Multiparty Computation in 2029: Boom, Bust, or Bonanza!

David Evans
mightBeEvil.org
University of Virginia
Microsoft Research
Applied Multiparty Computation
21 February 2014
Why 2029?
Why 15 years?
Neil deGrasse Tyson

science’s endless golden age
To quantify this golden-age claim in astrophysics, I performed a simple experiment. I spend some part of each week in the department of astrophysics at Princeton University, whose library subscribes to twin copies of the *Astrophysical Journal*—one circulating and one not. Along one uninterrupted stretch of the library walls is every single issue ever published of this journal, which goes back to 1895 (about when the word *astrophysics* was coined—born in the marriage of the analysis of laboratory spectra with the analysis of stellar spectra). One day while browsing the journals I asked myself, “What year corresponds to the geometric middle of this wall?”
MPC in 2014

"multi-party computation"

Articles

Canon-MPC, a system for casual non-interactive secure multi-party computation
A Jarous, B Pinkas - Proceedings of the 12th ACM workshop on ..., 2013 - dl.acm.org
Abstract This work intends to bring secure multi-party computation to the masses by designing and implementing a browser-based system that enables non-interactive secure computation. The system, denoted Canon-MPC for Casual NON-interactive secure Multi- ... Related articles Cite Save

[ CITATION ] Erratum: A Dynamic Tradeoff between Active and Passive Corruptions in Secure Multi-Party Computation
... Erratum: A Dynamic Tradeoff between Active and Passive Corruptions in Secure Multi-Party Computation. Martin Hirt, Christoph Lucas, Ueli Maurer; ... show all 3 hide. Citations. Download Book (6,754 KB) As a courtesy to our readers the eBook is provided DRM-free. ... Cite Save

A Dynamic Tradeoff Between Active and Passive Corruptions in Secure Multi-
M Hirt, U Maurer, C Lucas - Advances in Cryptology–CRYPTO 2013, 2013 - Springer
MPC in 1999

"multi-party computation"

Secure multi-party computation
More than ten years have elapsed since the rst complete multi-party fault-tolerant computation have been announced and Wigderson, respectively). Analogous theorems have
Cited by 507 Related articles All 18 versions Cite

Adaptively secure multi-party computation
R Canetti, U Friege, O Goldreich, M Naor - 1996 - dl.ac
Abstract A fundamental problem in designing secure multi-party adaptive adversaries (i.e., adversaries that may choose the course of the computation), in a setting where the challenge
Cited by 333 Related articles All 28 versions Cite

Complete characterization of adversaries tolerant
M Hirt, U Maurer - Proceedings of the sixteenth annual
Abstract The classical results in unconditional multi-party
players state that less than n/2 passive or less than n

1999
Invited Talk:
Multi-Party Computations: Past and Present
Shafi Goldwasser*

SHAFI GOLDWASSER
ACM A.M. Turing Award
United States, Israel – 2012
READ FULL CITATION AND ESSAY
CITATION
Along with Silvio Micali, for transforming complexity-theoretic foundations for cryptography, and in the process pioneered new mathematical proofs in complexity.

PODC 1997

Whereas in the 80’s the focus of research was to show the most general result possible yielding multi-party protocol solutions for any probabilistic function, any adversary class, and any network constraints, the theme of the 90’s is different. Much of current work is to focus on efficient and non-interactive solutions to special important problems such as joint-signatures, joint-encryption, and secure and private data base access. Some of the new conceptual issues that researchers are currently tackling are the deniability of users actions in presence of a coercing adversary and the anonymity of users.

We believe that the field of multi party 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.
MPC in 1984

[HTML] Microsoft Research Redmond Cryptography Colloquium Past Speakers
G Segev, S Agrawal, P Mohassel… - University of ..., 1908 - research.microsoft.com
Microsoft Research Redmond Cryptography Colloquium Past Speakers. ...
Non-free NOR gate (from Apollo Guidance Computer)
Where should multiparty computation be in 2029?
US Government Investment in MPC

NSF: ~$25M
DARPA: ~$25M
AFOSR: ~$15M
IARPA, NSA: ?

$100M?

National Endowment for the Arts
$130M/year
US Government Investment in MPC

NSF: ~$25M
DARPA: ~$25M
AFOSR: ~$15M
IARPA, NSA: ?

$100M?

Virginia Snow Removal Last Week

> $100M
“Acceptable” Result (for “Us”)

- some significant papers
- interesting intellectual problems
- students get good jobs

Photo credit: Benny Pinkas
“Acceptable” Result (for Taxpayers)

Multi-billion dollar industry

Things that make everyday life better

Photo credit: Benny Pinkas
Where should multiparty computation be in 2029?
Claim #1

Secure multi-party computation industry should be bigger than malware industry in 2029.
Worldwide IT Security Market: 
~$70B/year, 
growing 8.7%/year 
[\textit{Gartner}] 

projected continued 8.7% growth
Worldwide IT Security Market: ~$70B/year, growing 8.7%/year [Gartner]
Claim #2

High cost is no longer the main impediment to widespread use of secure (two-party) computation.
(De)Motivating Application: “Genetic Dating”

Your offspring will have good immune systems!

WARNING! Don’t Reproduce

WARNING! Don’t Reproduce

Genome Compatibility Protocol
Progress in MPC!

1982

Protocols for Secure Computations (extended abstract)

Andrew C. Yao
University of California
Berkeley, California 94720

1. INTRODUCTION.

Two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other’s wealth. How can they carry out such a conversation?
New App Prevents Icelanders from Sleeping With their Relatives

Monday, 15 April 2013 06:04 | Font size | Print | Email
A user commented on the app's website:

"If I would have had this app last year I probably wouldn't have gone home with my cousin"
Cost to sequence genome

“Moore’s Law”

$100,000,000
$10,000,000
$1,000,000
$100,000
$10,000
$1,000

Aug 2001
Mar 2002
Oct 2002
May 2003
Dec 2003
Jul 2004
Feb 2005
Sep 2005
Apr 2006
Nov 2006
Jun 2007
Jan 2008
Aug 2008
Mar 2009
Oct 2009
May 2010
Dec 2010
Jul 2011
Feb 2012
Sep 2012
Apr 2013
Nov 2013
From $100M to $0.001 in less than a decade!
From $80B to $0.005 in less than a decade!
Costs that Still Matter

**Many Parties:** costs for > 3 parties are still way off the charts (and interesting applications need millions of parties)

**Energy:** MPC requires $10,000\times (?)$ energy of unencrypted computation

– Data centers today $\sim 5M$ homes
Things That Really Matter

Understanding what outputs leak
Embedding auditing? Privacy models?
Meaningful end-user value
How do I trust the client code?
(Human) cost to build MPC systems
Easy integration/separation with standard computation
Claim #3

We don’t yet know what the “killer app” for MPC is.*

* Maybe we will after the Business Case panel today!
Claim #3

We don’t yet know what the “killer app” for MPC is and its probably not privacy.
<table>
<thead>
<tr>
<th>Action Description</th>
<th>Percentage of Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Borrowed a book from thousands of miles away</td>
<td>73%</td>
</tr>
<tr>
<td>Crossed the country without asking for directions</td>
<td>82%</td>
</tr>
<tr>
<td>Sent someone a fax from the beach</td>
<td>44%</td>
</tr>
<tr>
<td>Paid a toll without slowing down</td>
<td>64%</td>
</tr>
<tr>
<td>Bought concert tickets from a cash machine</td>
<td>56%</td>
</tr>
<tr>
<td>Tucked your baby in from a phone booth</td>
<td>58%</td>
</tr>
<tr>
<td>Opened doors with the sound of your voice</td>
<td>18%</td>
</tr>
<tr>
<td>Carried your medical history in your wallet</td>
<td>20%</td>
</tr>
<tr>
<td>Attended a meeting in your bare feet</td>
<td>67%</td>
</tr>
<tr>
<td>Watched the movie you wanted to the minute you could</td>
<td>98%</td>
</tr>
<tr>
<td>Conducted business in a language you don’t understand</td>
<td>13%</td>
</tr>
<tr>
<td>Kept an eye on your home when you’re not at home</td>
<td>24%</td>
</tr>
<tr>
<td>Renewed your driver’s license at a cash machine</td>
<td>84%</td>
</tr>
<tr>
<td>Fixed your car with a television</td>
<td>16%</td>
</tr>
<tr>
<td>Had an assistant who lived in your computer</td>
<td>33%</td>
</tr>
</tbody>
</table>
It is difficult to predict, especially about the future
Theory vs. Practice
My New Theory of Computation Book!
Dori-Mic and the Universal Machine!

A Tragicomic Tale of Combinatorics and Computability for Curious Children of All Ages

Illustrations by Kim Dylla
“If only I had this book when I was a young student, I might have done something useful with my life like discover a new complexity class instead of dropping out and wasting my life flipping pancakes, playing with basic blocks, and eradicating polo.”

Gill Bates,
Founder of Mic-Soft Corporation
Finding the “killer app” for MPC...
“sending faxes from the beach”

“tucking your baby in from a phone booth”
WorldWideWeb
[Berners-Lee 1990]

multi-touch, pressure interface
[Negroponte 1984]
David Evans
evans@virginia.edu

MightBeEvil.com
dori-mic.org