

# SMPC as a Service

David Aparicio



14th MDPS Workshop, June 23, 2015

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

Appendix

## 1 Introduction

## 2 Secure multi-party computation

- Definitions
- Examples
- Models

## 3 SMPC Applications

- Classification
- Some applications

## 4 Our interests

- Verifiable
- Practical

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

Appendix

## 1 Introduction

## 2 Secure multi-party computation

- Definitions
- Examples
- Models

## 3 SMPC Applications

- Classification
- Some applications

## 4 Our interests

- Verifiable
- Practical

# Introduction

## Data is Everywhere with Internet of Everything

- Internet of People: 1,4B users
- Internet of Information: 60T/100Pb webpages
- Internet of Places: 7B checkins
- Internet of Things: 25B things (2020)

# Introduction

## Data is Everywhere with Internet of Everything

- Internet of People: 1,4B users
- Internet of Information: 60T/100Pb webpages
- Internet of Places: 7B checkins
- Internet of Things: 25B things (2020)

Common point?

# Introduction

## Data is Everywhere with Internet of Everything

- Internet of People: 1,4B users
- Internet of Information: 60T/100Pb webpages
- Internet of Places: 7B checkins
- Internet of Things: 25B things (2020)

## Common point?

Personal Information is involved and can be revealed.

# Introduction

## Data is Everywhere with Internet of Everything

- Internet of People: 1,4B users
- Internet of Information: 60T/100Pb webpages
- Internet of Places: 7B checkins
- Internet of Things: 25B things (2020)

## Common point?

Personal Information is involved and can be revealed.

## Possible solutions:

- Anonymization
- Obfuscation (noise)

# Introduction

## Data is Everywhere with Internet of Everything

- Internet of People: 1,4B users
- Internet of Information: 60T/100Pb webpages
- Internet of Places: 7B checkins
- Internet of Things: 25B things (2020)

## Common point?

Personal Information is involved and can be revealed.

## Possible solutions:

- Anonymization
- Obfuscation (noise)
- ... or use **Secure Multi-Party Computation theory**



David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions  
Examples  
Models

SMPC  
Applications

Our interests

Appendix

## 1 Introduction

## 2 Secure multi-party computation

- Definitions
- Examples
- Models

## 3 SMPC Applications

- Classification
- Some applications

## 4 Our interests

- Verifiable
- Practical

David Aparicio

Introduction

Secure  
multi-party  
computation

**Definitions**

Examples

Models

SMPC

Applications

Our interests

Appendix

- Yao and the Millionaires' Problem [1]

David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

Examples  
Models

SMPC

Applications

Our interests

Appendix

- Yao and the Millionaires' Problem [1]
- Goldreich, Micali, Wigderson  
How to play any mental game or A Completeness  
Theorem for Protocols with Honest Majority [2]

David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

Examples

Models

SMPC

Applications

Our interests

Appendix

Scenario:

## Definition: Private Information

Any information, recorded or otherwise, relating to an identifiable individual.

Examples: health, religion, history, location, habits, sex life...

David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

**Examples**

Models

SMPC

Applications

Our interests

Appendix

- Secure Sum protocol

David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

**Examples**

Models

SMPC

Applications

Our interests

Appendix

- Secure Sum protocol
- Secret Sharing [3]

David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

**Examples**

Models

SMPC

Applications

Our interests

Appendix

- Garbled circuits

David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

**Examples**

Models

SMPC

Applications

Our interests

Appendix

- Garbled circuits
- Homomorphic encryption



David Aparicio

Introduction

Secure  
multi-party  
computation

Definitions

**Examples**

Models

SMPC

Applications

Our interests

Appendix

- Garbled circuits
- Homomorphic encryption
- Zero-knowledge proof

# The different models [4]

David Aparicio

Introduction

Secure  
multi-party  
computation  
Definitions  
Examples  
Models

SMPC  
Applications

Our interests

Appendix

## Ideal model

Trusted party  
collects all inputs  
to calculate  
common result.

## Semi-honest model

No trusted party.  
All participants  
execute the  
protocol correctly.

## Real (malicious) model

No trusted party.  
Participants may  
deviate from the  
protocol.

# The different models [4]

David Aparicio

Introduction

Secure  
multi-party  
computation  
Definitions  
Examples  
Models

SMPC  
Applications

Our interests

Appendix

## Ideal model

Trusted party  
collects all inputs  
to calculate  
common result.

## Semi-honest model

No trusted party.  
All participants  
execute the  
protocol correctly.

## Real (malicious) model

No trusted party.  
Participants may  
deviate from the  
protocol.

## The Adversary

- Static
- Adaptative

# Outline

## 1 Introduction

## 2 Secure multi-party computation

- Definitions
- Examples
- Models

## 3 SMPC Applications

- Classification
- Some applications

## 4 Our interests

- Verifiable
- Practical

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

**Classification**

Some  
applications

Our interests

Appendix

Two kinds of input:

- Homogeneous SMPC model
- Heterogeneous SMPC model

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Classification  
Some  
applications

Our interests

Appendix

Two kinds of input:

- Homogeneous SMPC model
- Heterogeneous SMPC model

Privacy-preserving in:

- Database query
- Scientific computations
- Intrusion detection
- Statistical analysis
- Geometric computations
- Data mining

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Classification  
Some  
applications

Our interests

Appendix

- Elections
- Private auctions
- Query on private database
- Big Data with private databases
- and more...

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Classification  
Some  
applications

Our interests

Appendix

- Elections
- Private auctions
- Query on private database
- Big Data with private databases
- and more...
- The Danish farmers bet securely for the contracts to deliver sugar beets [6]



David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

Verifiable  
Practical

Appendix

## 1 Introduction

## 2 Secure multi-party computation

- Definitions
- Examples
- Models

## 3 SMPC Applications

- Classification
- Some applications

## 4 Our interests

- Verifiable
- Practical

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

**Verifiable**

Practical

Appendix

- Cloud Computing

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

**Verifiable**  
Practical

Appendix

- Cloud Computing
- Elections

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

**Verifiable**  
Practical

Appendix

- Cloud Computing
- Elections
- Public verification

David Aparicio

Introduction

Secure  
multi-party  
computation

SMPC  
Applications

Our interests

Verifiable




Practical

Appendix

- Beautiful protocols
  - Matrix Multiplication  $N*N$ , time in seconds
  - for  $25*25$  : PCPs  $10^{17}$  / GGP  $10^9$  / Ginger  $10^3$
  - for  $100*100$  : PCPs  $10^{21}$  / GGP  $10^{10}$  / Ginger  $10^5$

# Questions ?

# Bibliography I

-  A. C. Yao, “Protocols for secure computations,” in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pp. 160–164, IEEE, 1982.
-  O. Goldreich, S. Micali, and A. Wigderson, “How to play any mental game,” in *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pp. 218–229, ACM, 1987.
-  A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

# Bibliography II



Y. Lindell, “Tutorial on secure multi-party computation.” Presentation published on <http://u.cs.biu.ac.il/~lindell/research-statements/tutorial-secure-computation.ppt>, 6 2004.



W. Du and M. J. Atallah, “Secure multi-party computation problems and their applications: a review and open problems,” in *Proceedings of the 2001 workshop on New security paradigms*, pp. 13–22, ACM, 2001.



P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, *et al.*, “Secure multiparty computation goes live,” in *Financial Cryptography and Data Security*, pp. 325–343, Springer, 2009.