

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

David Evans
mightBeEvil.org
University of Virginia
Microsoft Research
Applied Multiparty Computation
21 February 2014



MONEY CHANGER
All DEBIT/CREDIT Card Accepted
AMERICAN EXPRESS MasterCard VISA Maestro

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"

Scholar

About 697 results (0.02 sec)

Articles

Case law

My library **New!**

Any time

Since 2014

Since 2013

Since 2010

Custom range...

Sort by relevance

Sort by date

[Canon-MPC, a system for casual non-interactive secure multi-party computation](#)

[A Jarrous](#), [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 Corruption in Secure Multi-Party Computation](#)

[M Hirt](#), [C Lucas](#), [U Maurer](#) - [Advances in Cryptology—CRYPTO 2013](#), 2013 - [Springer](#)

... 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"

Scholar

About 162 results (0.14 sec)

Articles

[\[PDF\] Secure multi-party computation](#)

[O Goldreich - Manuscript. Preliminary version, 1998 - C](#)

Case law

More than ten years have elapsed since the first complete multi-party fault-tolerant computation have been announced (by Goldreich and Wigderson, respectively). Analogous theorems have been proved (by Goldreich and Wigderson, respectively). Analogous theorems have been proved (by Goldreich and Wigderson, respectively).

My library **New!**

[Cited by 507](#) [Related articles](#) [All 18 versions](#) [Cite](#)

Any time

[Adaptively secure multi-party computation](#)

Since 2014

[R Canetti, U Friege, O Goldreich, M Naor - 1996 - dl.ac](#)

Since 2013

Abstract A fundamental problem in designing secure multi-party computation is to tolerate adaptive adversaries (ie, adversaries that may choose their strategy based on the course of the computation), in a setting where the adversary is computationally bounded.

Since 2010

[Cited by 333](#) [Related articles](#) [All 28 versions](#) [Cite](#)

Custom range...

1985 — 1999

Search

[Complete characterization of adversaries tolerating corrupt](#)

[M Hirt, U Maurer - Proceedings of the sixteenth annual](#)

Abstract The classical results in unconditional multi-party computation show that players state that less than $n/2$ passive or less than $n/3$ active players can be tolerated.



1999

2014

Invited Talk:

Multi-Party Computations: Past and Present

Shafi Goldwasser*

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-decryption, 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.

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 pioneering new mathematical proofs in complexity



Articles

Case law

My library **New!**

Any time

Since 2014

Since 2013

Since 2010

Custom range...

— 1984

Search

Sort by **relevance**

Sort by date

include patents

include citations

Create alert

[CITATION] Privacy-Preserving Hierarchical-k-Means Clustering on Horizontally Partitioned Data
X Anrong, J Dongjie... - International ..., 1900 - Hindawi Publishing Corporation
Cite Save

[Quantum Private Comparison Protocol with W States](#)

WW Zhang, D Li, YB Li - International Journal of Theoretical Physics, 1970 - Springer
... Secure **multi-party computation** (SMC) deals with computing a function with private inputs in a distributed network where each party holds one of the private inputs, and that no more information about one party's private input is revealed to other parties in the computation. ...
Related articles Cite Save

[Object-Oriented Approach to Specify Secret Sharing Protocol in Security Critical System Using Formal Method](#)

YK Meng, MZ Rahman, SP Lee - Malaysian Journal of ..., 1970 - umrefjournal.um.edu.my
... 383-395, IEEE. [14] ID Ronald Cramer and U. Maurer, "Span Programs and General Secure **Multi-Party Computation**," Brics, 1997. [15] GR Roger Duke, Paul King and G. Smith, "The Object-Z Specification Language: Version 1.," Tech. Rep. ...
Related articles Cite Save More

Related articles Cite Save More

[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. ...

Cite Save More

K Lai - Communications of the ACM, 1970 - hub.hku.hk

Page 1. Title Solving multiparty private matching problems using Bloom-filters Author(s) Lai, Ka-ying.; Citation Issue Date 2006 URL http://hdl.handle.net/10722/50824 Rights The author retains all proprietary rights, (such as patent rights) and the right to use in future works. ...
Related articles All 2 versions Cite Save More

[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. ...
Cite Save More

[PDF] [68P01 General](#)

PAS Valdes, O Weerts, IV Halpern - see Section 04 in that area 1063 - 105 130 120 108

MPC in 1984



MPC in 1969

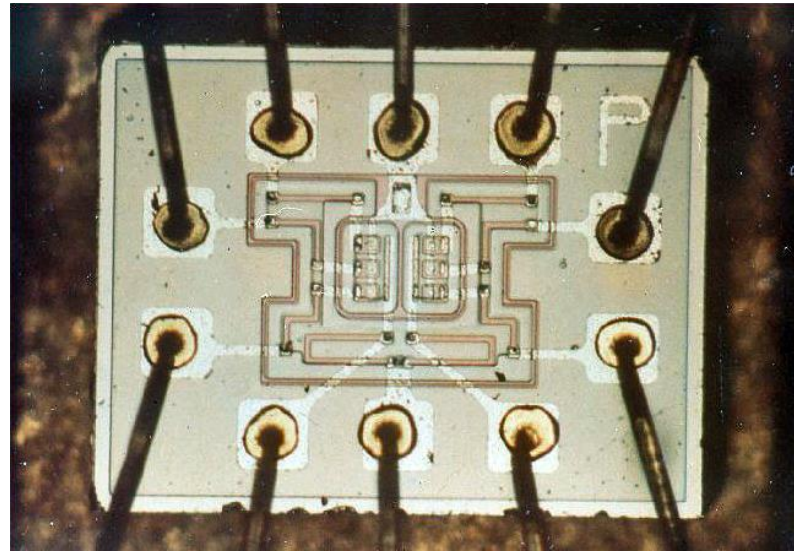


↑
1969

↑
1984

↑
1999

10 2014



Non-free NOR gate (from Apollo Guidance Computer)

Where should
multiparty computation
be in 2029?

US Government Investment in MPC

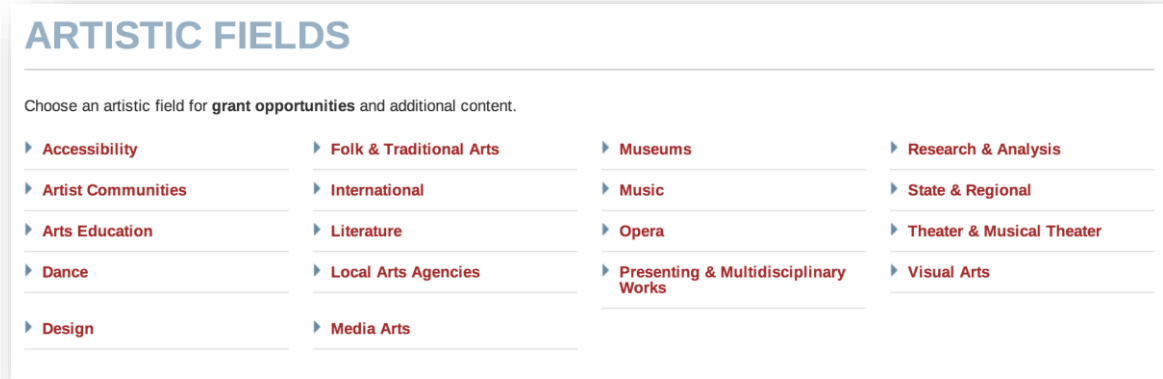
NSF: ~\$25M

DARPA: ~\$25M

AFOSR: ~\$15M

IARPA, NSA: ?

\$100M?



ARTISTIC FIELDS

Choose an artistic field for grant opportunities and additional content.

▶ Accessibility	▶ Folk & Traditional Arts	▶ Museums	▶ Research & Analysis
▶ Artist Communities	▶ International	▶ Music	▶ State & Regional
▶ Arts Education	▶ Literature	▶ Opera	▶ Theater & Musical Theater
▶ Dance	▶ Local Arts Agencies	▶ Presenting & Multidisciplinary Works	▶ Visual Arts
▶ Design	▶ Media Arts		

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”)



Photo credit: Benny Pinkas

some significant papers

interesting intellectual problems

students get good jobs

“Acceptable” Result (for Taxpayers)



Photo credit: Benny Pinkas

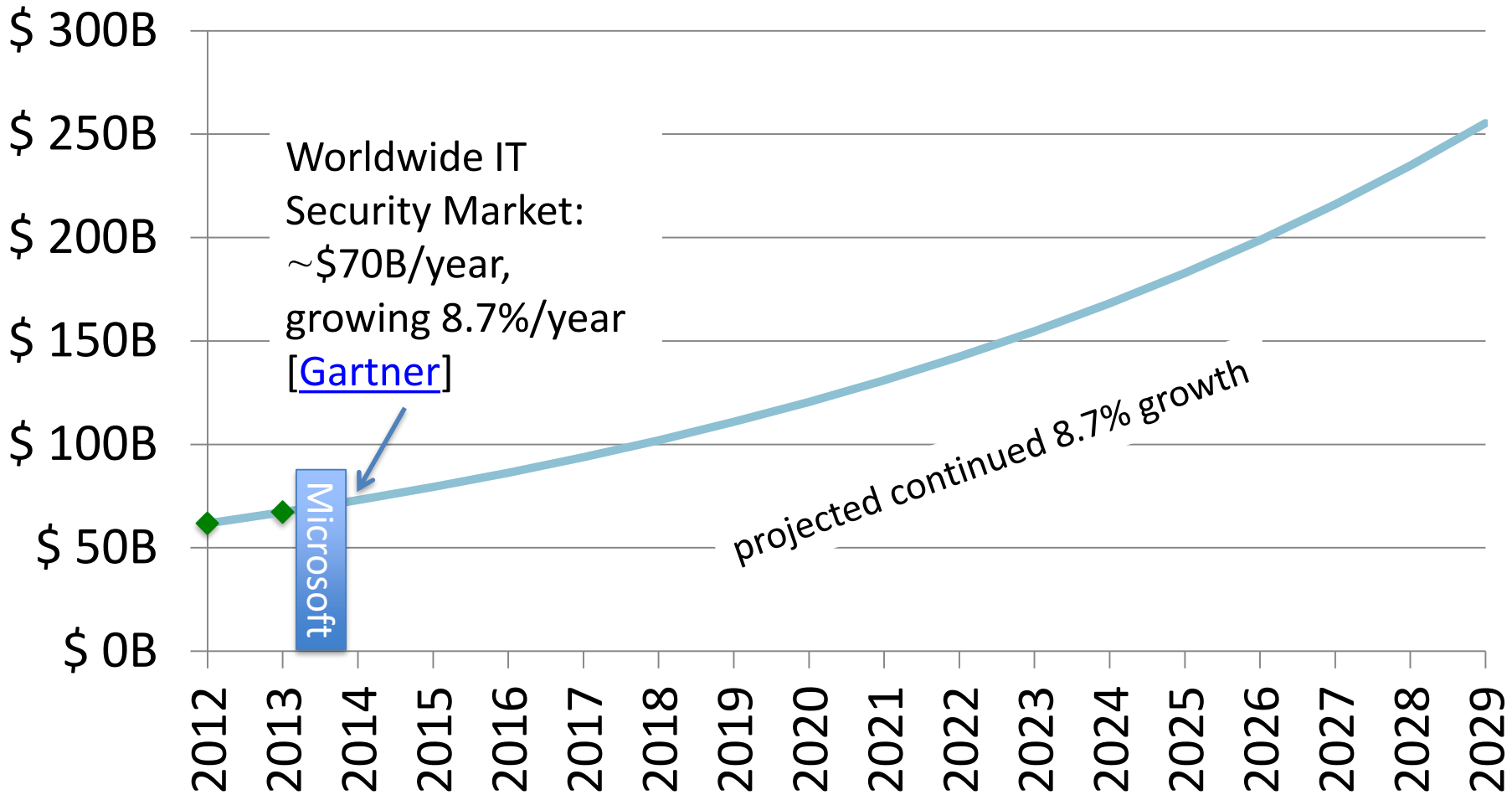
Multi-billion dollar industry

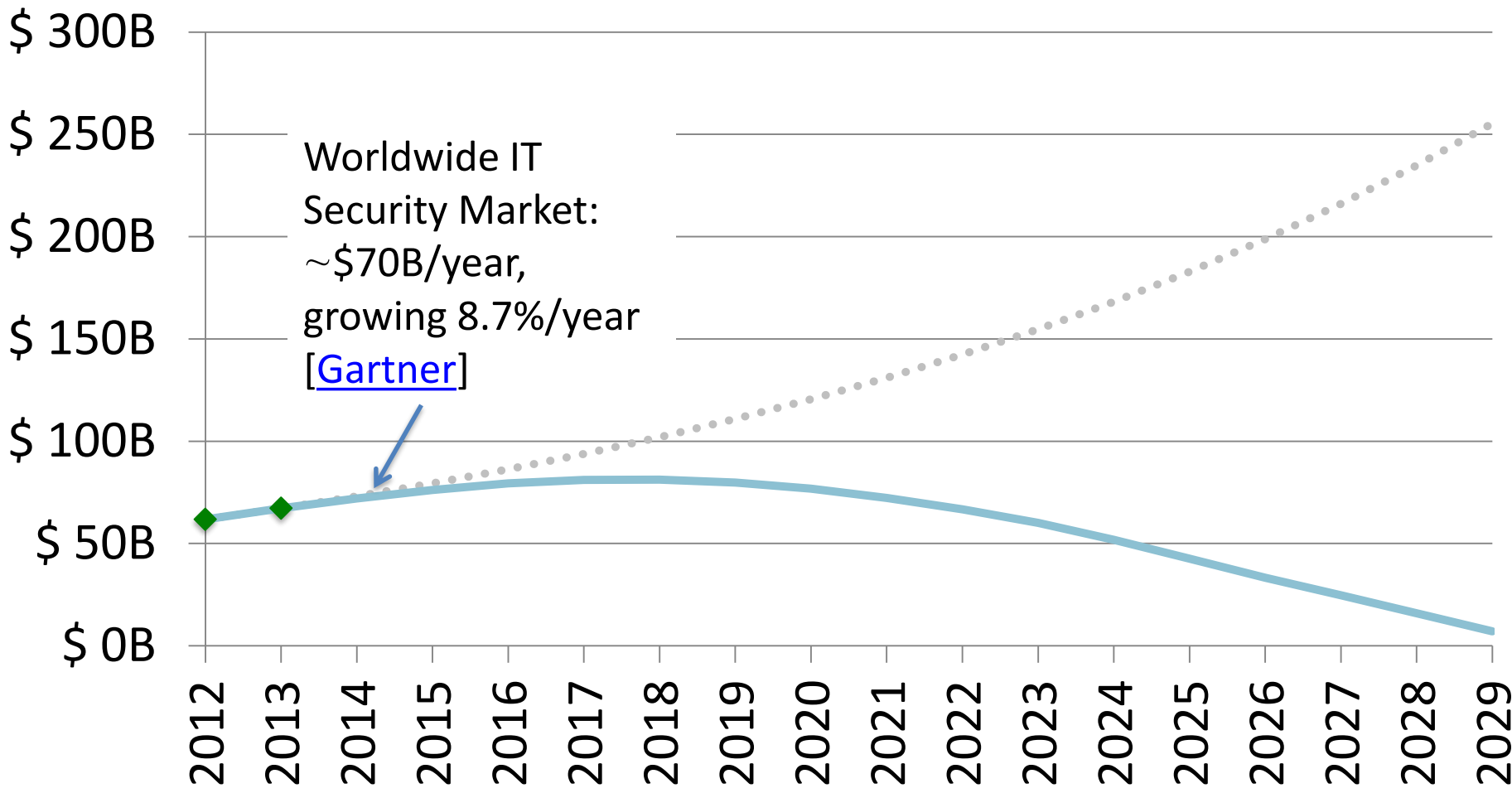
Things that make everyday life better

Where should
multiparty computation
be in 2029?

Claim #1

Secure multi-party computation industry should be bigger than malware industry in 2029.





Claim #2

High cost is no longer the main impediment to widespread use of secure (two-party) computation.

(De)Motivating Application: “Genetic Dating”



Bob



Alice



Genome Compatibility
Protocol

WARNING!
Don't Reproduce

WARNING!
Don't Reproduce

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?

desirable to have a
can be related, and
developed for provi
fundamentally, such
understand the intri
functions. For exam
to answer a questio



Genetic Dating

Millionaires' Problem

1984

1999

New App Prevents Icelanders from Sleeping With their Relatives

Monday, 15 April 2013 06:04 | font size - + | Print | Email



MOST READ TODAY...

Ben Stiller walking around in Icelandic nature

Iceland is the Coolest Place to go on Vacation

Icelandic Goat Trains Dogs

Iceland has signed a free trade agreement with China - First in Europe

Taekwondo: Fight for the gold at the Icelandic Championships 2013 - VIDEO

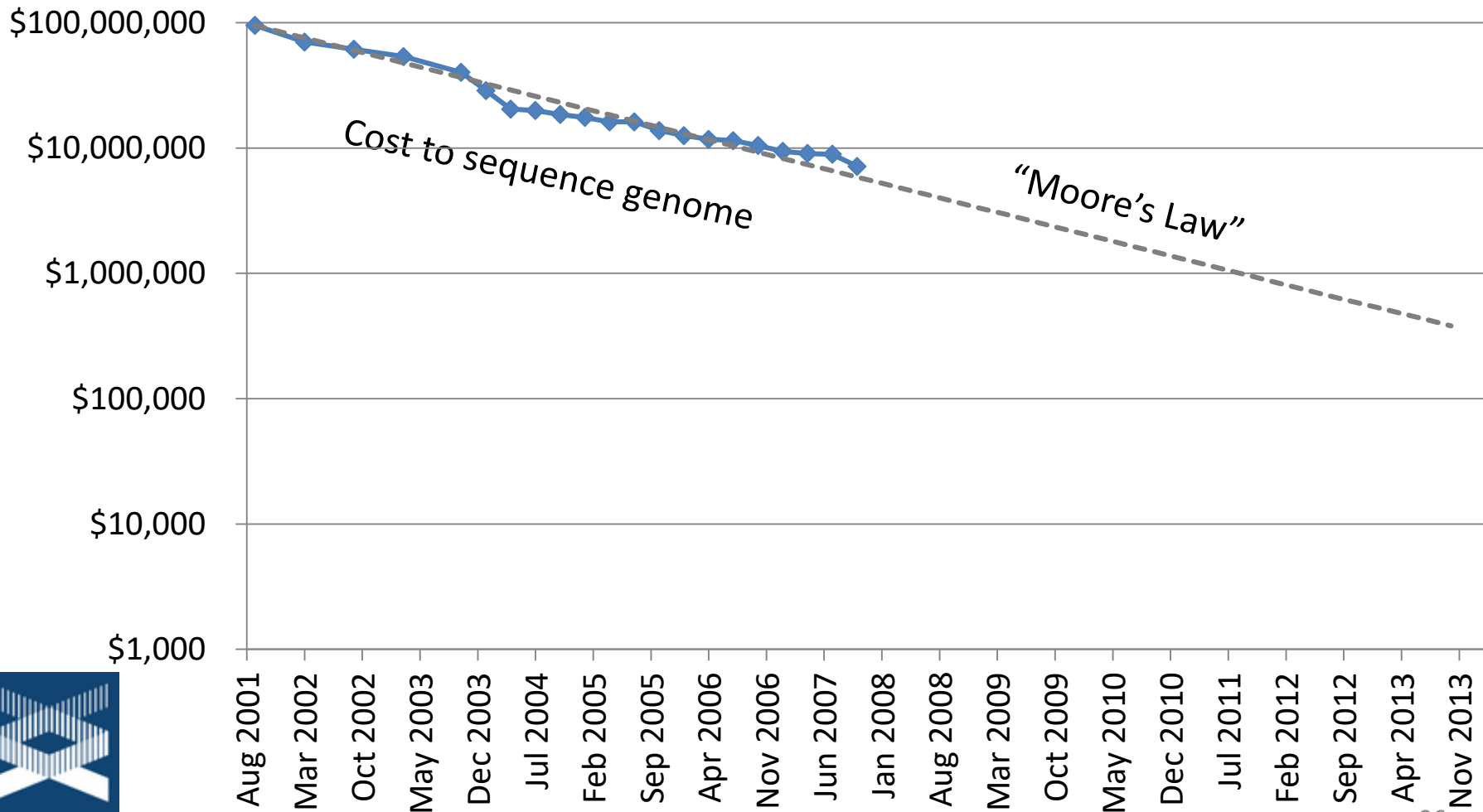
Spotify Finally Available in Iceland

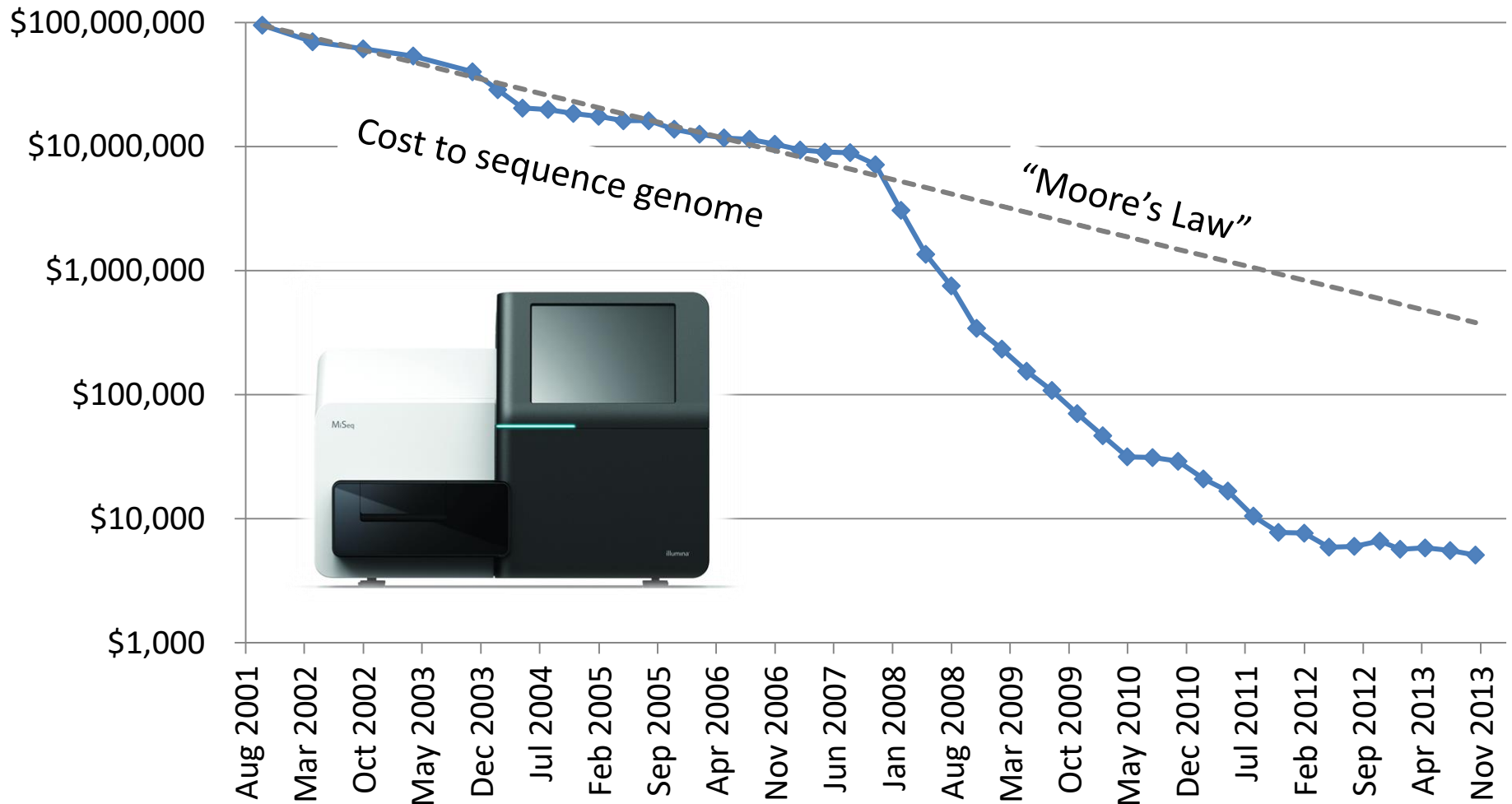


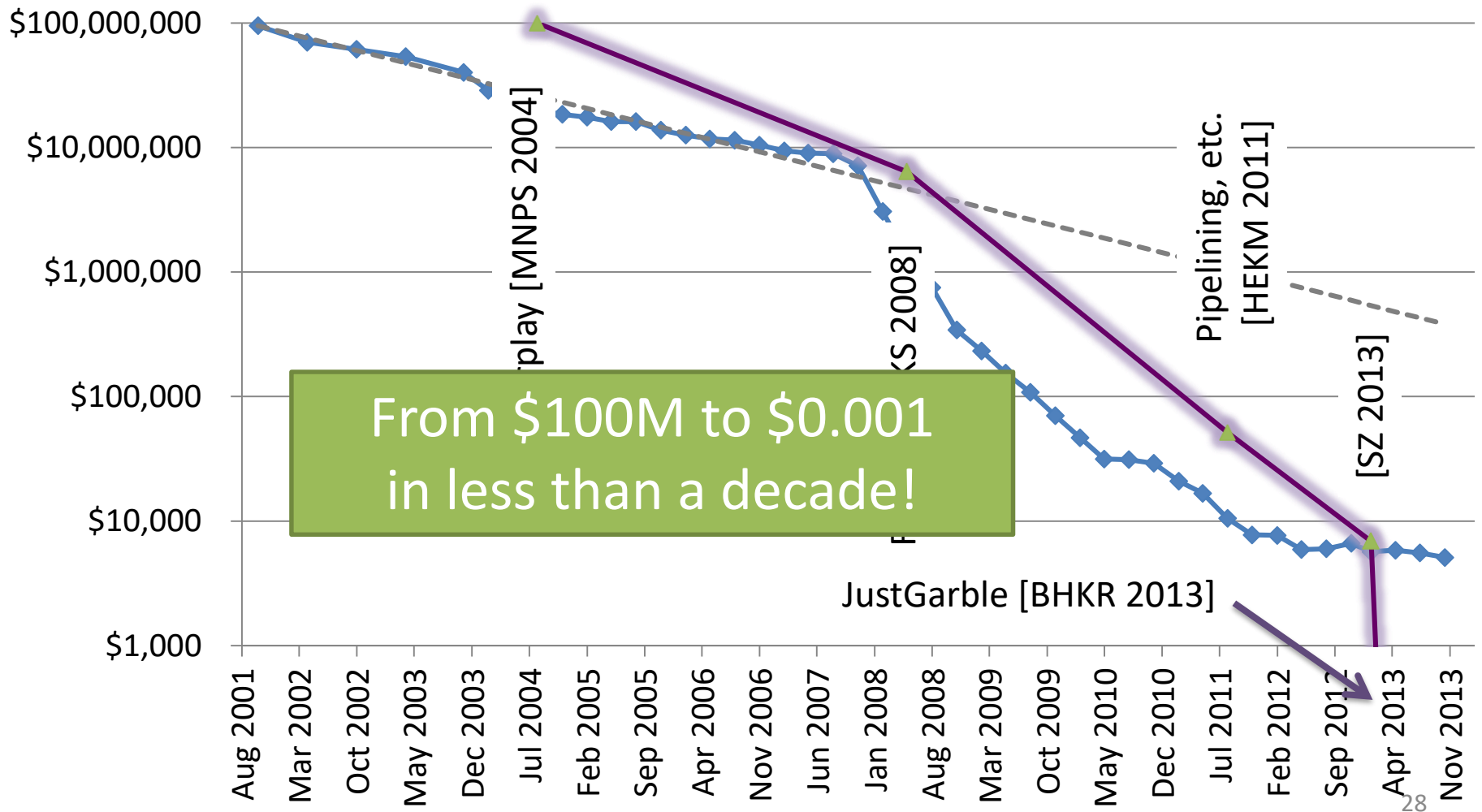
A user commented on the app's website:

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









From \$100M to \$0.001
in less than a decade!

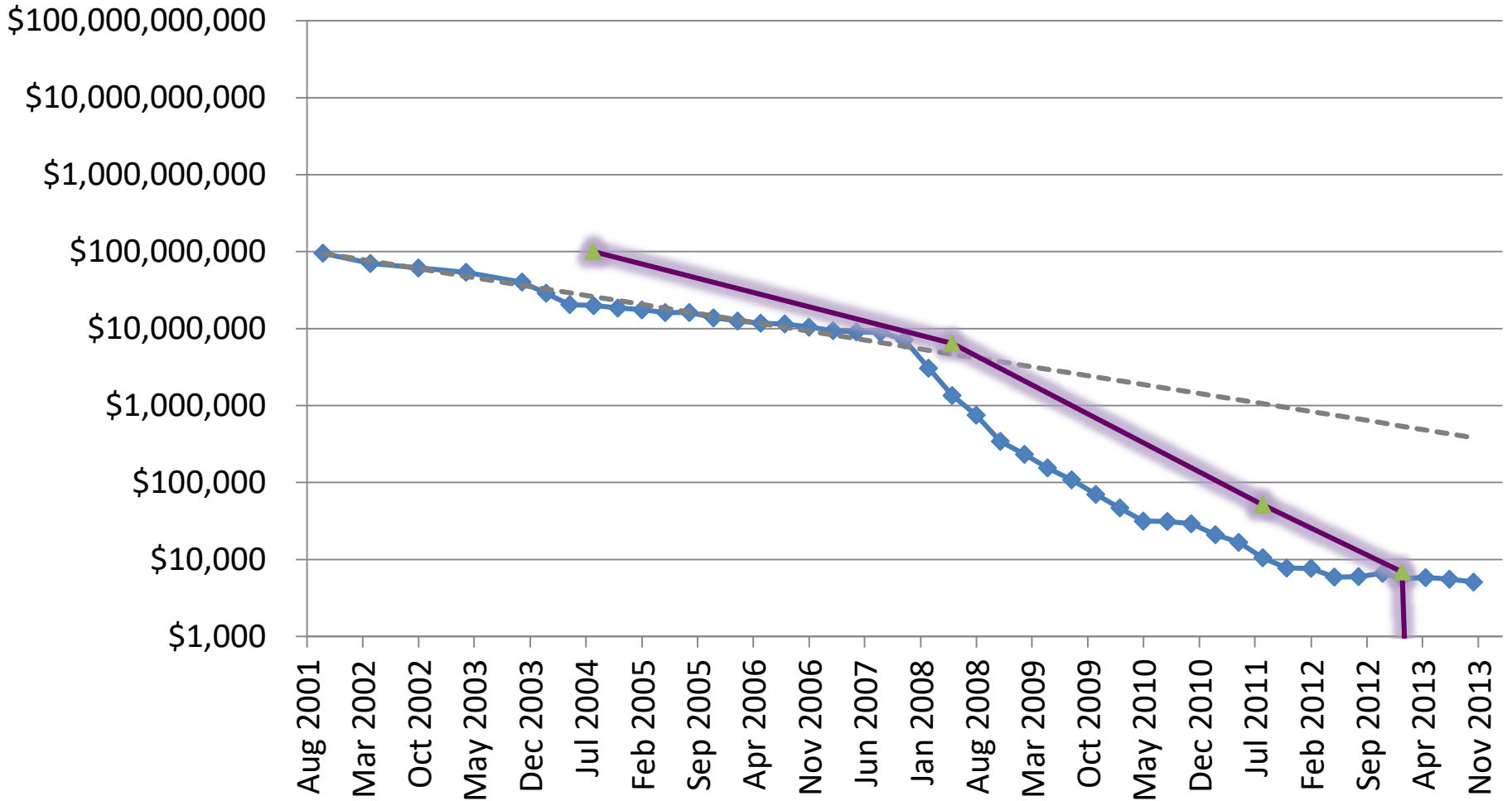
play [MNPS 2004]

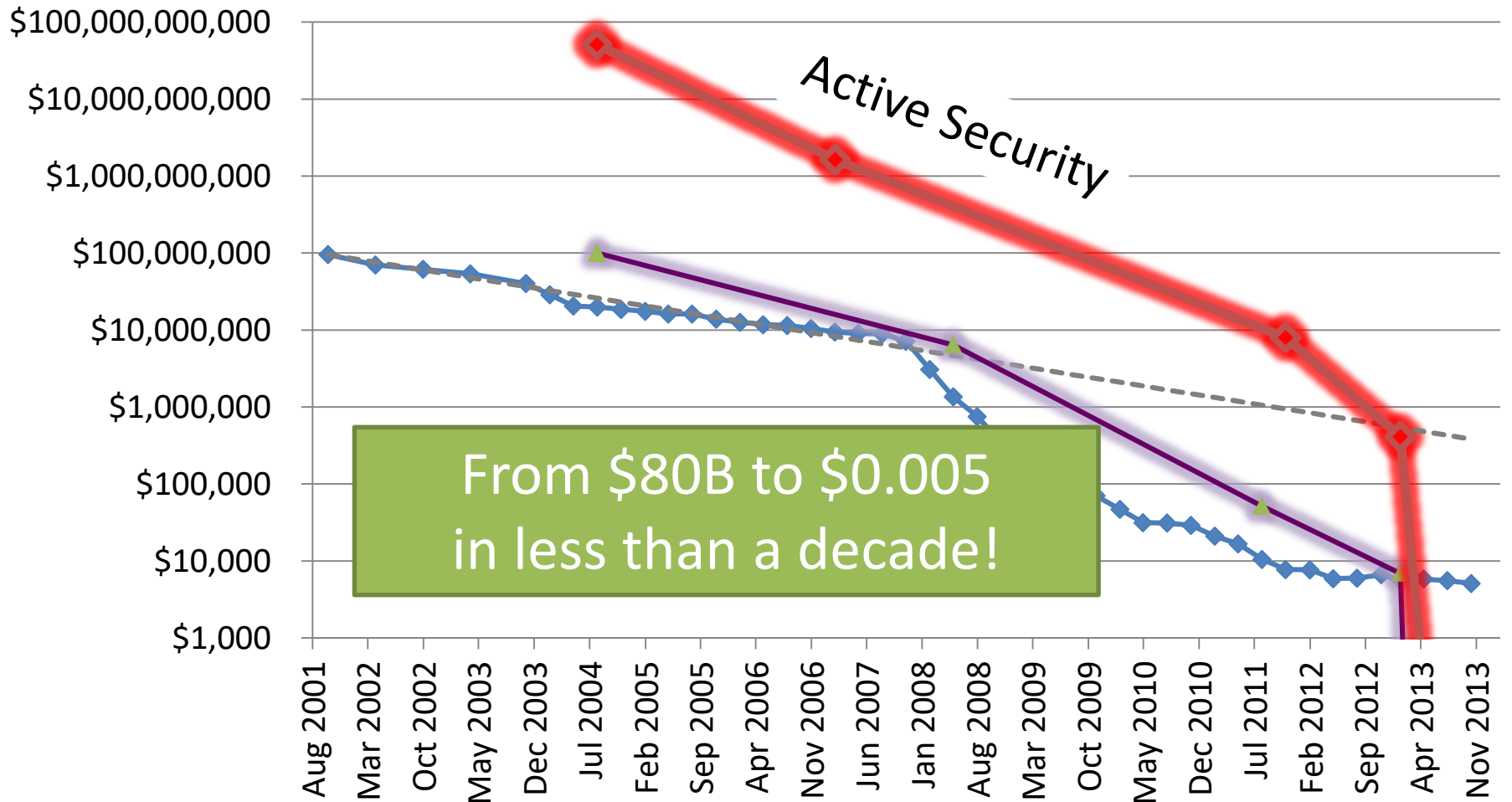
[KS 2008]

Pipelining, etc.
[HEKM 2011]

[SZ 2013]

JustGarble [BHKR 2013]





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 10,000x (?) energy of unencrypted computation

– Data centers today ~ 5 M 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

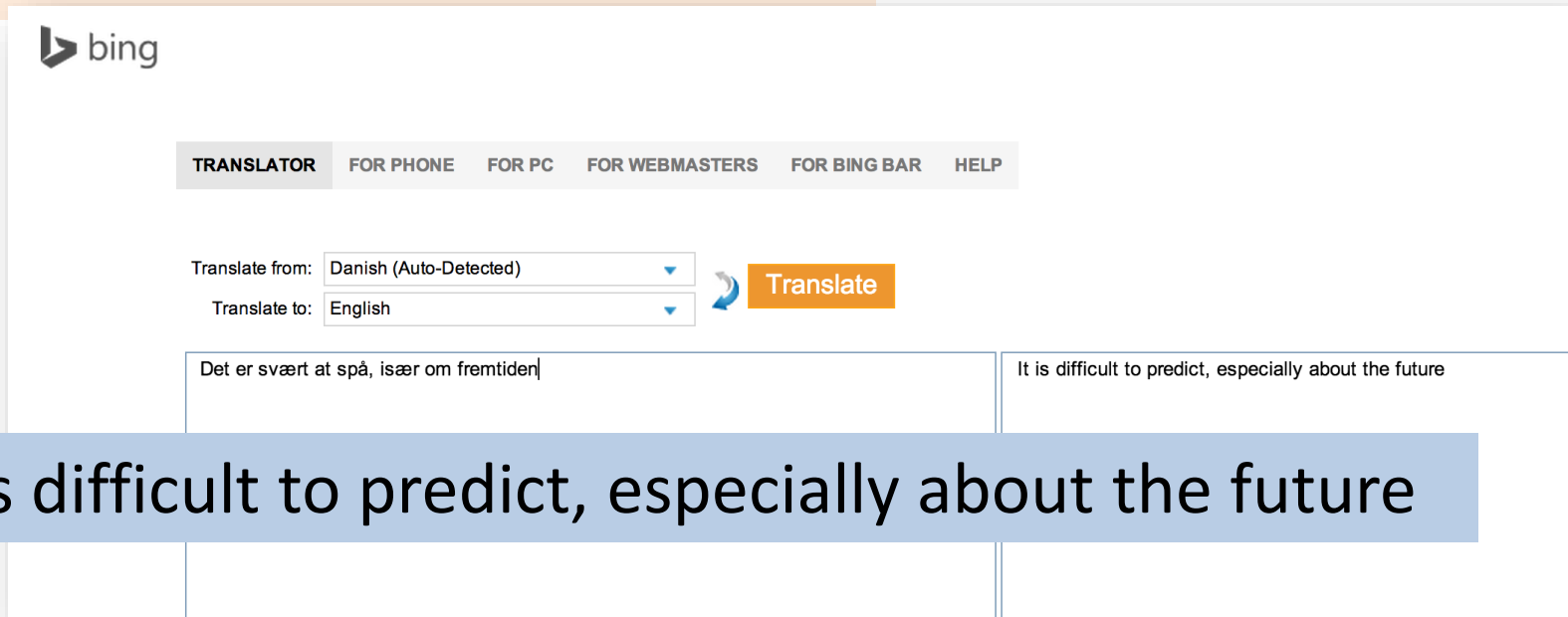
We don't yet know what the "killer app" for MPC is and its probably not privacy.





Det er svært at spå, især om fremtiden.

Robert Storm Petersen



The screenshot shows the Bing Translator interface. At the top left is the Bing logo. Below it is a navigation bar with links: TRANSLATOR, FOR PHONE, FOR PC, FOR WEBMASTERS, FOR BING BAR, and HELP. The main area contains two dropdown menus: 'Translate from: Danish (Auto-Detected)' and 'Translate to: English'. To the right of these is a blue circular arrow icon and an orange 'Translate' button. Below the dropdowns is a text input field containing the Danish sentence 'Det er svært at spå, især om fremtiden'. To the right of this field is the translated English sentence 'It is difficult to predict, especially about the future'.

It is difficult to predict, especially about the future

Theory vs. **Practice**

My New
Theory of Computation
Book!

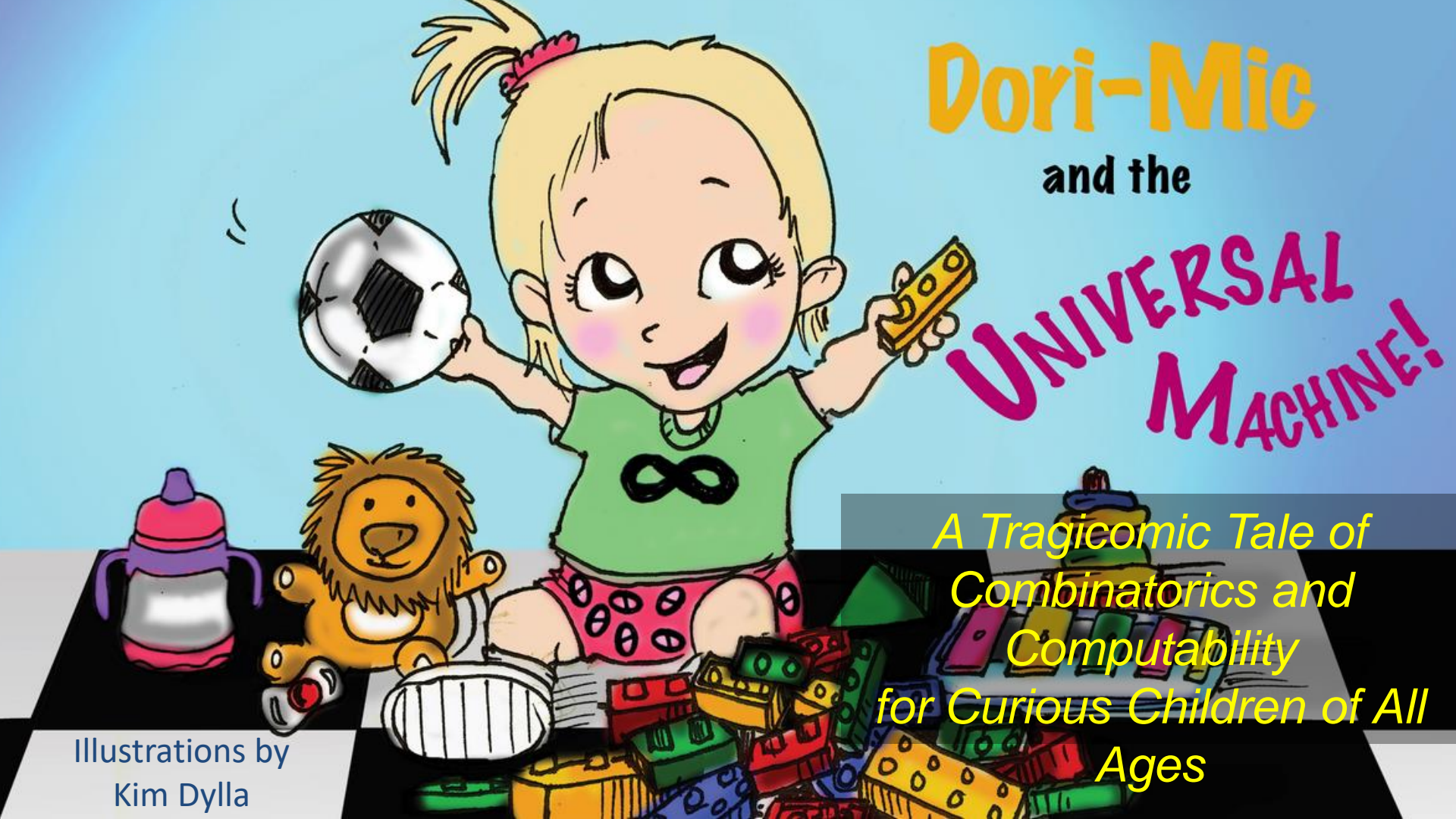
Dori-Mic

and the

UNIVERSAL MACHINE!

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

Illustrations by
Kim Dylla



dori-mic.org

“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**



MiniLEGO [FJNNO 2013]

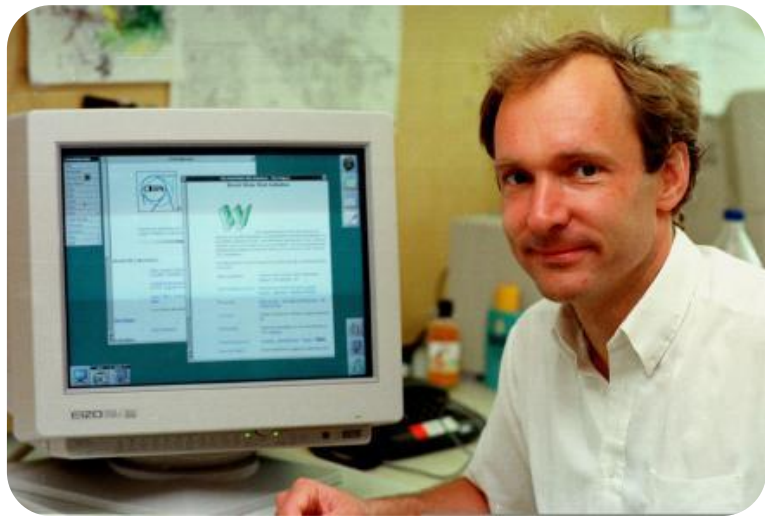
Finding the “killer app” for MPC...



“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

