Secure Multi-Party Computation in a nutshell

Shengchao Ding

East China Normal University

20180916

Slides source: Professor Wang Huaxiong from NTU and Professor Nigel Smart from KU Leuven

Cryptography：Basic Tools / Protocols

- Basic Tools
  - Encryption schemes
  - Digital Signatures / Message Authentication
  - Hash Function
  - Psuderandom generators
- Protocols
  - Fault Tolerant Protocols
  - Zero Knowledge Proofs
  - Secure Multiparty Computation(SMPC)
    - Coin Tossing
      - securely and fairly produce a random number for parties, e.x. ZCash Powers of Tau
    - Secret Sharing
    - Oblivious Transfer
  - SMPC Application
    - Voting/Election
    - Poker
    - Privacy Presering Machine Learning

Basic Tools / Protocols Relation

The design of secure protocols that implement arbitrarily desired functionalities is a major part of modern cryptography. Taking the opposite perspective, the design of any cryptographic scheme may be viewed as the design of a secure protocol for implementing a suitable functionality. Still, we believe that it makes sense to differentiate between basic cryptographic primitives (which involve little interaction) like encryption and signature schemes, on the one hand, and general cryptographic protocols, on the other hand.

Goldreich, Oded. Foundations of cryptography: volume 2, basic applications. Cambridge university press, 2009. Page 601

Introduction

In 1997, Shafi Goldwasser (Turing Award recipient 2012) gave an invited talk at ACM SPDC: Multiparty Computations: Past and Present

The field of multiparty computations is today where public-key cryptography was ten years ago, namely an extremely powerful tool and rich theory whose real-life usage is at this time only beginning but will become in the future an integral part of our computing reality.

Introduction

- Secure MPC was introduced by Yao in 1982.
- The Millionaire Problem: Two millionaires want to know who is richer without revealing the amount of their actual wealth to each other.
- The problem was generalized by Goldreich, Micali and Wigderson to general n parties.
- Secure MPC is one of the most important crypto primitives: almost all the distributed secure protocols are based on secure MPC.

1. A. C. Yao, Protocols for secure computation. FOCS, 1982
2. O. Goldreich, S. Micali, and A. Wigderson, How to Play any Mental Game, STOC 1987

Defination

- Secure MPC: A group of participants $P_1, \ldots, P_n$ collaboratively computes a common function $f(x_1, \ldots, x_n)$ of their private inputs $x_1, \ldots, x_n$.
- Privacy: user P_i does not learn anything about $x_j, j \neq i$.
- Ideal functionality:
  1. Each user securely sends their x_i to a trusted third party (TTP).
  2. TTP computes $f(x_1, \ldots, x_n)$.
  3. Users receive result from trusted party.
- Goal: replace TTP with interactive protocol.

Defination cont.

A protocol $\prod$ computing f is said to be t-private if no coalition of t participants can obtain any information other than what is inferred by their common inputs and $f(x_1, \ldots, x_n)$.

The coalition of participants can be:

- passive (semi-honest): each of the t members follows the protocol.
- active (malicious): at least one of the t members is assumed to deviate from the protocol.

Security Models

Computationally secure: the adversary is polynomially bounded

Unconditionally secure: the adversary has unlimited computational power (information theoretic security)

Whiteboard Example
Millionare Problem illustrated

Computational MPC: GMW87, $t < n$

Goldreich, Micali and Wigderson in 1987 gave a solution to the general MPC computation problem.

In the presence of passive adversaries, assuming that one-way functions with a trapdoor exist (i.e. computationally secure), every function can be computed by n parties, in such a way that no subset of less than n parties can learn any additional useful information apart from the function value.

1. O. Goldreich, S. Micali, and A. Wigderson, How to Play any Mental Game, STOC 1987

Information-Theoretic MPC: BGW88, CCD88, $t < n/2$

- Positive Results:
  - Any function can be t-privately computed in the passive model when $t < \frac{n}{2}$.
  - Any function can be t-privately computed in the active model when $t < \frac{n}{3}$.
- Drawbacks: very inefficient in general.

1. M. BEN-OR, S. GOLDWASSER, AND A. WIGDERSON, Completeness theorems for non-cryptographic fault tolerant distributed computation, in 20th Annual ACM Symposium on Theory of Computing, ACM Press, 1988
2. D. CHAUM, C. CREPEAU AND I. DAMGARD, Multi-party unconditionally secure protocols, in 20th Annual ACM Symposium on Theory of Computing, ACM Press, 1988

Technology Readiness Levels

Nine levels TRL 1 to TRL 9.

We take the following few from the DoD defi ons

MPC in 1980s
till about 2005
(say)

Where does your research fit?

TRL 1

Basic principles observed and reported

Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology's basic properties. Published research that identifies the principles that underlie this technology. References to who, where, when.

Technology Readiness Levels

TRL 2

Technology concept and/or application formulated

Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.

Technology Readiness Levels

TRL 2

Techno c pplication formulated

In principles are observed, practical applications can be in speculative, and there may be no proof or detailed ptions. Examples are limited to analytic studies.

Typical of work in the 1990s

Technology Readiness Levels

TRL 3

Analytical and experimental critical function and/or characteristic proof of concept

Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative

Technology Readiness Levels

TRL 3

Analytical and experimental critical function and/or characteristic proof of concept

Activ R&D is … Thi includes analytical studies and laboratory studies to physic … va … tical predictions of separate elements of the techno … ponents that are not yet integrated or

Perhaps typified by creation of FairPlay by Pinkas et al

Technology Readiness Levels

TRL 4

Component and/or breadboard validation in laboratory environment

Basic technological components are int grate o establish that they will work together. This is relatively "low fidelity" m d wi h the eventual system. Examples include integration c d h n the laboratory.

Perhaps typified by creation of VIFF and SPDZ

Technology Readiness Levels

TRL 5
Component and/or breadboard validation in relevant environment

TRL 6
System/subsystem model or prototype demonstration in a relevant environment

TRL 7
System prototype demonstration in an operational environment.

TRL 8
Actual system completed and qualified through test and demonstration.

TRL 9
Actual system proven through successful mission operations.

Techn... Readiness Levels

TRL 5
Componen... and/or breadboard validation in releva...

TRL 6
System/subsystem mod... or prototype demonstrat... ...environment

TRL 7
System p... ...tion in an operational environme...

TRL 8
Actual system completed and qualified throu... ...n.

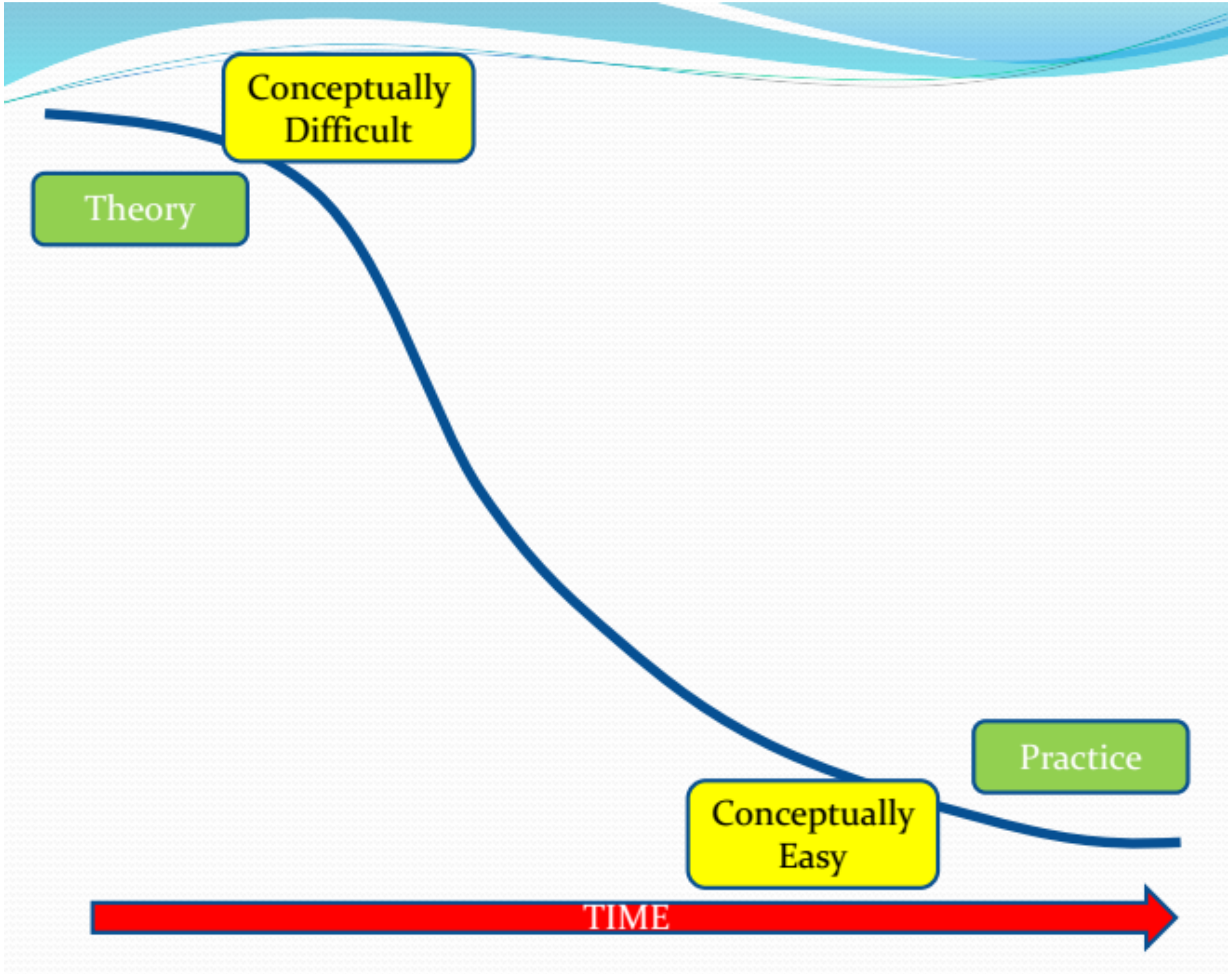
TRL 9
Actual system proven through successful missio... ...ions.

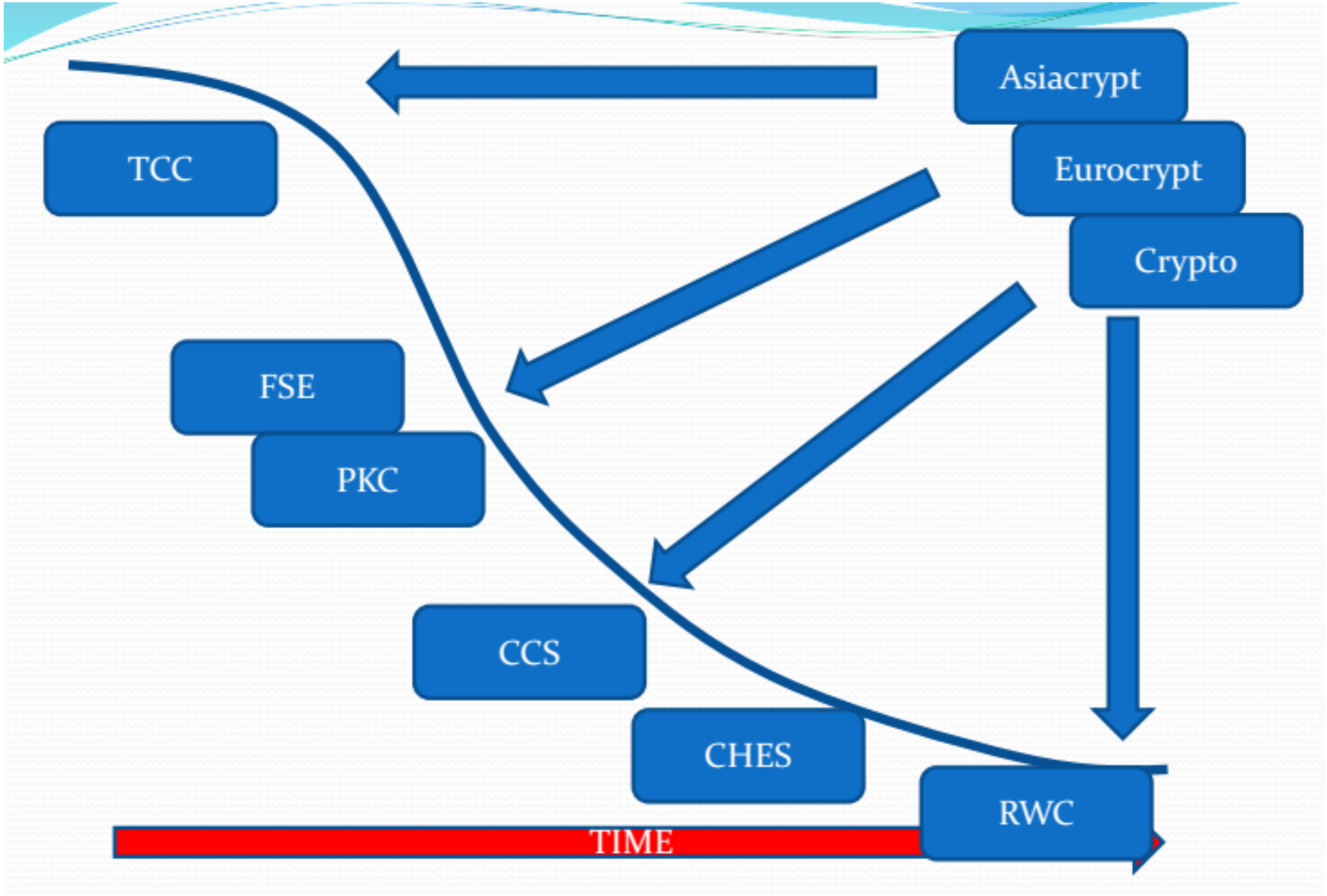
DARPA
Brandeis

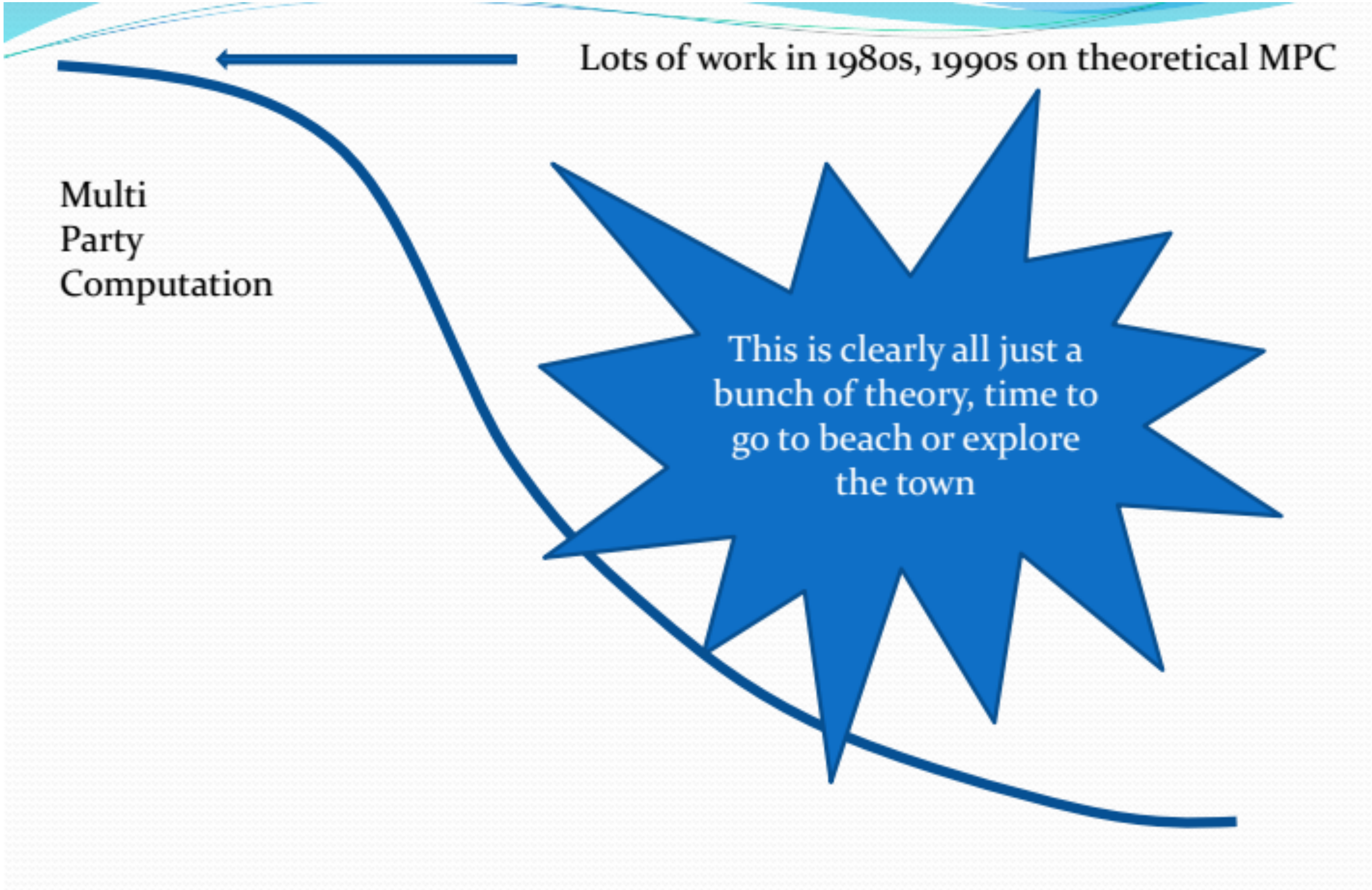
Cybernetica's
ShareMind

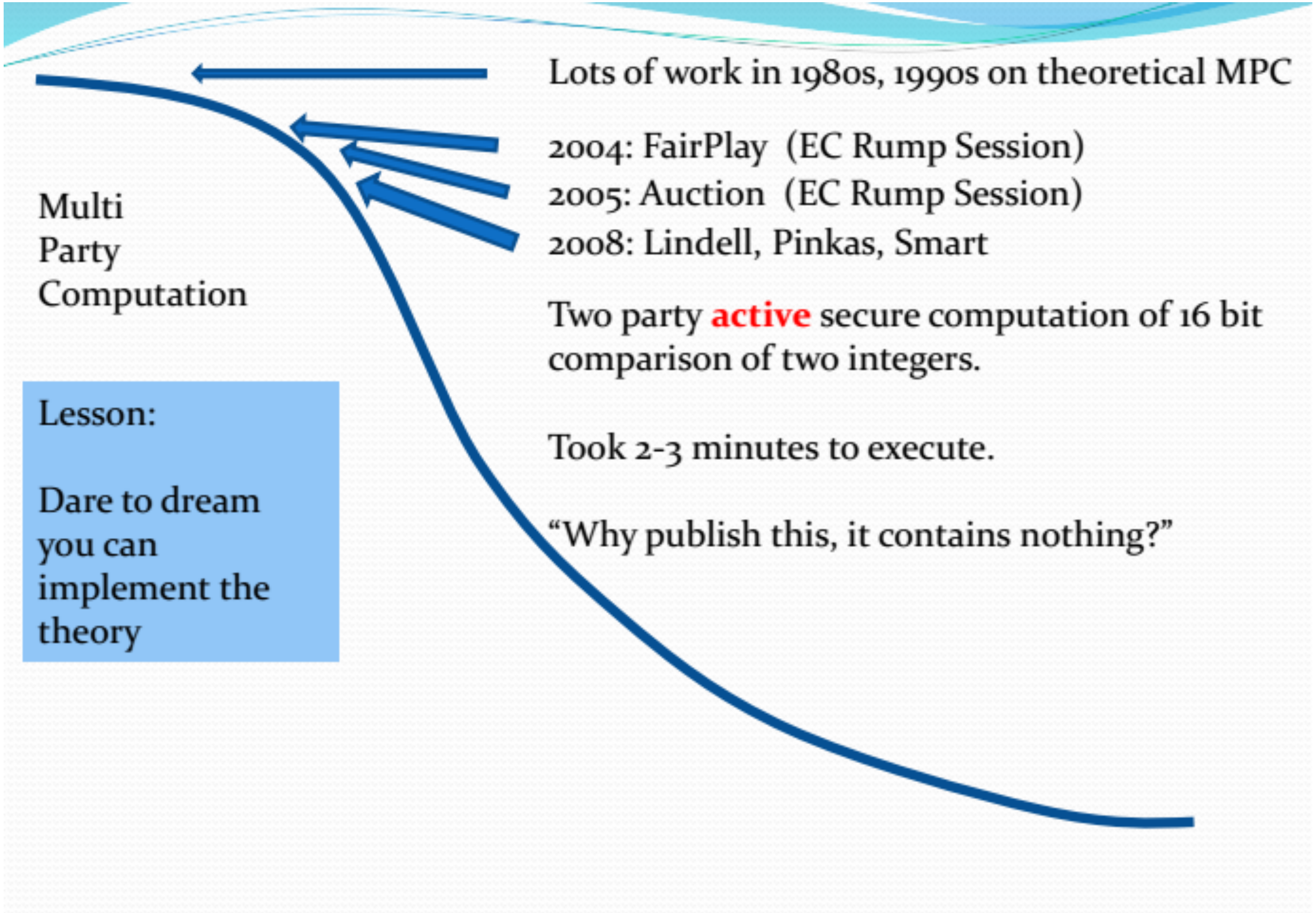
Partisia's
Auctions

Dyadic's
vHSM


Conceptually Difficult
Theory
Practice
Conceptually Easy
TIME


Asiacrypt
Eurocrypt
Crypto
TCC
FSE
PKC
CCS
CHES
RWC
TIME


Lots of work in 1980s, 1990s on theoretical MPC
Multi
Party
Computation
This is clearly all just a bunch of theory, time to go to beach or explore the town


Lots of work in 1980s, 1990s on theoretical MPC
2004: FairPlay (EC Rump Session)
2005: Auction (EC Rump Session)
2008: Lindell, Pinkas, Smart
Multi Party Computation
Two party **active** secure computation of 16 bit comparison of two integers.
Took 2-3 minutes to execute.
"Why publish this, it contains nothing?"
Lesson:
Dare to dream you can implement the theory

Lots of work in 1980s, 1990s on theoretical MPC

2009: Pinkas, Schneider, Smart, Williams

Multi
Party
Computation

AES

Two party AES

Why AES?

It took

- 1148 seconds active
- 7 seconds passive
- 60 seconds covert

Lots of work in 1980s, 1990s on theoretical MPC

2009: Pinkas, Schneider, Smart, Williams
2PC: Active: 1148 seconds
2 PC: Pass: 7 seconds

2010: 2PC: Pass: - : 4.5 sec
2011: 2PC: Pass: - : 211 ms
2012 2PC: Active: - : 0.6 sec (*)

2010: 3PC: Pass: - : 2000 ms (1C)
2012: 3PC: Pass: 320/sec : 14 ms (1C)
2012 3PC: Active: - : 0.6 sec (*)
2012 5PC: Active: - : 0.7 sec (*)
2012 10PC: Active: - : 1.0 sec (*)

2013: 2PC: Pass: - : 16 ms
2013: 2PC: Active: 2000 /sec : 12 ms (*)
2015: 2PC: Pass: 18/sec : 5 ms

2013: 3PC: Pass: 3450/sec : 323 ms (1C)
2016: 3PC: Pass: 25,000/sec : 223 ms (1C)
2016: 3PC: Pass: 1.3 m/sec : 116 ms (1C)
2016: 3PC: Pass: 90,000/sec : - (1C)
2017: 3PC: Active: 212,000/sec : - (1C)

2017: 2PC: Pass: 700/sec : 1.4 ms
2017: 2PC: Active: 64/sec : 15 ms
2017: 2PC: Active: 222000/sec : 0.9 ms (*)
2017: 2PC: Active: 3 million/sec : - ms

1C = Tolerate one corruption

* = Online runtimes only

Thanks!
Questions?