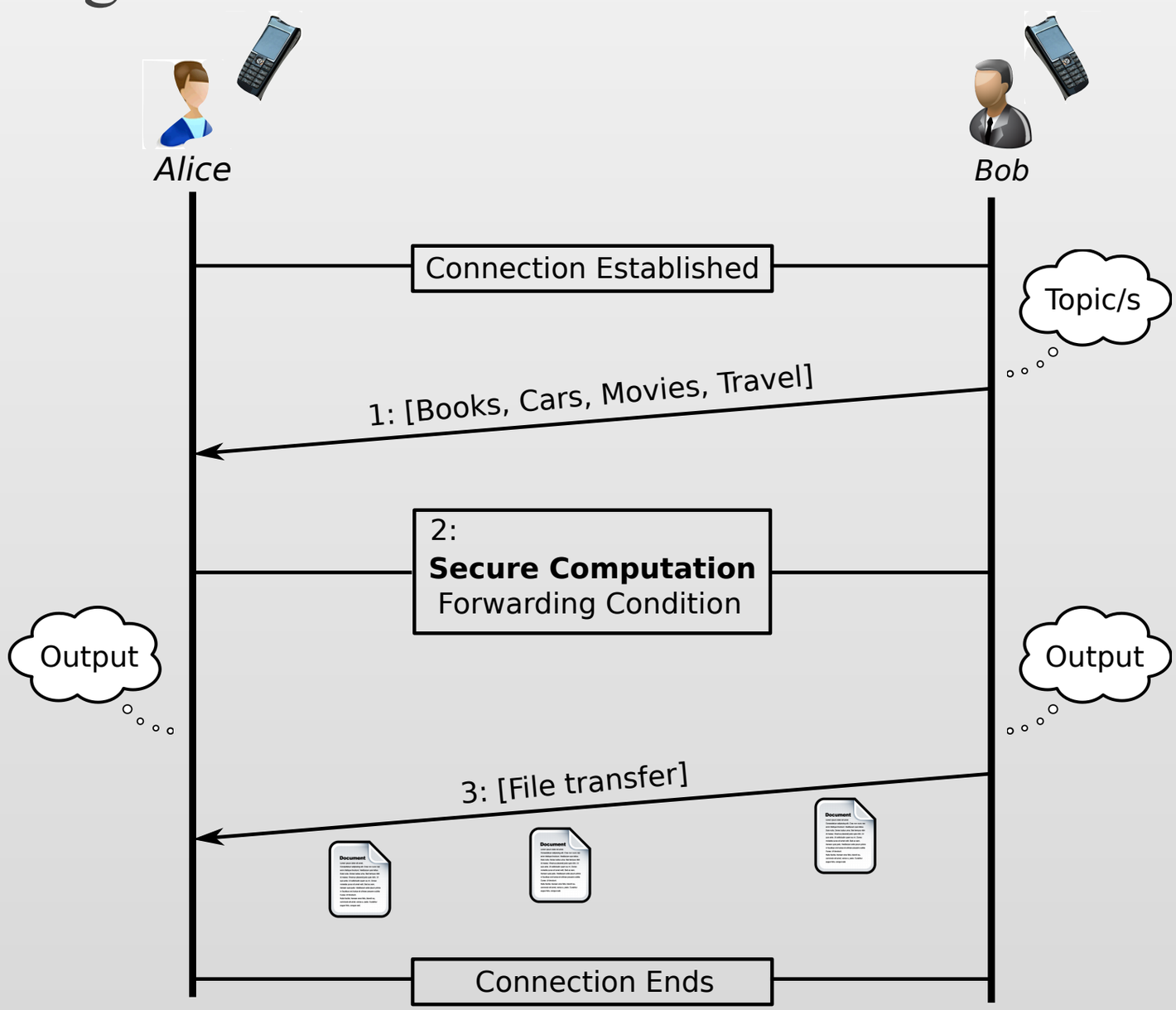
Mobile FairPlay .3

- Setting up the user's profile:



Mobile FairPlay .4

- Starting a new connection:



Evaluation

Computation Time

- We collected time-results needed to:
  - compile the SFDL function (1 and 4 topics);
  - run the secure function (1 and 4 topics).
- We used the following Smartphone for our test:

Smartphone	CPU	RAM
Samsung Galaxy S2	Dual-core 1228 MHz	1 GB
Samsung Galaxy Plus	Single-core 1443 MHz	512 MB
Samsung Galaxy S	Single-core 1024 MHz	512 MB
Lg Optimus Dual	Dual-core 1024 MHz	512 MB
HTC desire	Single-core 1024 MHz	512 MB

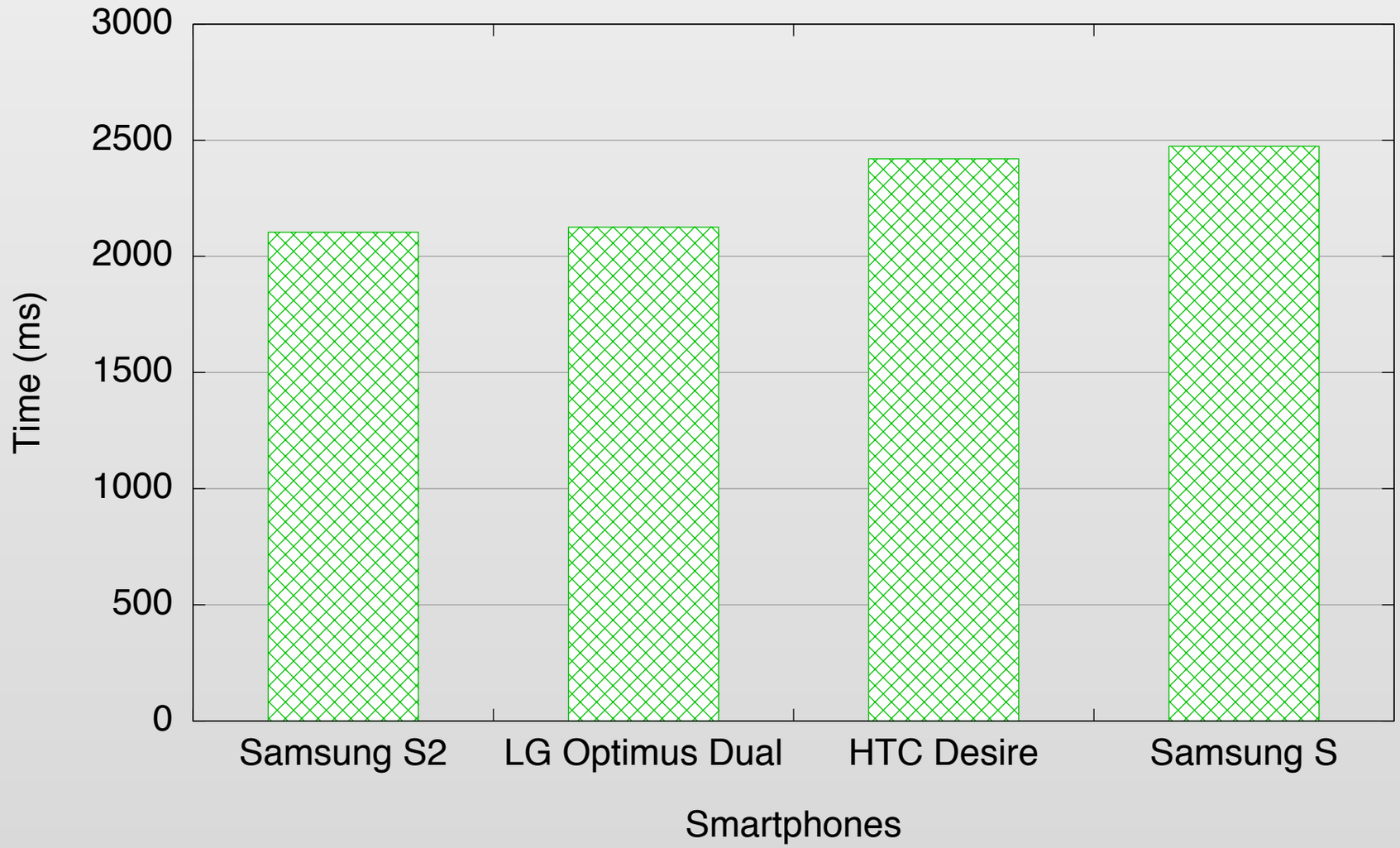
Compiling Time

- Four topics comparison:

Smartphone	Time (ms)
Samsung Galaxy S2	43721
Samsung Galaxy Plus	54457
Samsung Galaxy S	64825
Lg Optimus Dual	54592
HTC desire	64892

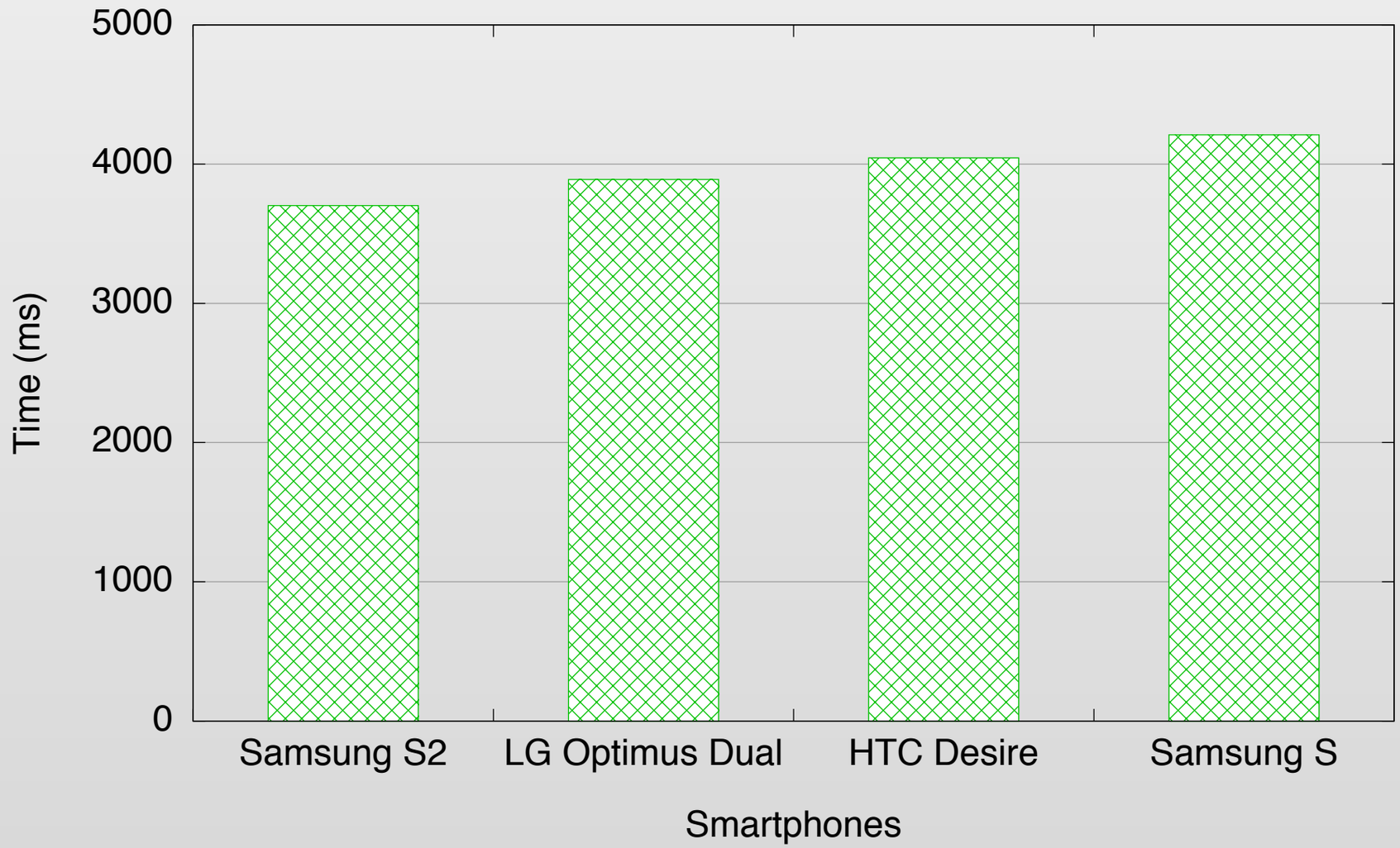
Running Time

- One topic comparison



Running Time

- Four topics comparison



Conclusion

- Opportunist communications should preserve users' privacy.
  - Avoiding to disclose out sensible information;
- MobileFairPlay can provide users' privacy with our secure function:
  - Reasonable running time, also for 4 topics;

- Future work:
  - Improving of reliability and efficiency of our app;
  - Extending the support of MobileFairPlay to other platforms.