Living Between the Ideal and Real Worlds

(Or Living Between a Rock and a Hard Place)

Nigel Smart
University Of Bristol

What to talk about?

What to talk about?

“Theory vs Practice” vs “Theory and Practice”

A key problem is someone’s theory is someone else’s practice, and vice versa

And this changes over time.

- Indeed it should.

How to measure Theory and Practice, and all shades in between

- In this talk I will focus (mainly) on the applications of MPC

A common methodology is the Technology Readiness Levels (TRLs)

Technology Readiness Levels

Nine levels TRL 1 to TRL 9.

We take the following few from the DoD definitions

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

Nine levels TRL 1 to TRL 9.

We take the following few from the DoD defi[illegible]ns

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 [illegible] application formulated

In[illegible] principles are observed, practical applications can be in[illegible] speculative, and there may be no proof or detailed [illegible]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 ti Thi includes analytical studies and laboratory studies to physic val 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

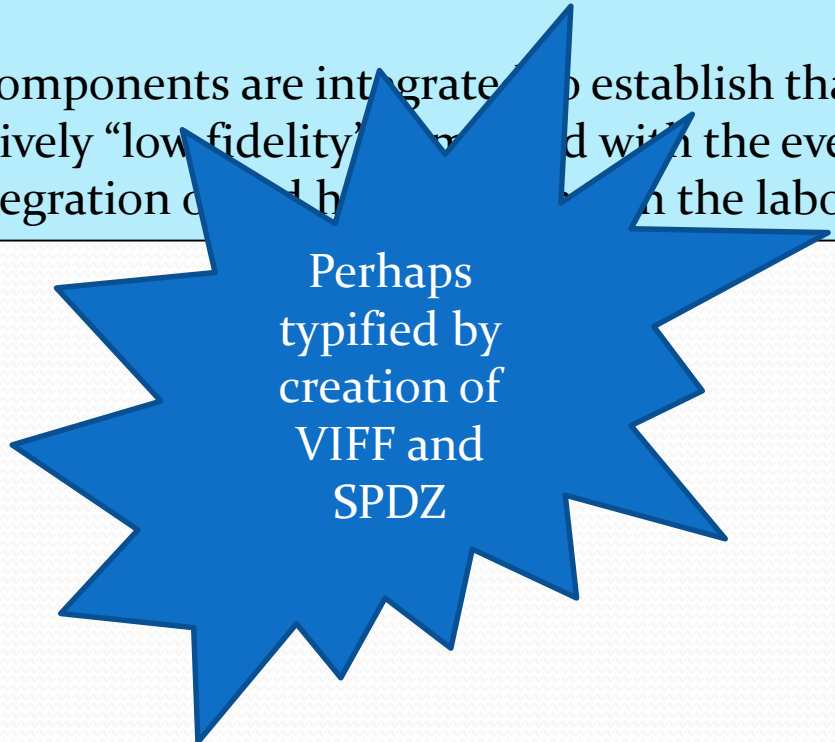
Basic technological components are integrated to establish that they will work together. This is relatively “low fidelity” compared with the eventual system. Examples include integration of “ad hoc” hardware in the laboratory.

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" d wi the eventual system. Examples include integration d b the laboratory.



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.

Technology Readiness Levels

DARPA Brandeis

Cybernetica's ShareMind

Partisia's Auctions

Dyadic's vHSM

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.

Translation

- Moving from the theoretical (Ideal) world to the practical (Real) world is what technology should do
- But that requires research, and venues which support such translational research
- Often this translational work gets rubbished...
  - “Paper does not contain new theoretical ideas”
  - “Paper does not implement something useful to practioners”

Translation

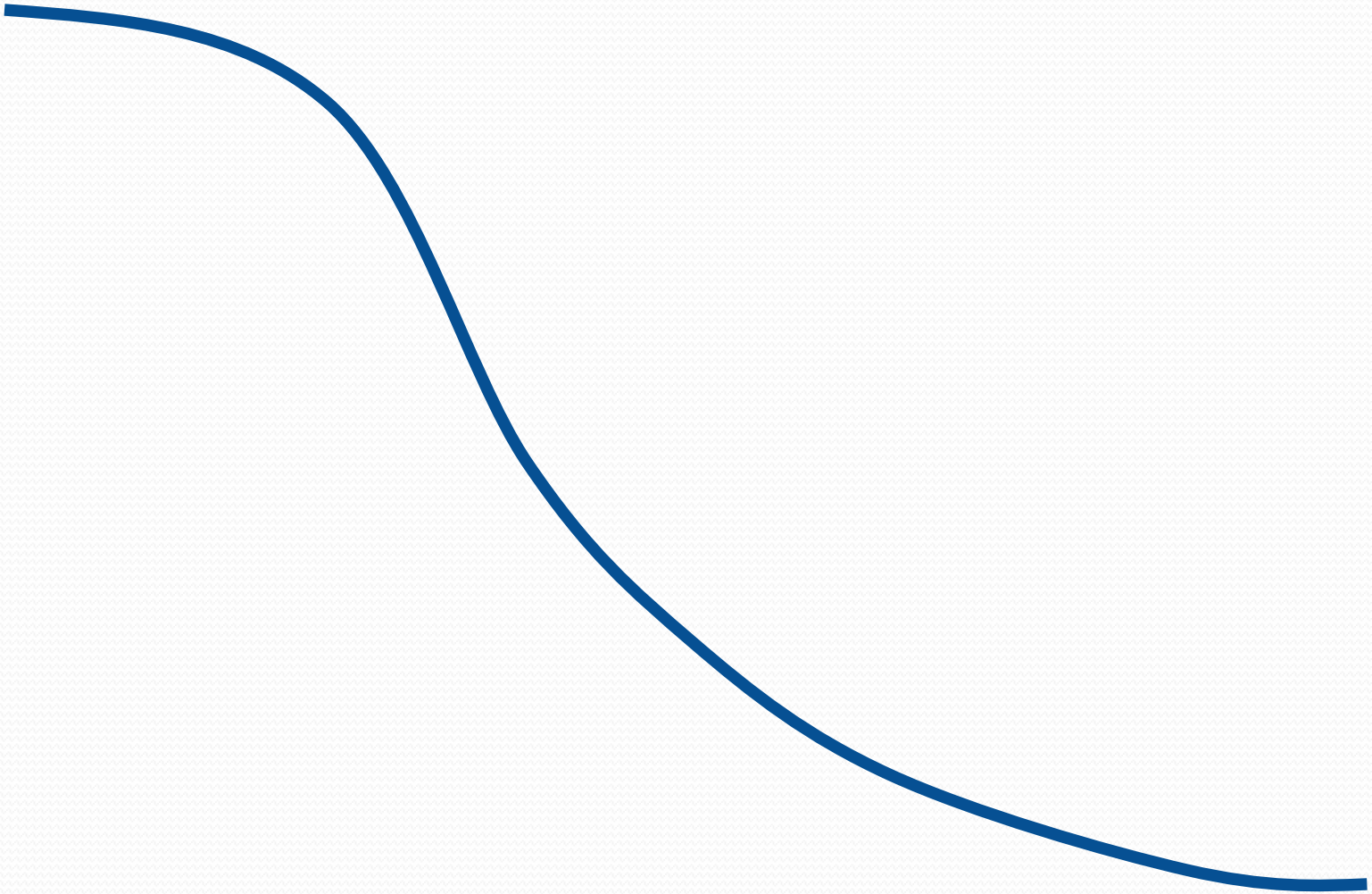
- Moving from the theoretical (Ideal) world to the practical (Real) world is what technology should do
- But that requires research, and venues which support such translational research
- Often this translational work gets rubbished...
  - “Paper does not contain new theoretic
  - “Paper does not implement som

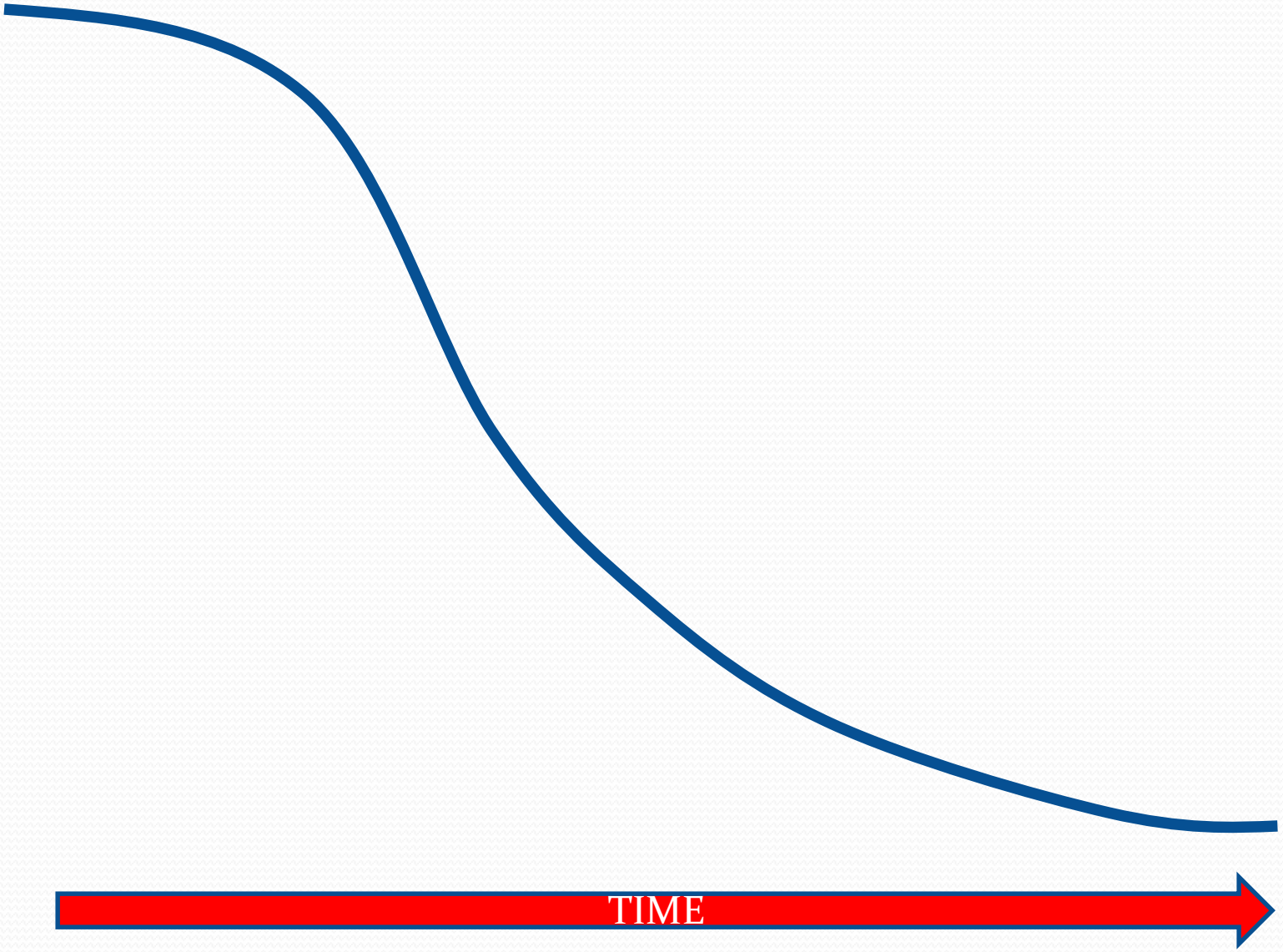
Birch's Curve

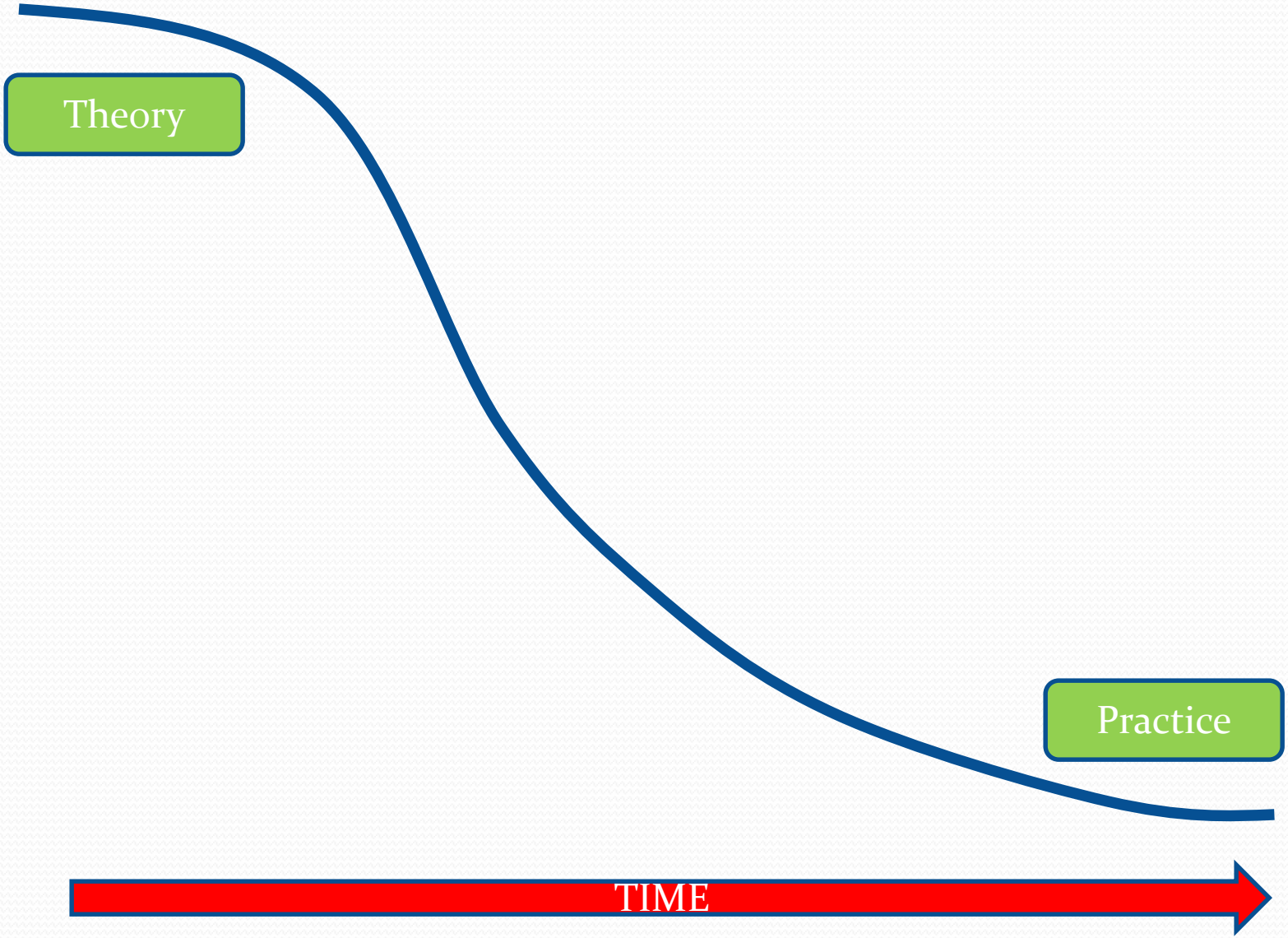
The following curves was introduced to me in an invited talk by Bryan Birch at a meeting around 20 years ago.

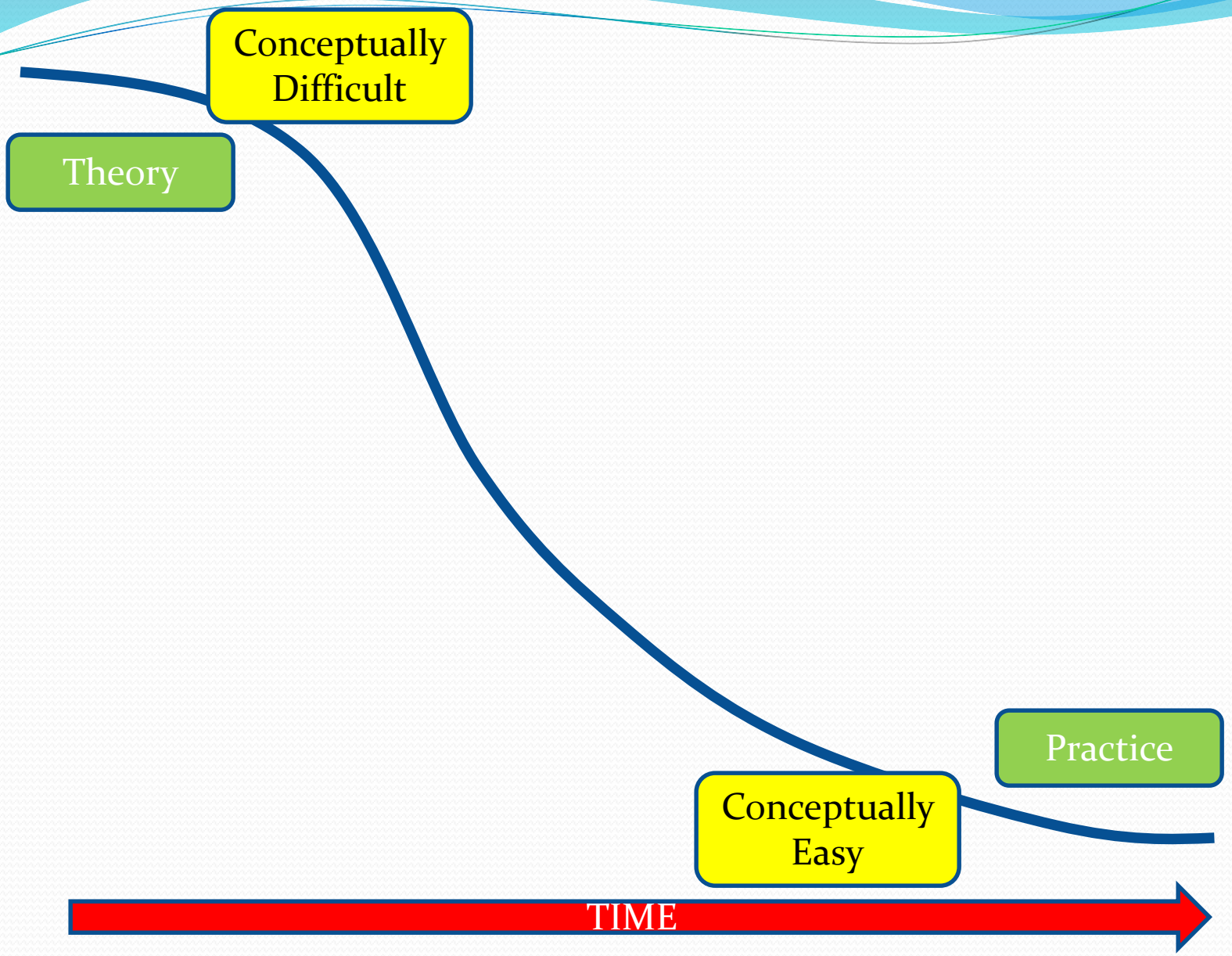
Pretty much captures the progress of technology and where we are

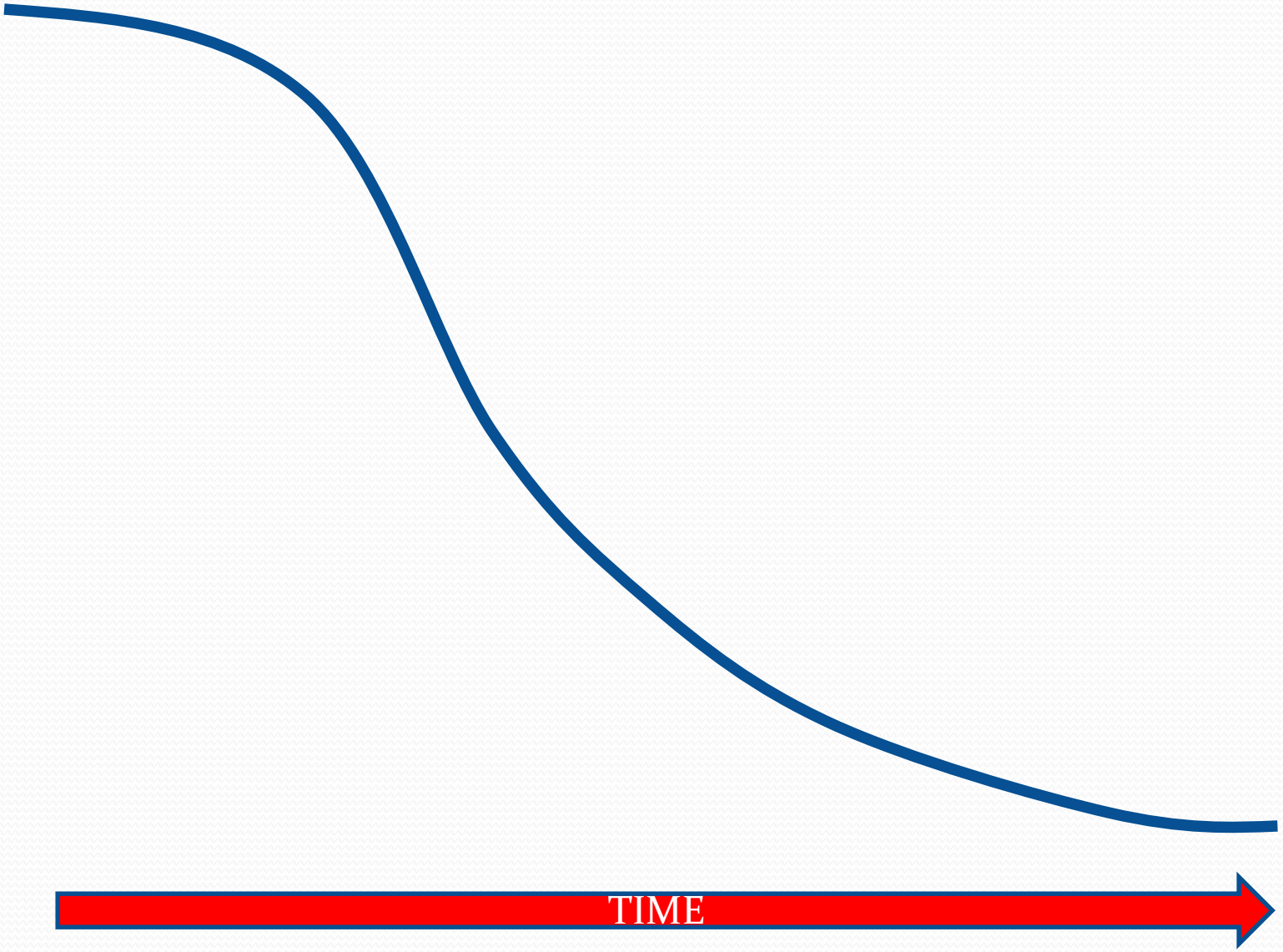
I will use it for the rest of the talk to examine stories of theory to practice from Crypto I have witnessed.

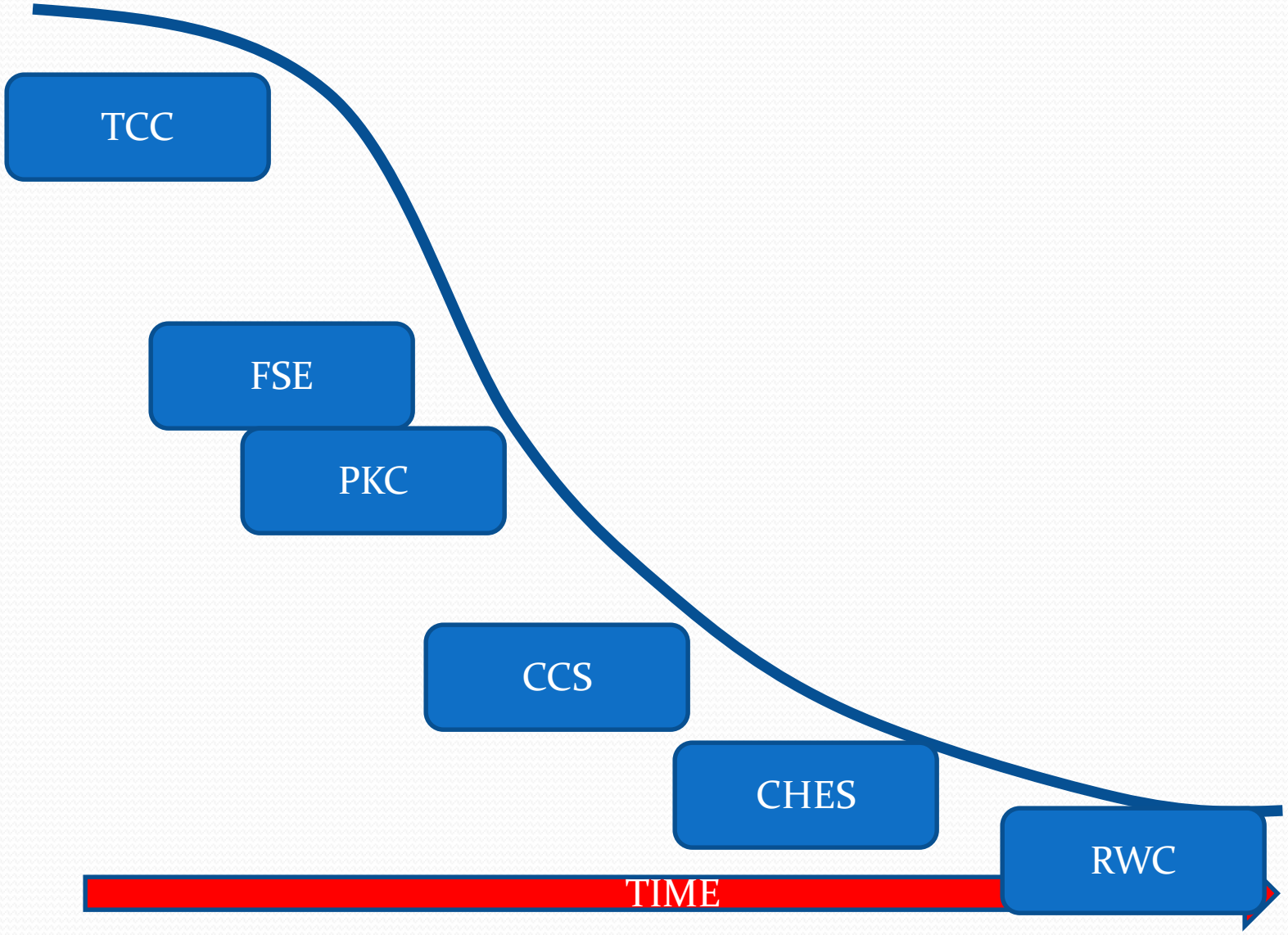


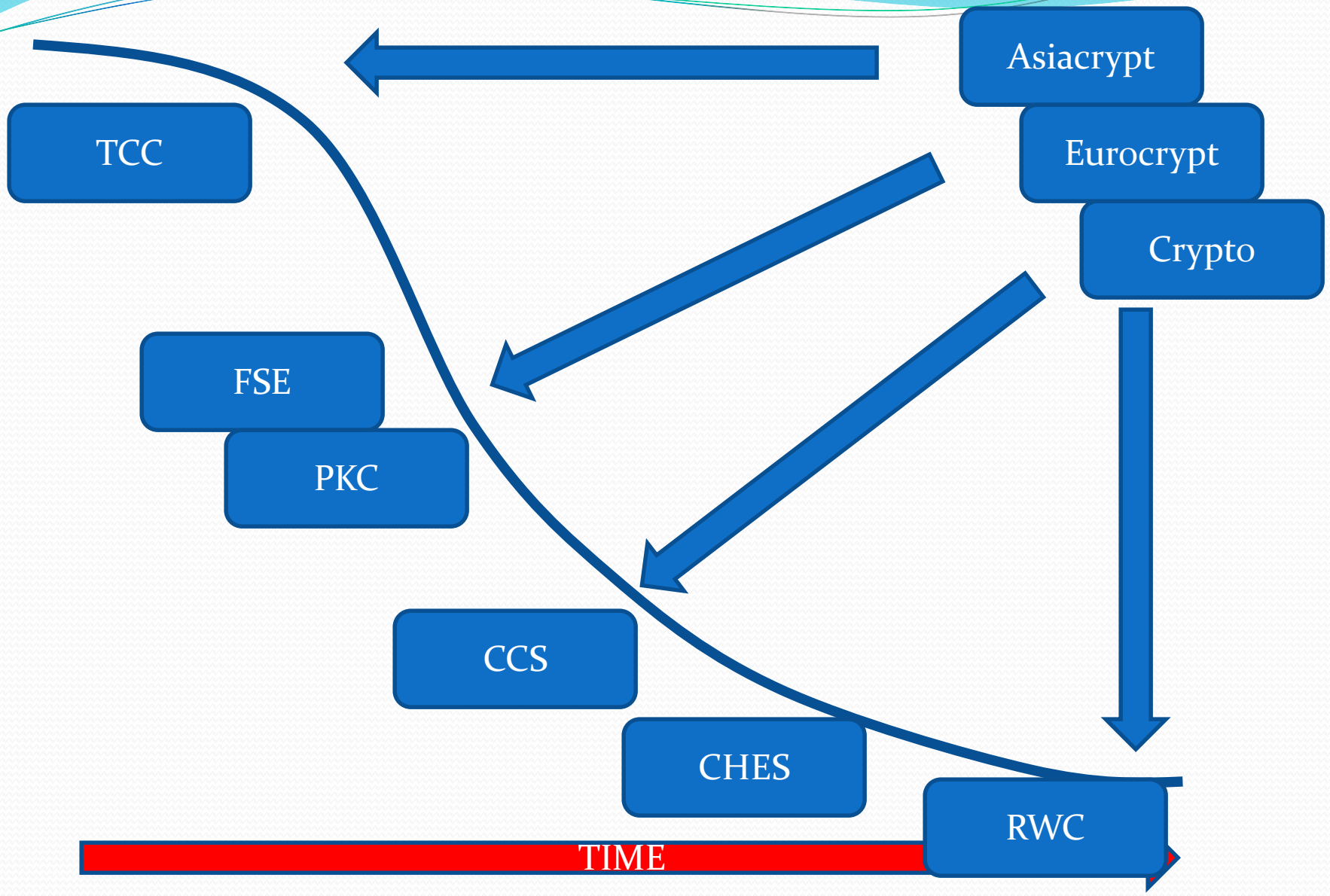

TIME

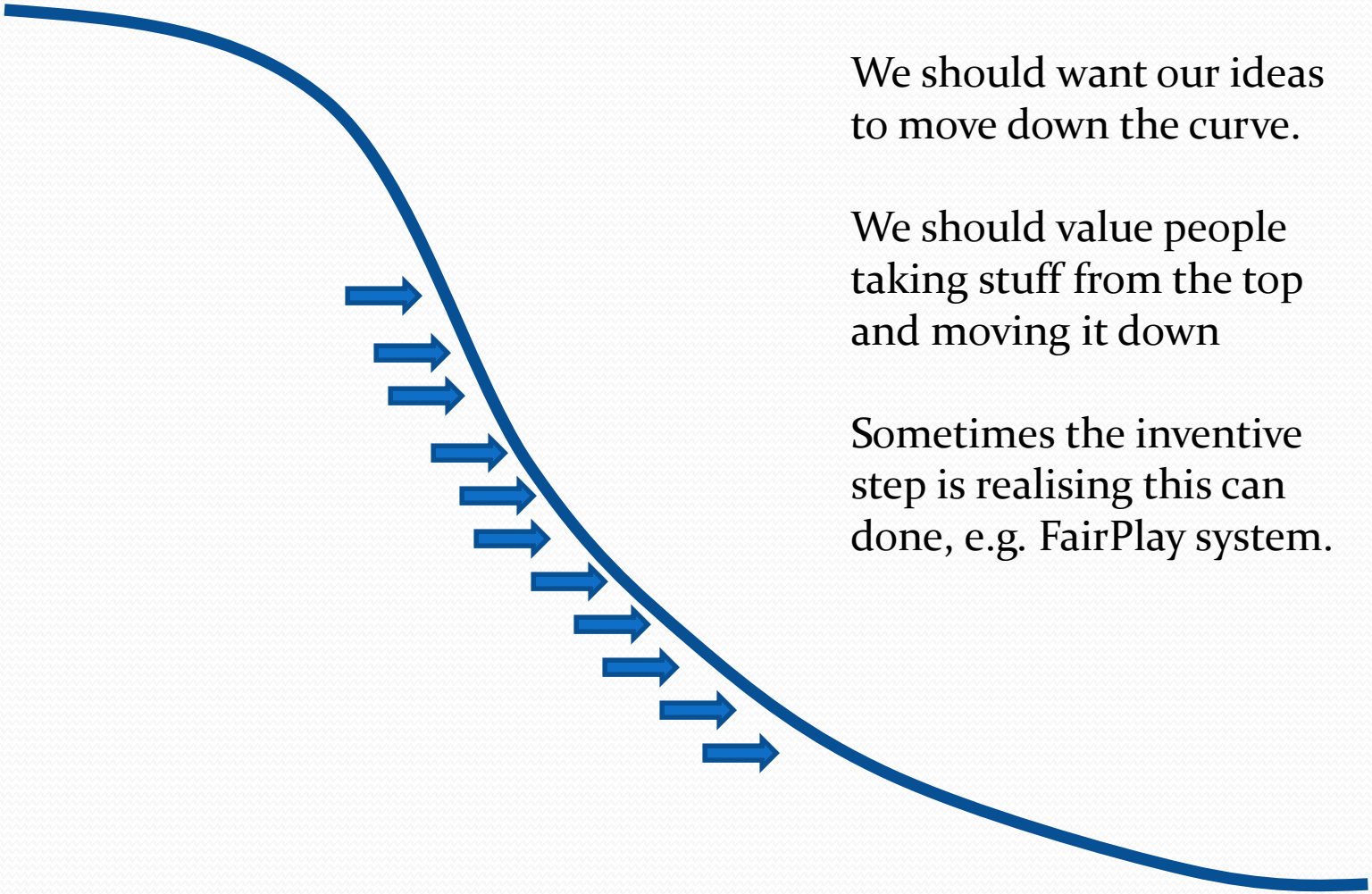

Theory
Practice
TIME


Conceptually Difficult
Theory
Practice
Conceptually Easy
TIME


TIME


TCC
FSE
PKC
CCS
CHES
RWC
TIME

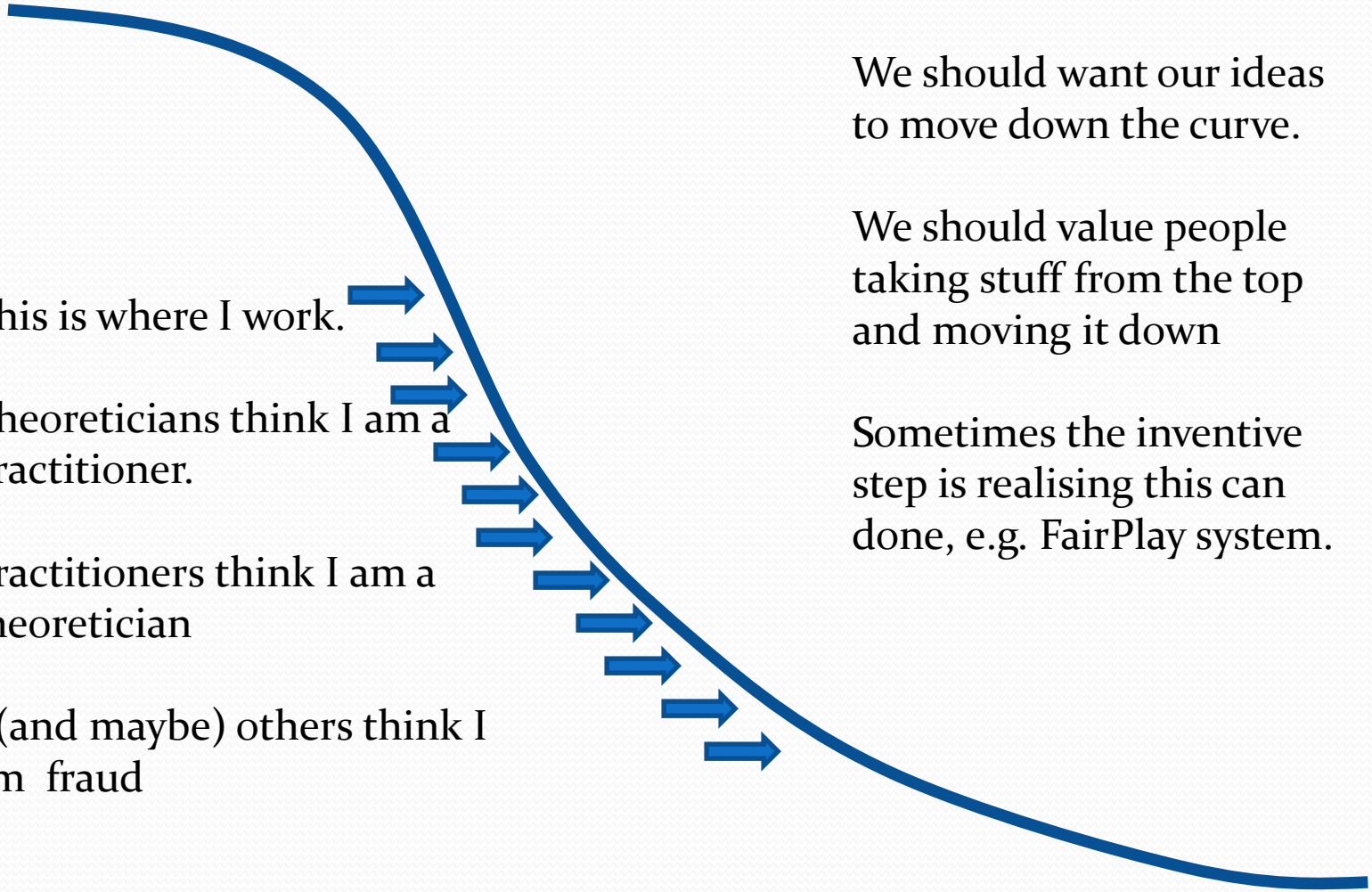

Asiacrypt
Eurocrypt
Crypto
TCC
FSE
PKC
CCS
CHES
RWC
TIME



We should want our ideas to move down the curve.

We should value people taking stuff from the top and moving it down

Sometimes the inventive step is realising this can done, e.g. FairPlay system.



This is where I work.

Theoreticians think I am a practitioner.

Practitioners think I am a theoretician

I (and maybe) others think I am fraud

We should want our ideas to move down the curve.

We should value people taking stuff from the top and moving it down

Sometimes the inventive step is realising this can done, e.g. FairPlay system.

Case Studies

I will now look at some case studies of from my career of moving stuff down the curve, and where I think the breakthroughs/great ideas came from.

How/why did we drive theory to practice?

How did the Ideal become Real?

- S-Unit Equations
- ECDLP
- Fully Homomorphic Encryption
- Multi Party Computation

I am not a cryptographer.....

The first stuff I did was working on finding algorithms to solve equations such as

$$\eta_1^{a_1}\eta_2^{a_2}\ldots.\eta_n^{a_n}+\eta_1^{b_1}\eta_2^{b_2}\ldots.\eta_n^{b_n}=1$$

Where η_i are elements in some number field.

Previously only considered in theory, but have “applications” in solving various problems in number theory

I am not a cryptographer.....

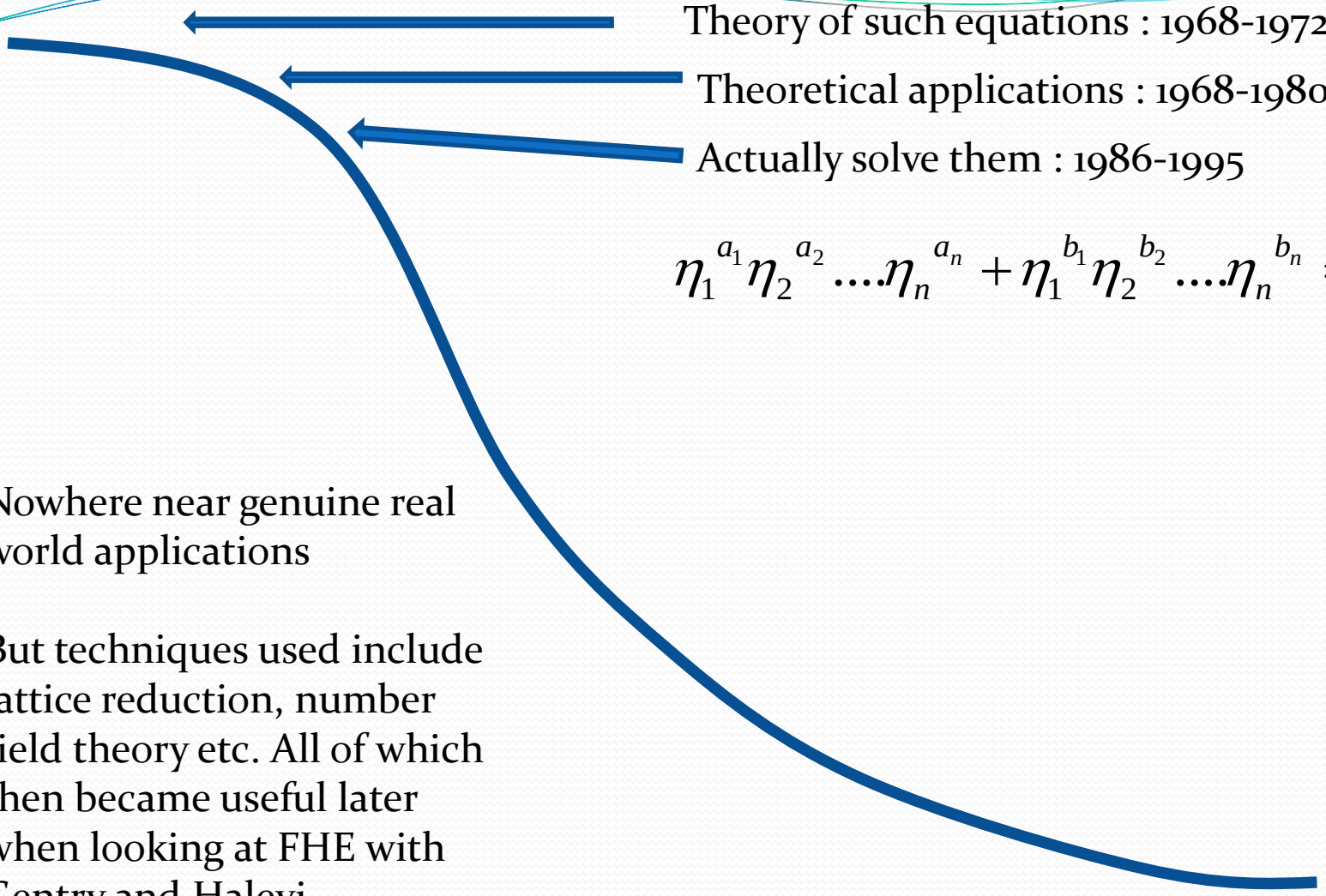
The first stuff I did was working on finding algorithms to solve equations such as

$$\eta_1^{a_1}\eta_2^{a_2}\ldots\eta_n^{a_n}+\eta_1^{b_1}\eta_2^{b_2}\ldots\eta_n^{b}=1$$

Where η_i are elements in some num

Previously only considered in theory, but ving various problems in number theory

Recall: One persons practice is another persons theory



Theory of such equations : 1968-1972

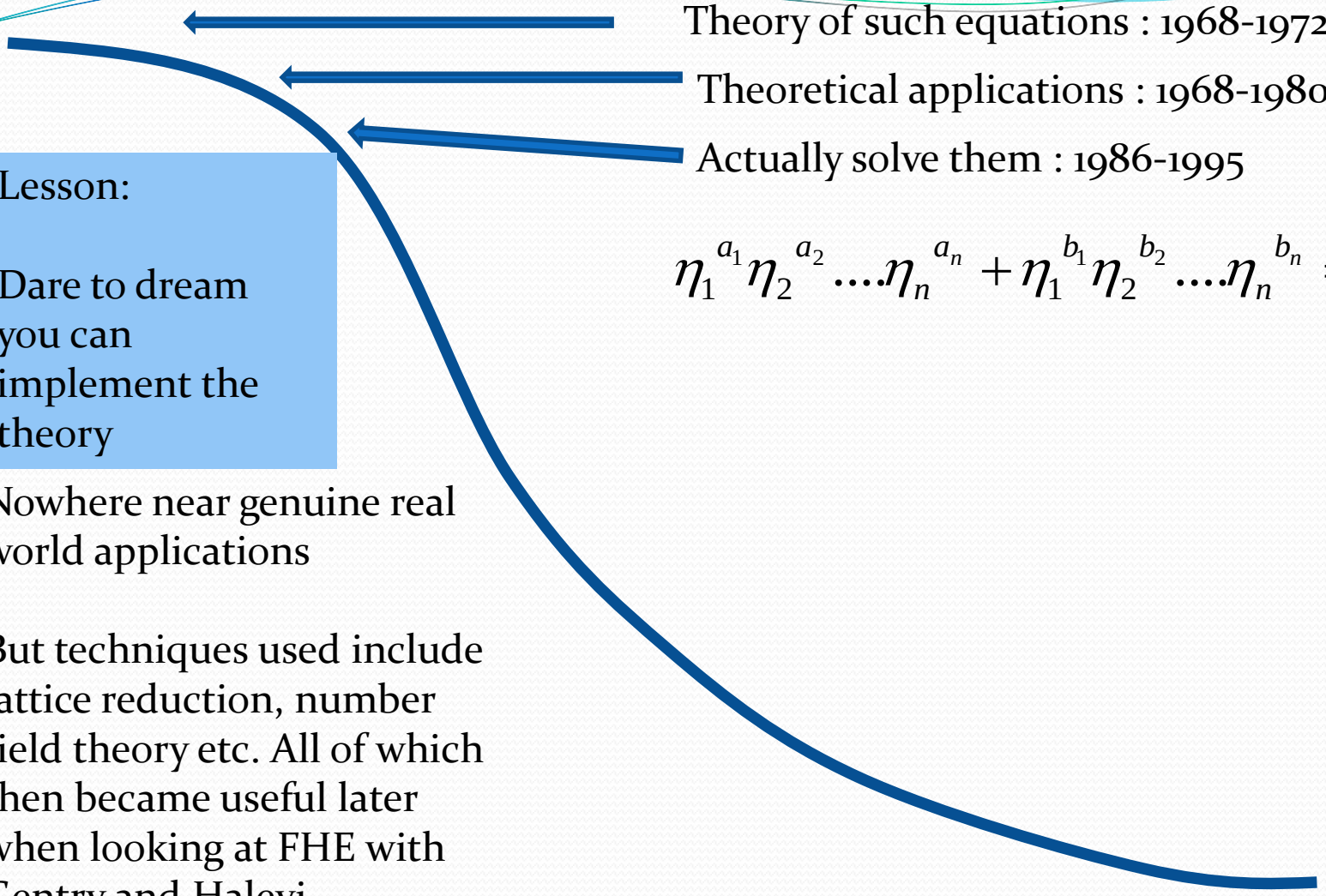
Theoretical applications : 1968-1980

Actually solve them : 1986-1995

$$\eta_1^{a_1}\eta_2^{a_2}....\eta_n^{a_n} + \eta_1^{b_1}\eta_2^{b_2}....\eta_n^{b_n} = 1$$

Nowhere near genuine real world applications

But techniques used include lattice reduction, number field theory etc. All of which then became useful later when looking at FHE with Gentry and Halevi.



Theory of such equations : 1968-1972

Theoretical applications : 1968-1980

Actually solve them : 1986-1995

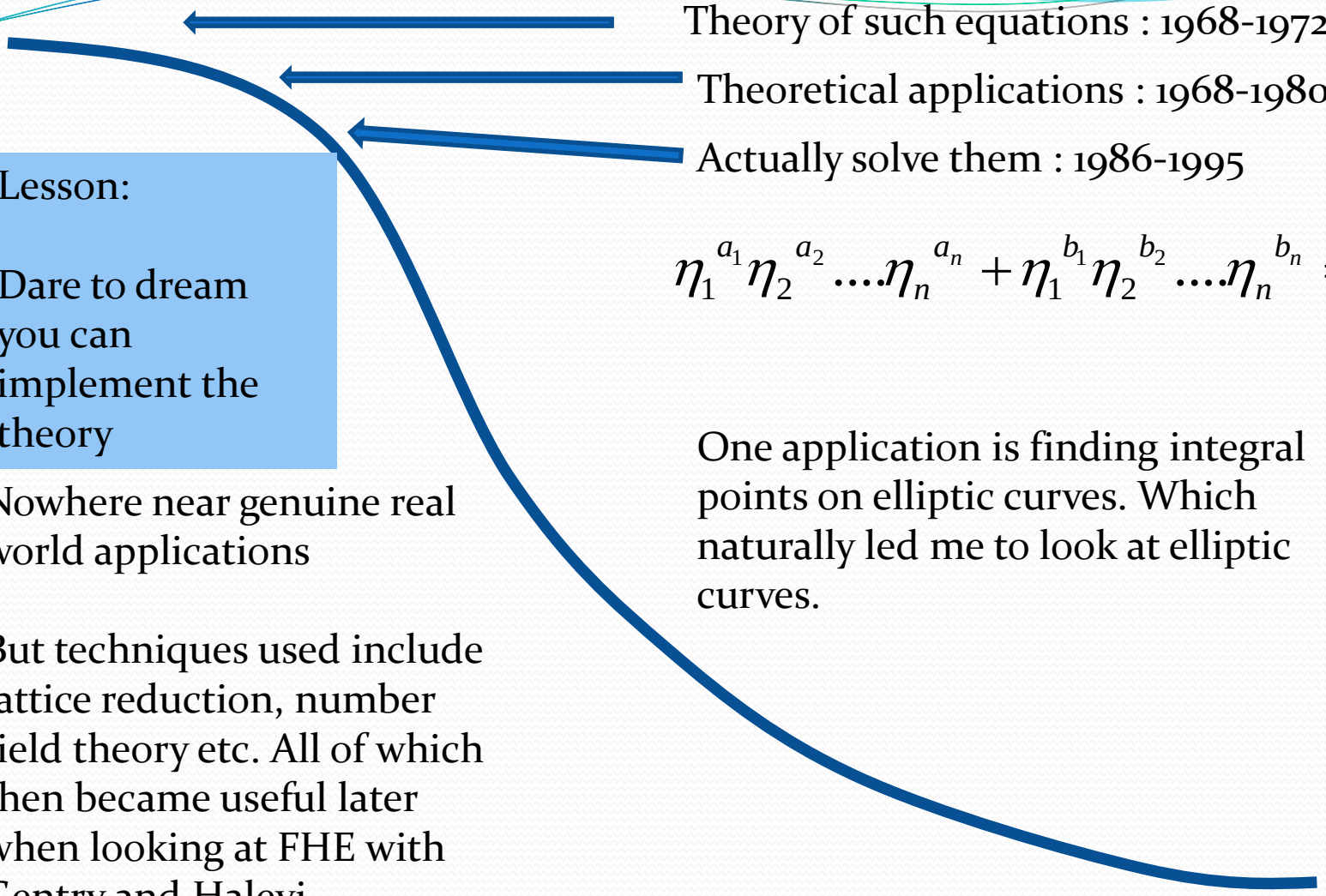
$$\eta_1^{a_1}\eta_2^{a_2}....\eta_n^{a_n} + \eta_1^{b_1}\eta_2^{b_2}....\eta_n^{b_n} = 1$$

Lesson:

Dare to dream you can implement the theory

Nowhere near genuine real world applications

But techniques used include lattice reduction, number field theory etc. All of which then became useful later when looking at FHE with Gentry and Halevi.



Theory of such equations : 1968-1972

Theoretical applications : 1968-1980

Actually solve them : 1986-1995

$$\eta_1^{a_1}\eta_2^{a_2}\ldots\eta_n^{a_n}+\eta_1^{b_1}\eta_2^{b_2}\ldots\eta_n^{b_n}=1$$

Lesson:

Dare to dream you can implement the theory

Nowhere near genuine real world applications

But techniques used include lattice reduction, number field theory etc. All of which then became useful later when looking at FHE with Gentry and Halevi.

One application is finding integral points on elliptic curves. Which naturally led me to look at elliptic curves.

How to become a cryptographer....

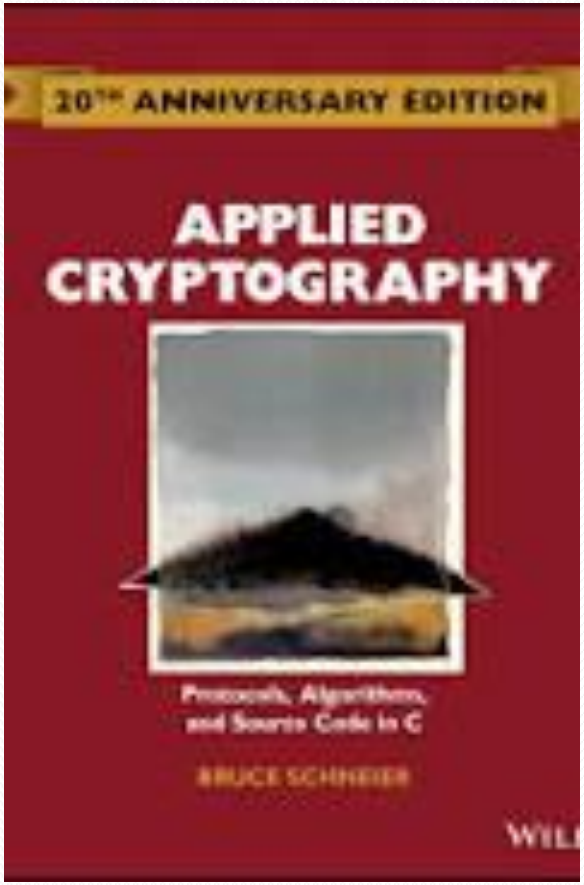
Blag through an interview for HP

But how do you blag with zero knowledge....

How to become a cryptographer....

Blag through an interview for HP

But how do you blag with zero knowledge....



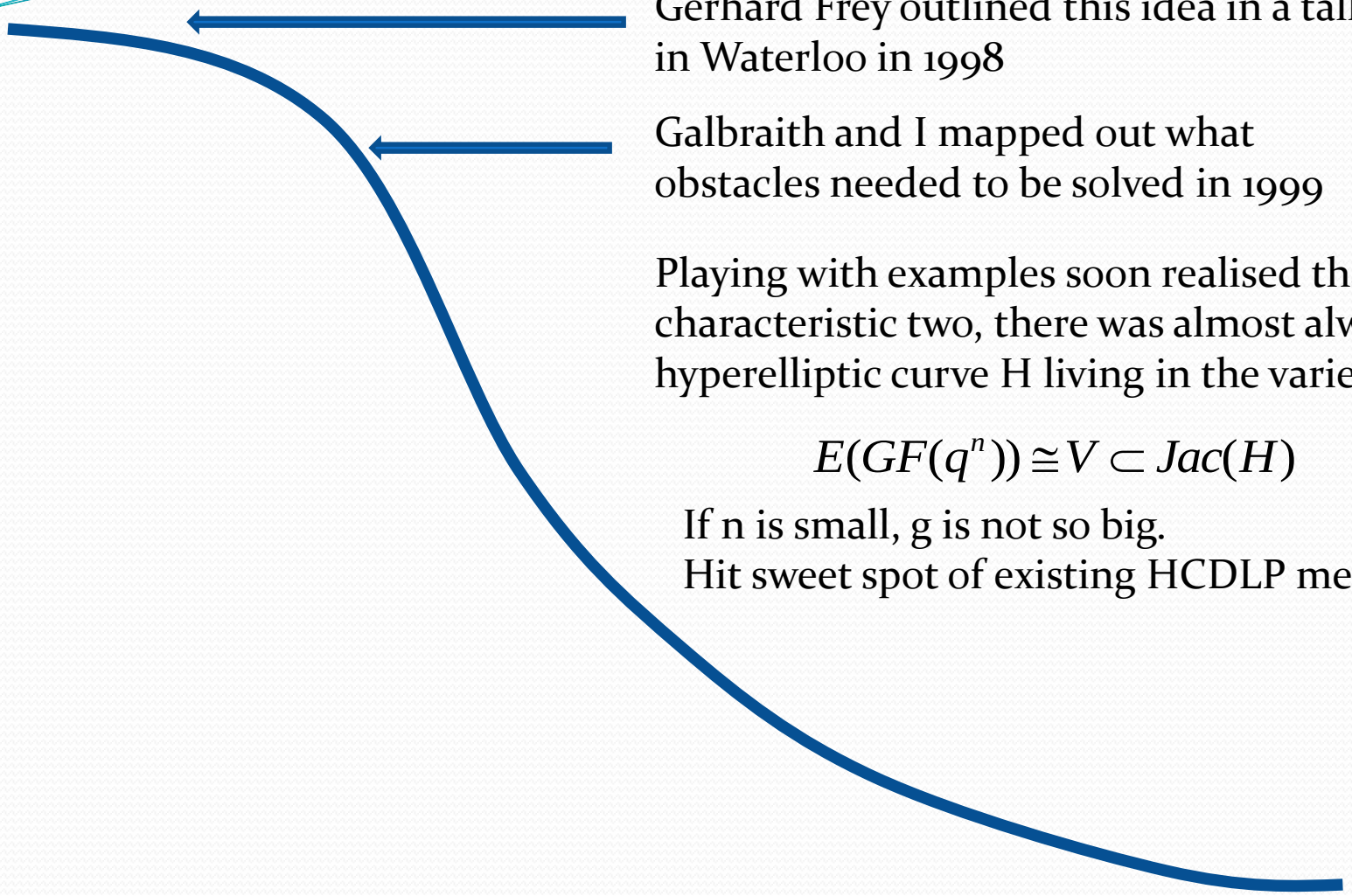
ECDLP

Major work was on the method of Weil Descent for attacking the ECDLP.

- This is now old news so perhaps worth a recap for the youngsters...

Want to solve ECDLP on $E(GF(q^n))$ for some q and n.

- Instead of one equation in two unknowns (X,Y) over $GF(q^n)$ think of this as n equations in 2n unknowns over GF(q)
- It is still a group, i.e. an algebraic variety V
- So it is a sub-variety of a Jacobian of a higher genus curve J(C)
- We know how to solve in sub-exp time a DLP in a Jacobian of a high genus curve. Sub-exp in q^g
- If we could find the curve, maybe the genus is small enough so this is practical method of attack.



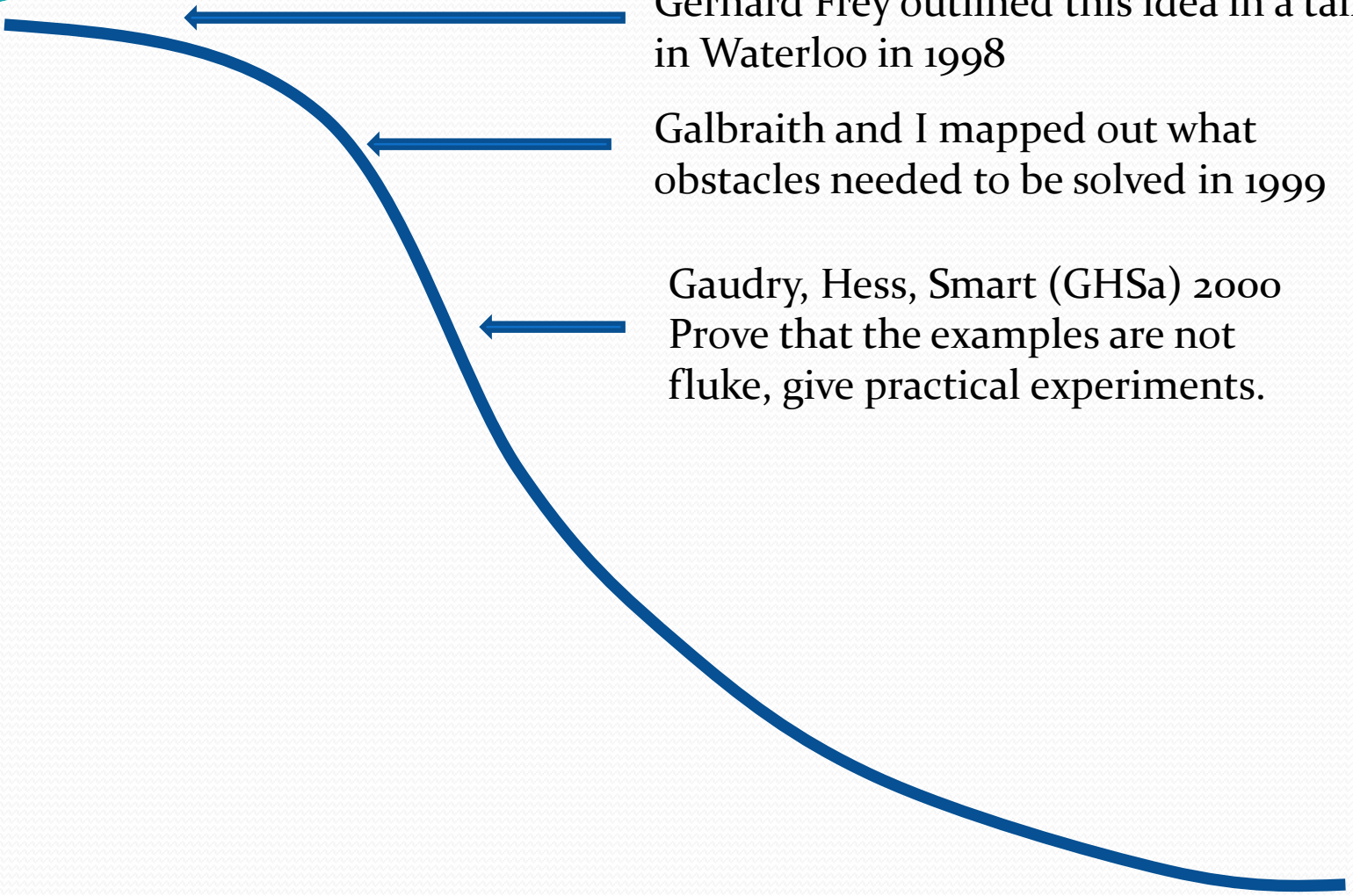
Gerhard Frey outlined this idea in a talk in Waterloo in 1998

Galbraith and I mapped out what obstacles needed to be solved in 1999

Playing with examples soon realised that in characteristic two, there was almost always a hyperelliptic curve H living in the variety V.

$$E(GF(q^n)) \cong V \subset Jac(H)$$

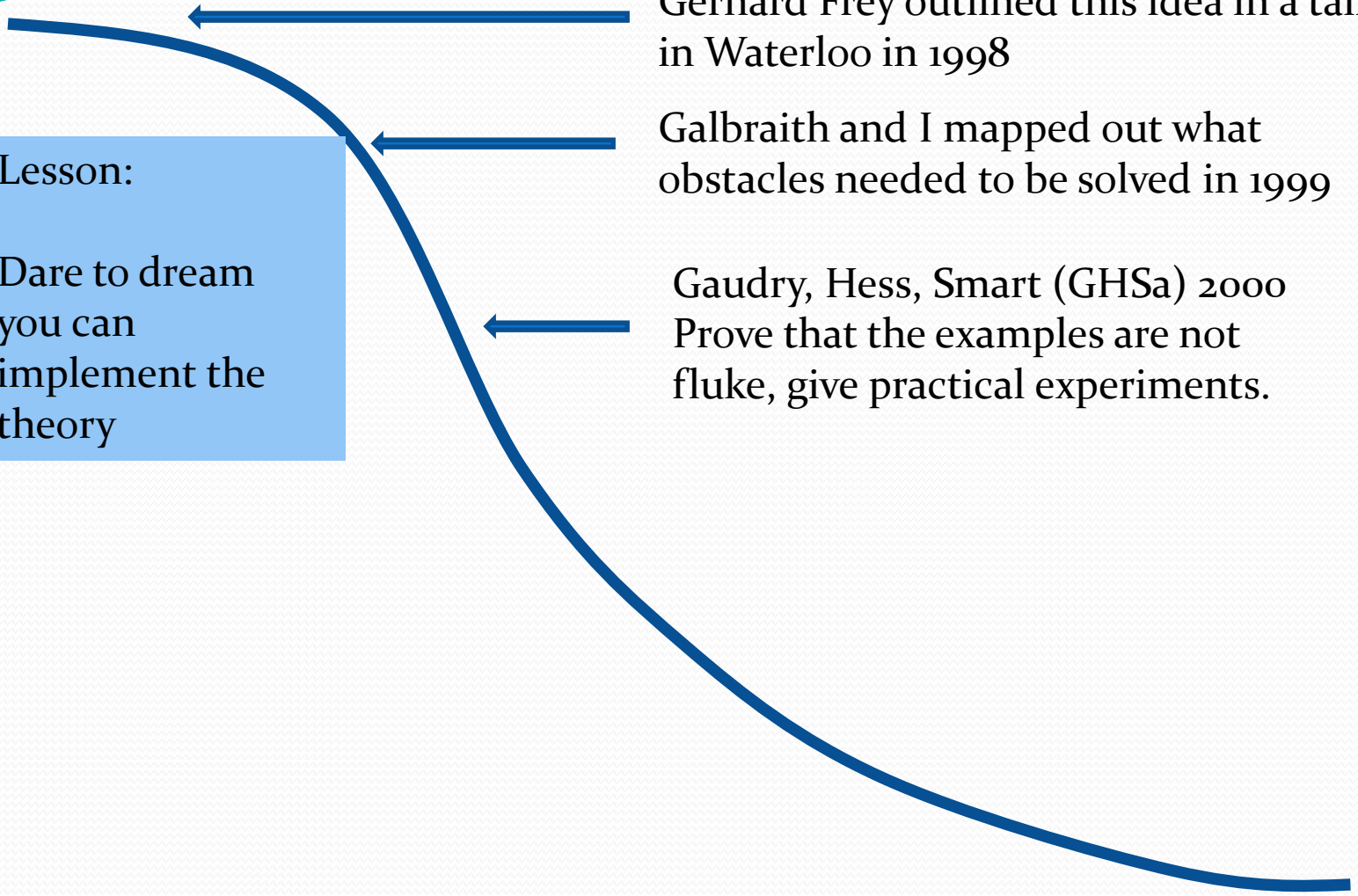
If n is small, g is not so big.
Hit sweet spot of existing HCDLP methods



Gerhard Frey outlined this idea in a talk in Waterloo in 1998

Galbraith and I mapped out what obstacles needed to be solved in 1999

Gaudry, Hess, Smart (GHSa) 2000
Prove that the examples are not fluke, give practical experiments.



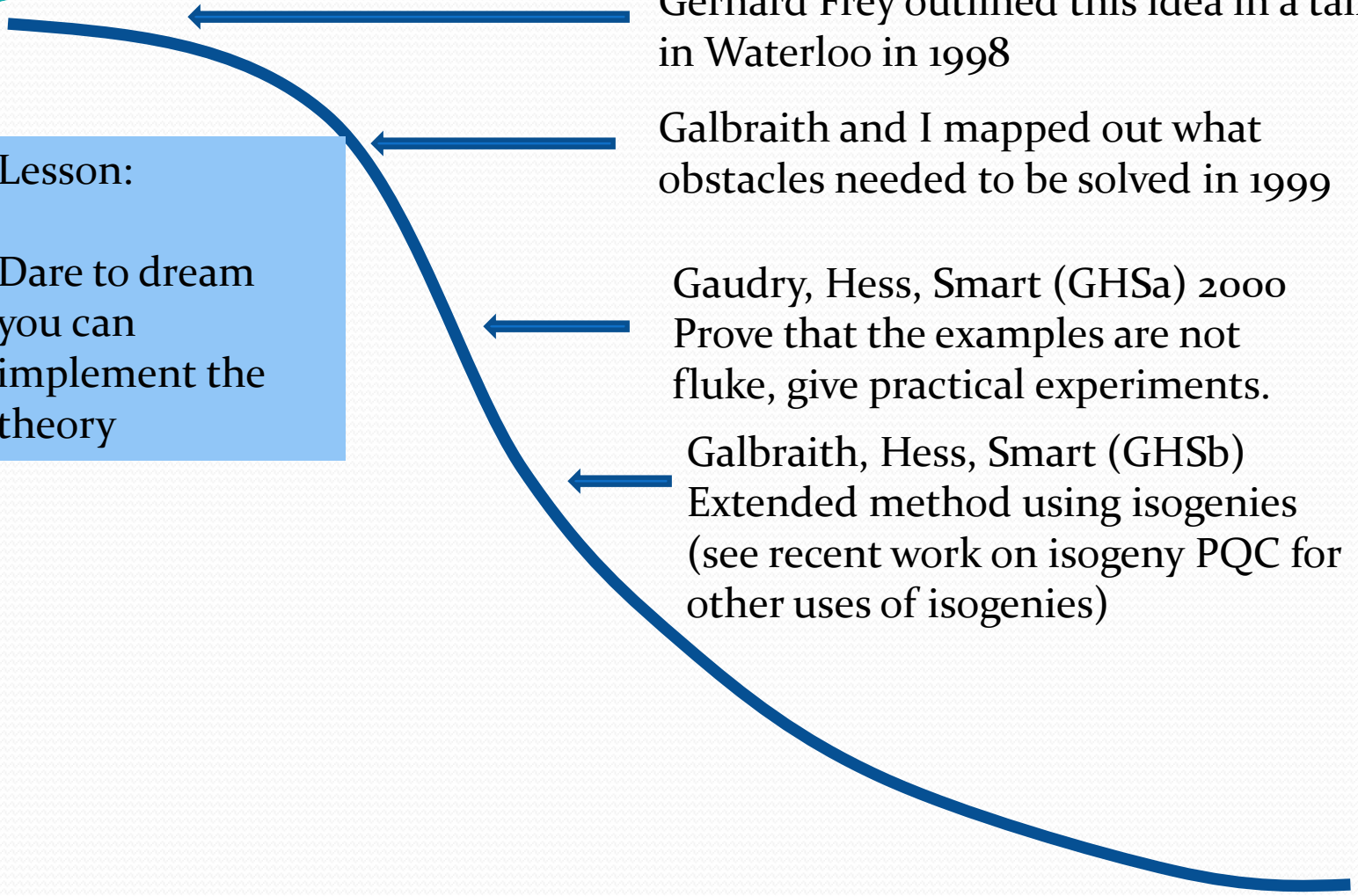
Gerhard Frey outlined this idea in a talk in Waterloo in 1998

Galbraith and I mapped out what obstacles needed to be solved in 1999

Gaudry, Hess, Smart (GHSa) 2000
Prove that the examples are not fluke, give practical experiments.

Lesson:

Dare to dream you can implement the theory



Gerhard Frey outlined this idea in a talk in Waterloo in 1998

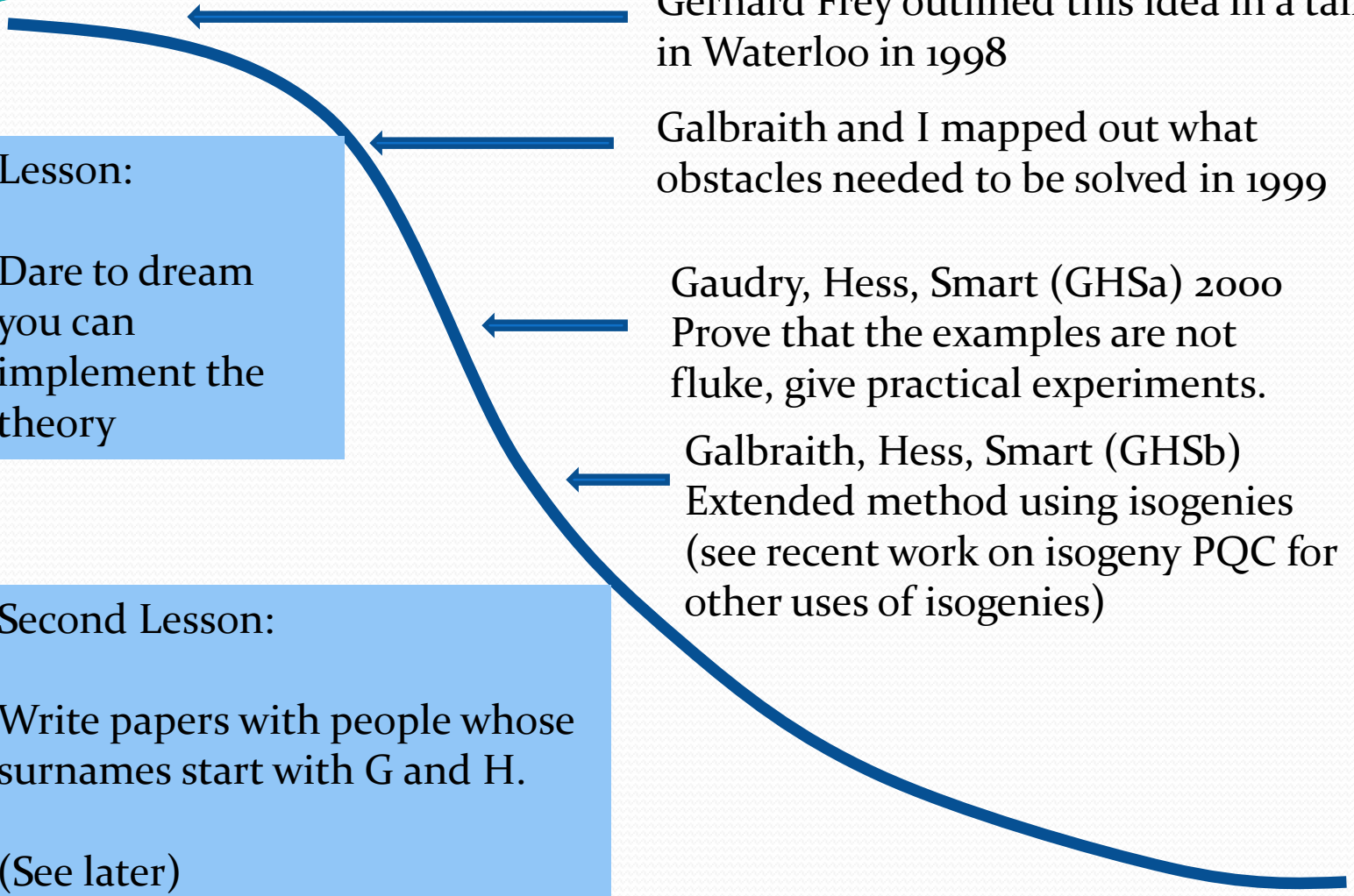
Galbraith and I mapped out what obstacles needed to be solved in 1999

Gaudry, Hess, Smart (GHSa) 2000
Prove that the examples are not fluke, give practical experiments.

Galbraith, Hess, Smart (GHSb)
Extended method using isogenies (see recent work on isogeny PQC for other uses of isogenies)

Lesson:

Dare to dream you can implement the theory



Gerhard Frey outlined this idea in a talk in Waterloo in 1998

Galbraith and I mapped out what obstacles needed to be solved in 1999

Gaudry, Hess, Smart (GHSa) 2000
Prove that the examples are not fluke, give practical experiments.

Galbraith, Hess, Smart (GHSb)
Extended method using isogenies (see recent work on isogeny PQC for other uses of isogenies)

Lesson:

Dare to dream you can implement the theory

Second Lesson:

Write papers with people whose surnames start with G and H.

(See later)

ECDLP Summary

Notice the pattern

- Someone comes up with theory (Frey)
- Realise you can implement it
- Start building techniques for implementing it
- Series of papers needed to turn theory into practice
  - Many of these papers really contain nothing
    - e.g. My initial paper with Galbriath
  - But if these papers do not exist the whole program falls down

FHE

Similar story with FHE work

- Initial paper of Gentry
- Vercauteren and I decided to see if it could be implemented.
- Resulting paper is basically Gentry's thesis for dummies. Contains nothing new, only that you could do it
- This scheme is now considered "broken". But showed SHE was possible

FHE

Similar story with FHE work

- Initial paper of Gentry
- Vercauteren and I decided to see if it could be implemented.
- Resulting paper is basically Gentry's thesis for dummies. Contains nothing new, only that you could do it
- This scheme is now considered "broken". But showed SHE was possible

Lesson:

Dare to dream you can implement the theory

FHE

Similar story with FHE work

- Initial paper of Gentry
- Vercauteren and I decided to see if it could be implemented.
- Resulting paper is basically Gentry's thesis for dummies. Contains nothing new, only that you could do it
- This scheme is now considered "broken". But showed SHE was possible

Lesson:

Dare to dream you can implement the theory

Lets see what can be implemented?
What functions do we know the circuits for?
Why lets try AES..... (for other reasons see later)

FHE

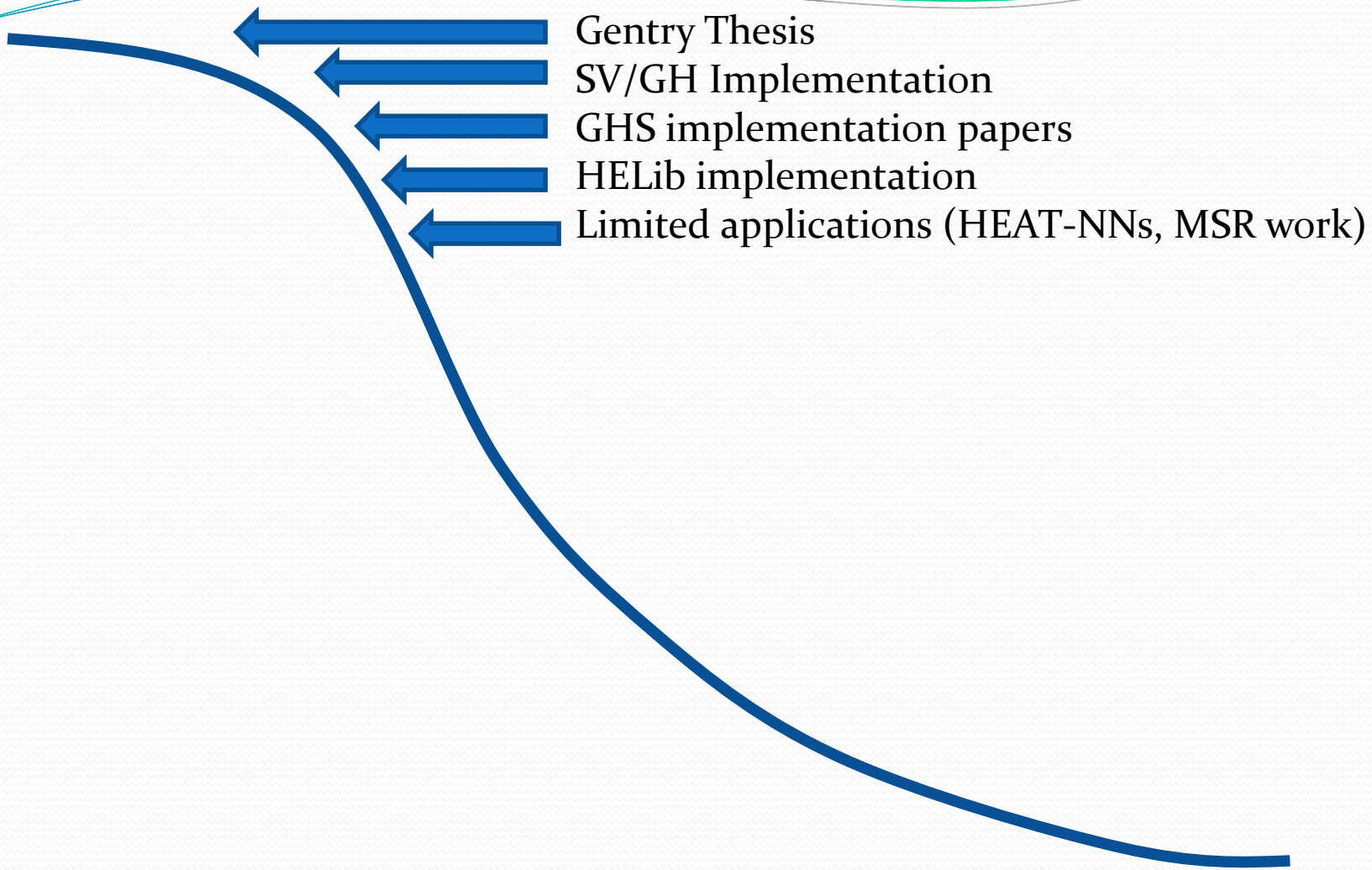
Working with Gentry and Halevi (another “G” and “H”) worked to get AES implemented in FHE

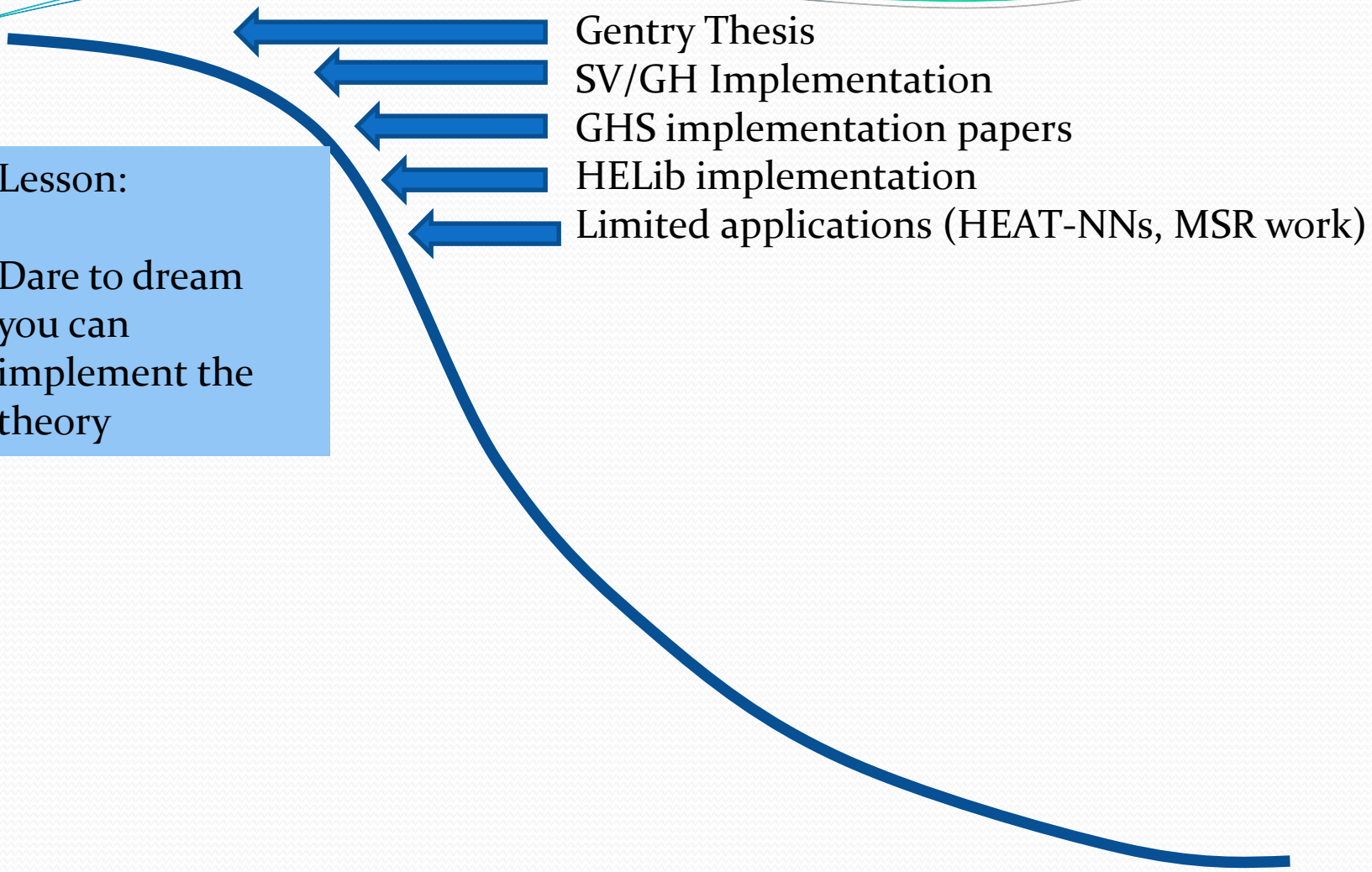
On way needed to build all sorts of other optimizations

- Slot manipulation
- DCRT representation
- Modulus switching up
- Lots of implementation tricks useful in bootstrapping etc

The third of our papers actually did the AES implementation

Again, just trying to implement something generates new ideas and pushes stuff down the curve from theory to practice.


Gentry Thesis
SV/GH Implementation
GHS implementation papers
HELib implementation
Limited applications (HEAT-NNs, MSR work)



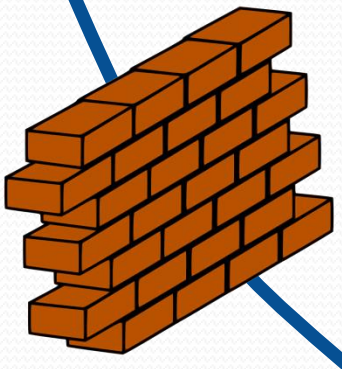
Lesson:

Dare to dream you can implement the theory

Gentry Thesis
SV/GH Implementation
GHS implementation papers
HELib implementation
Limited applications (HEAT-NNs, MSR work)

Lesson:

Dare to dream you can implement the theory



We seem to have hit a brick wall in pushing it further to practice.

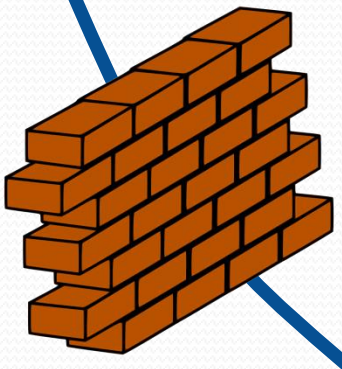
Need more people to try doing stuff.

e.g. working on NNs led to new work in SHE+Floating point operations.

Gentry Thesis
SV/GH Implementation
GHS implementation papers
HELib implementation
Limited applications (HEAT-NNs, MSR work)

Lesson:

Dare to dream you can implement the theory



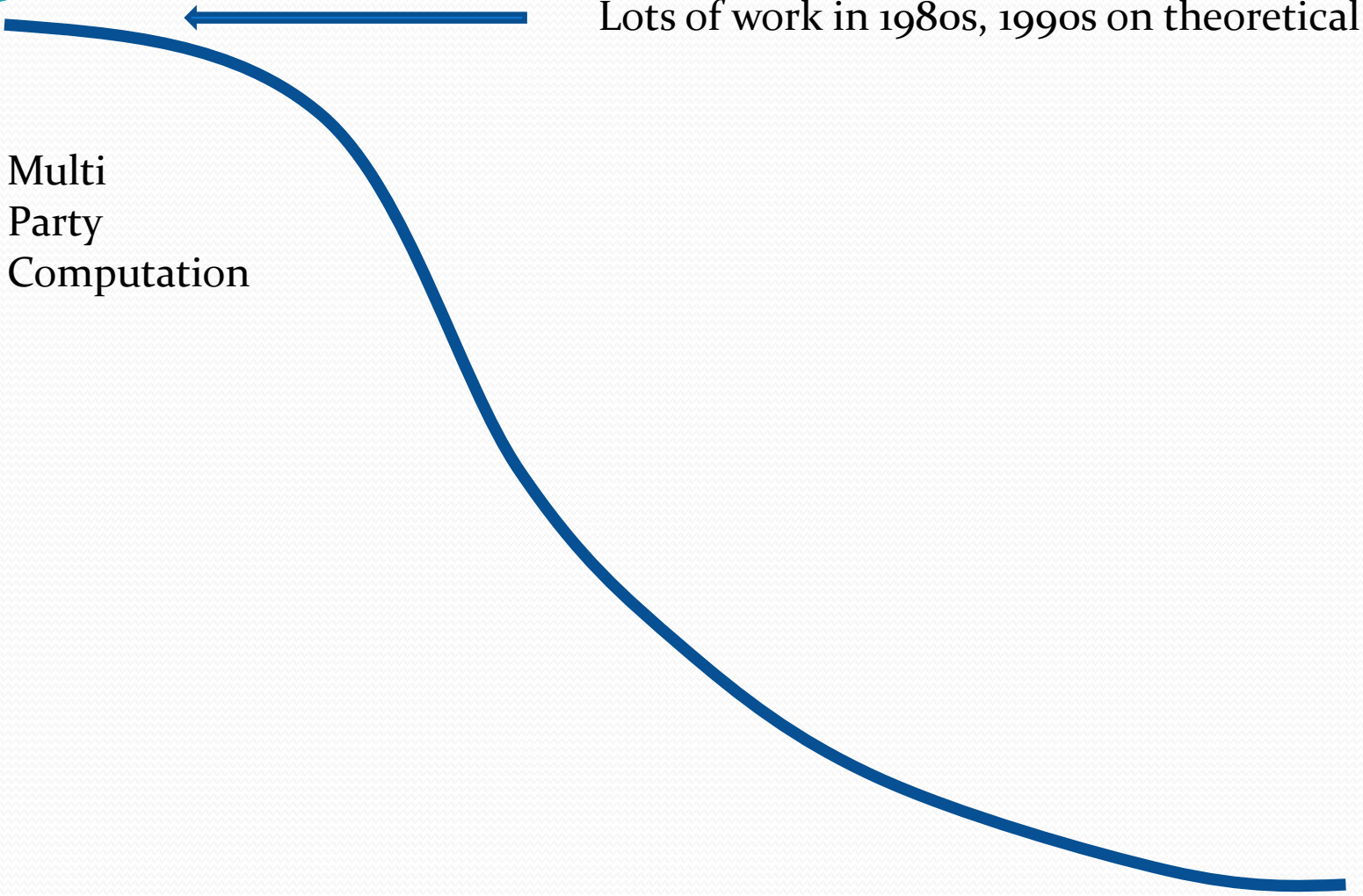
We seem to have hit a brick wall in pushing it further to practice.

Need more people to try doing stuff.

e.g. working on NNs led to new work in SHE+Floating point operations.

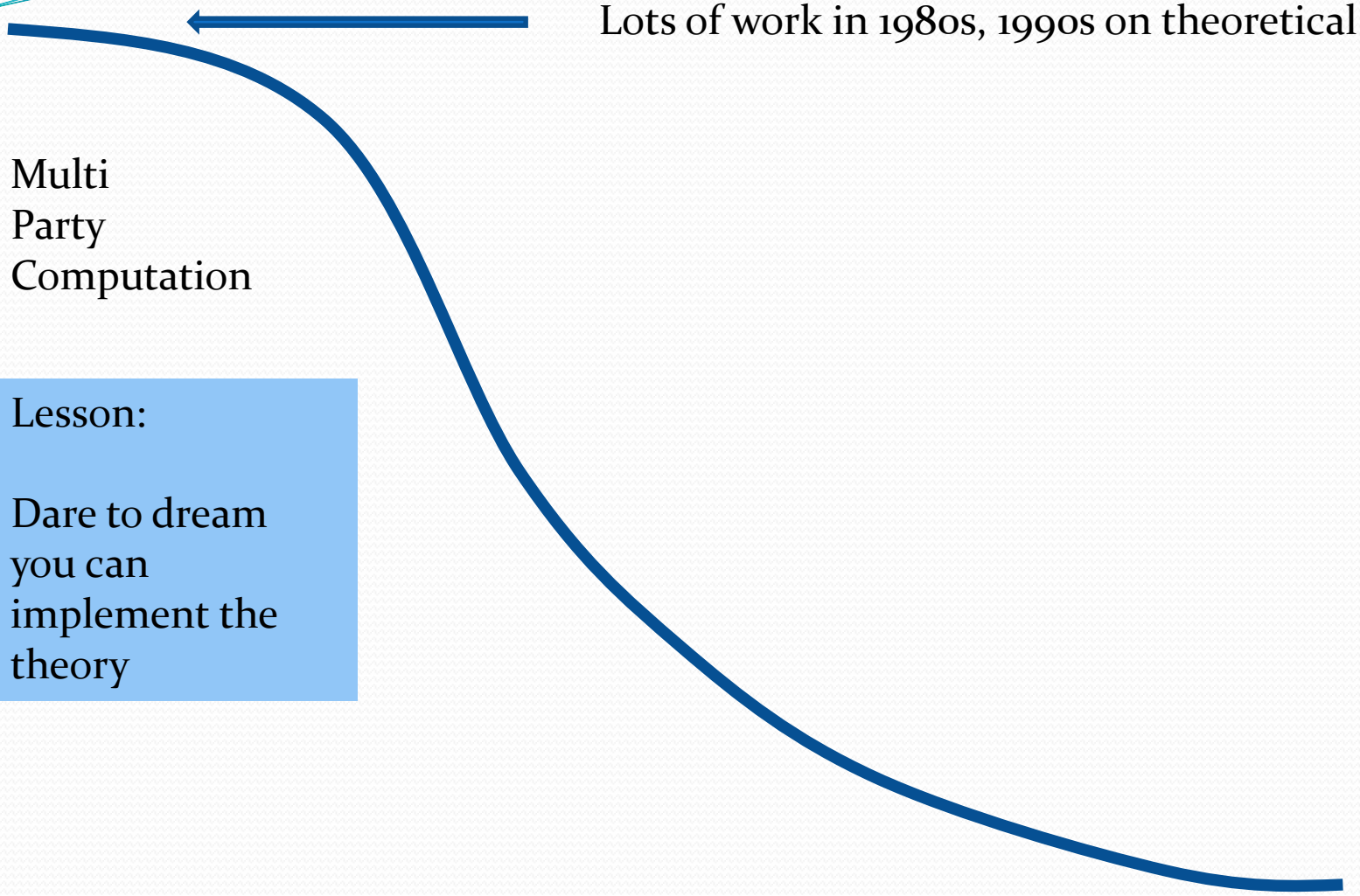
Maybe trying other challenges (such as AES or NNs) can lead to a big breakthrough?

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



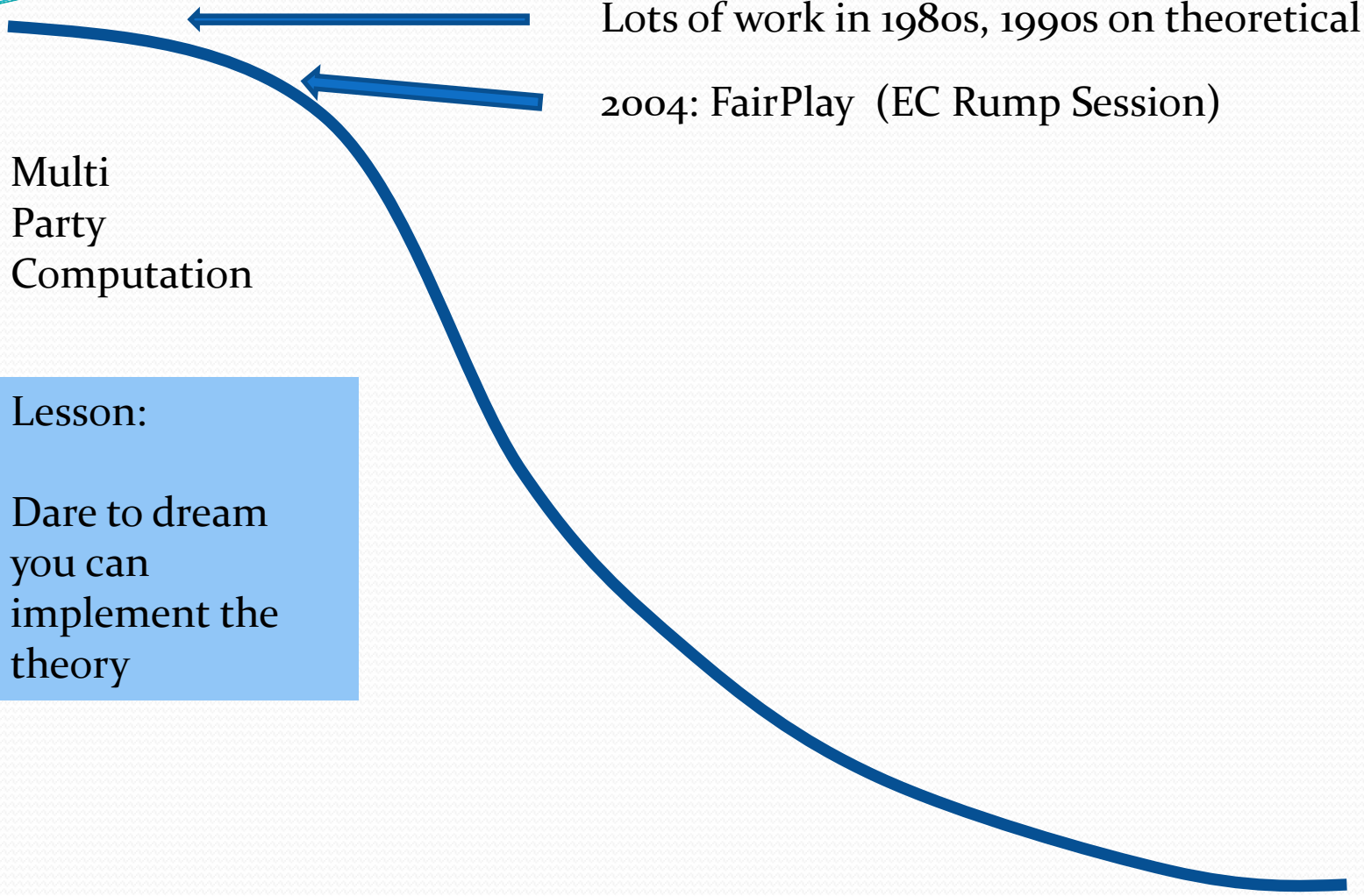
Lots of work in 1980s, 1990s on theoretical MPC

Multi
Party
Computation



Lesson:

Dare to dream you can implement the theory



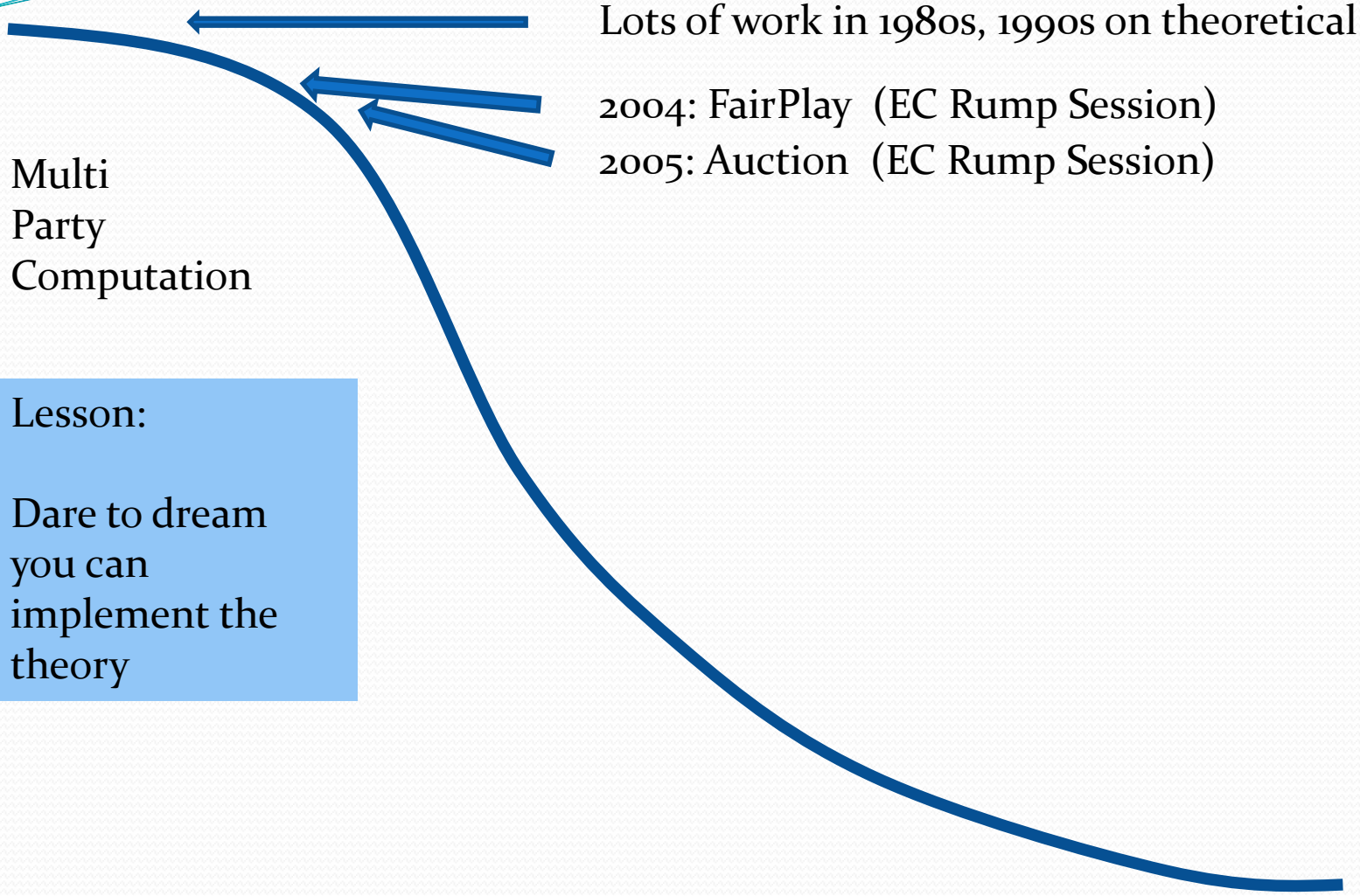
Lots of work in 1980s, 1990s on theoretical MPC

2004: FairPlay (EC Rump Session)

Multi
Party
Computation

Lesson:

Dare to dream you can implement the theory



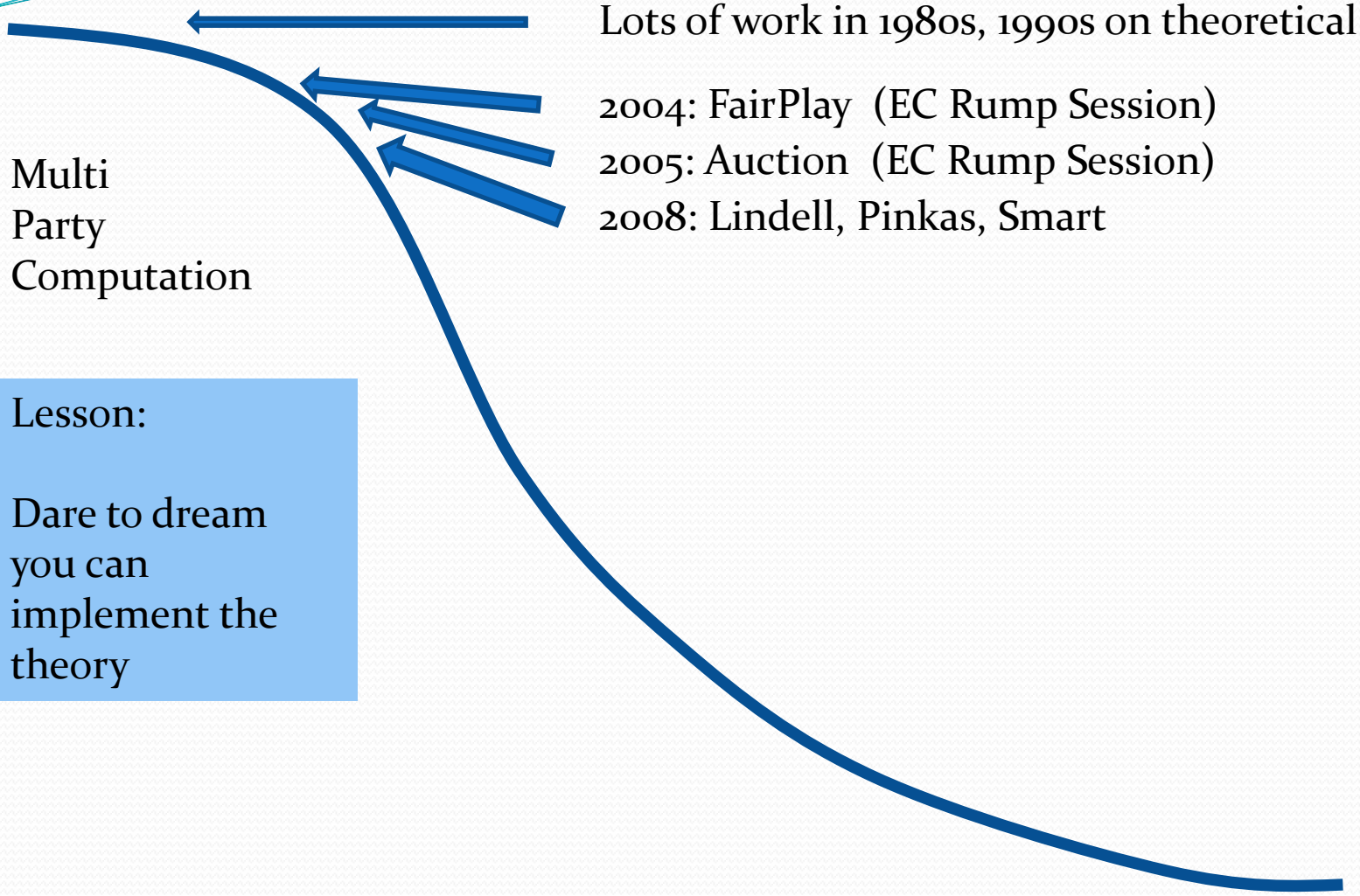
Lots of work in 1980s, 1990s on theoretical MPC

2004: FairPlay (EC Rump Session)
2005: Auction (EC Rump Session)

Multi
Party
Computation

Lesson:

Dare to dream you can implement the theory



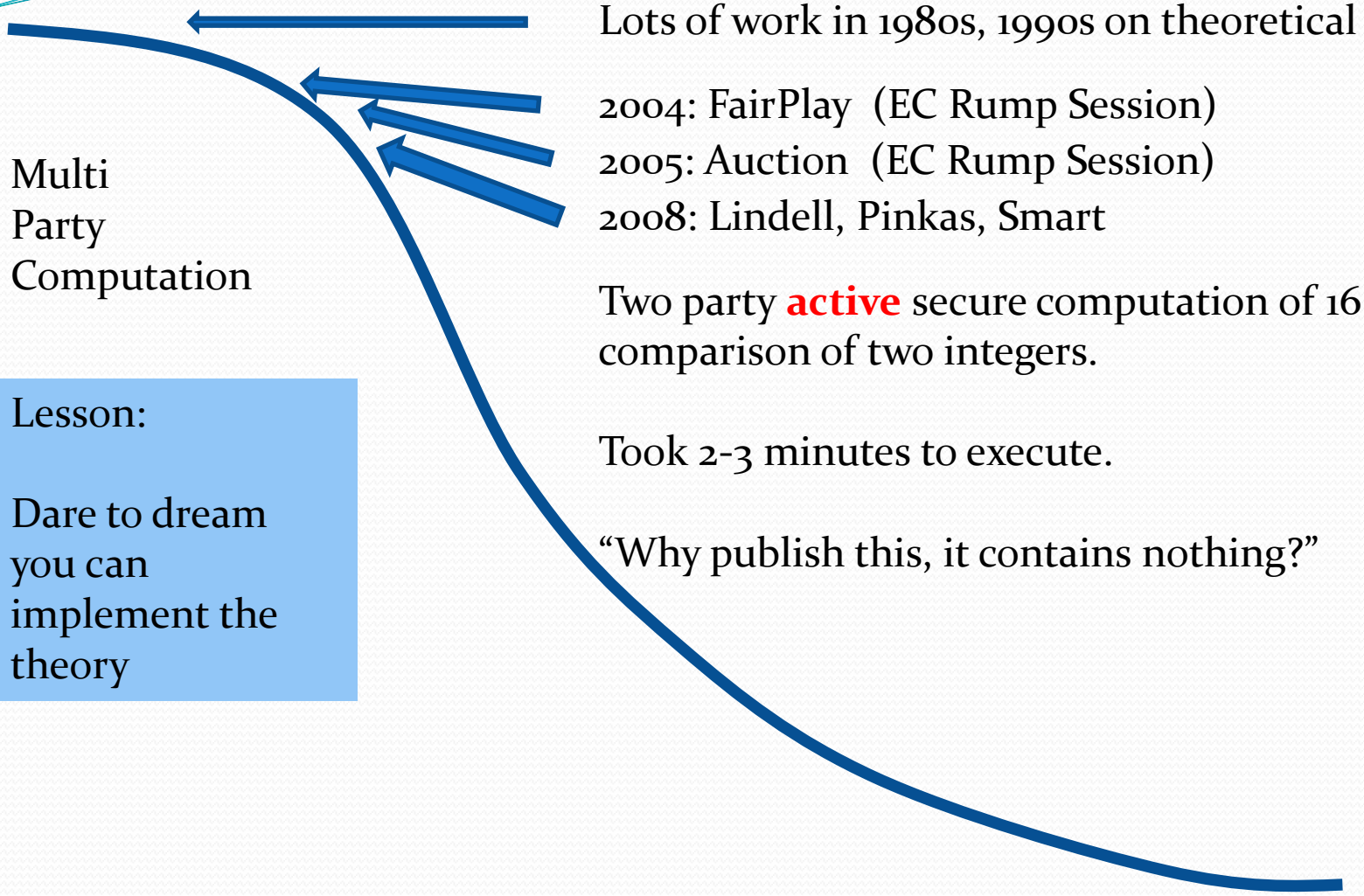
Lots of work in 1980s, 1990s on theoretical MPC

2004: FairPlay (EC Rump Session)
2005: Auction (EC Rump Session)
2008: Lindell, Pinkas, Smart

Multi Party Computation

Lesson:

Dare to dream you can implement the theory



Multi
Party
Computation

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

2004: FairPlay (EC Rump Session)
2005: Auction (EC Rump Session)
2008: Lindell, Pinkas, Smart

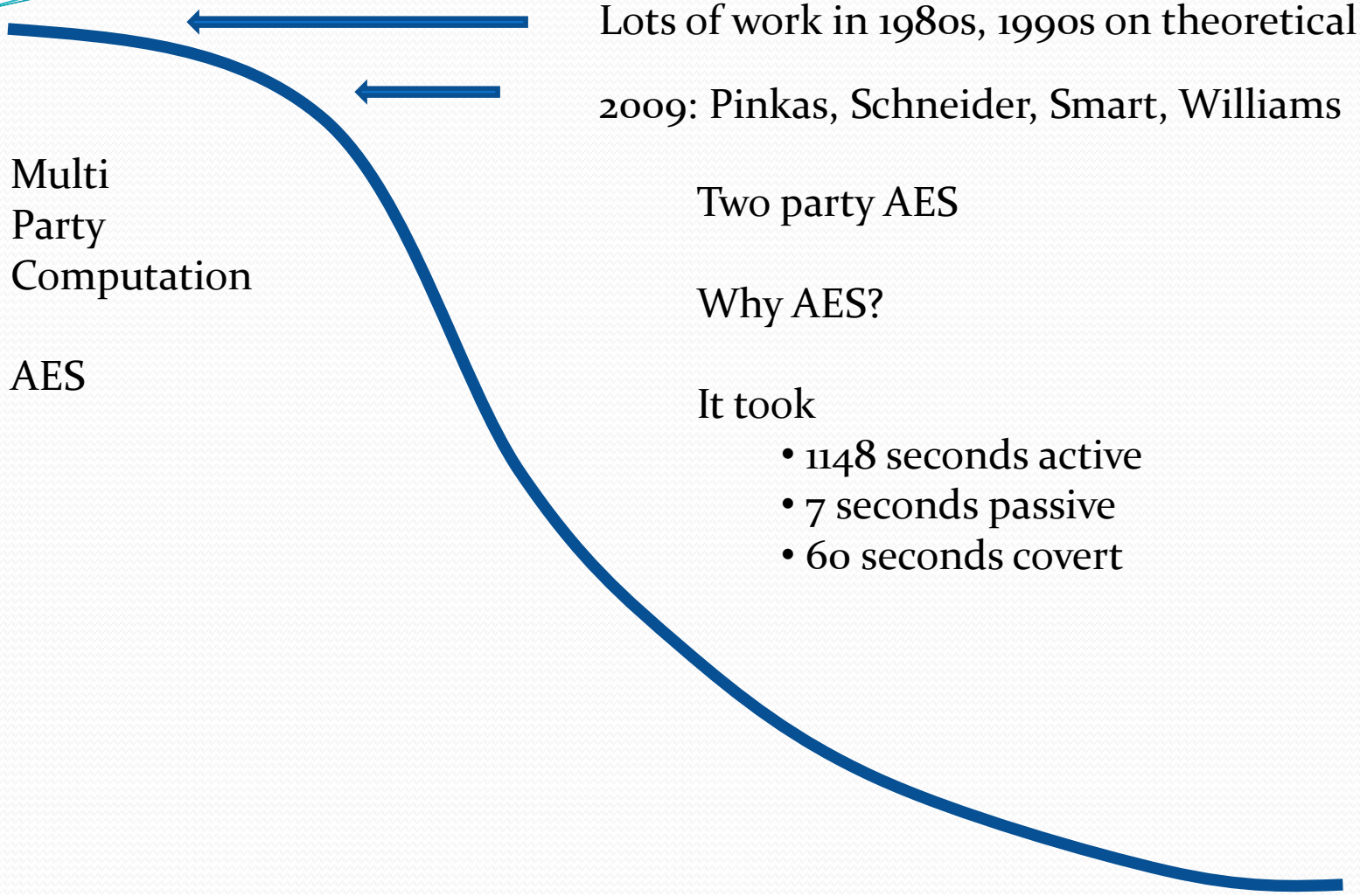
Two party **active** secure computation of 16 bit comparison of two integers.

Took 2-3 minutes to execute.

"Why publish this, it contains nothing?"

Lesson:

Dare to dream you can implement the theory



Multi
Party
Computation

AES

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

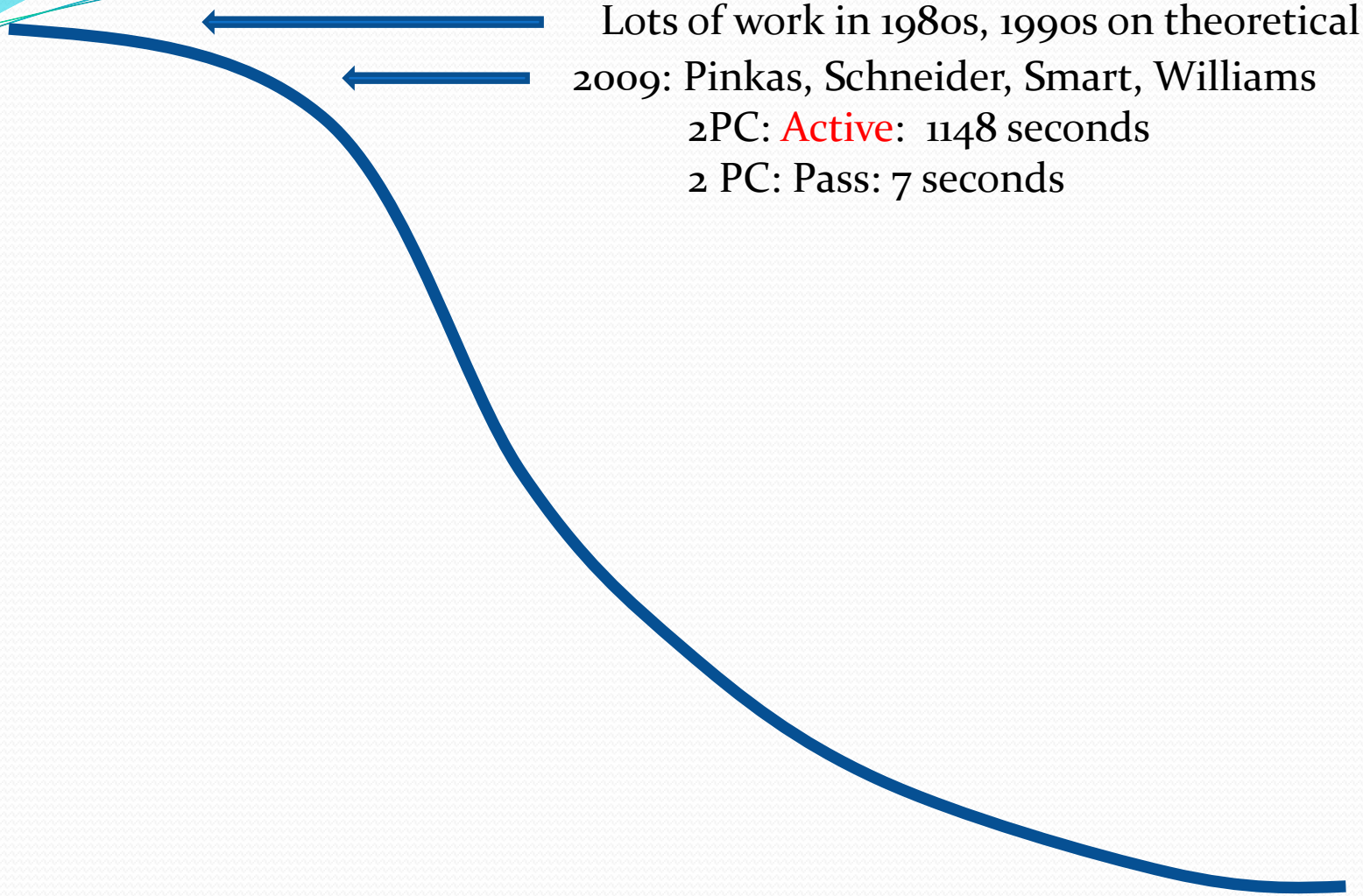
2009: Pinkas, Schneider, Smart, Williams

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

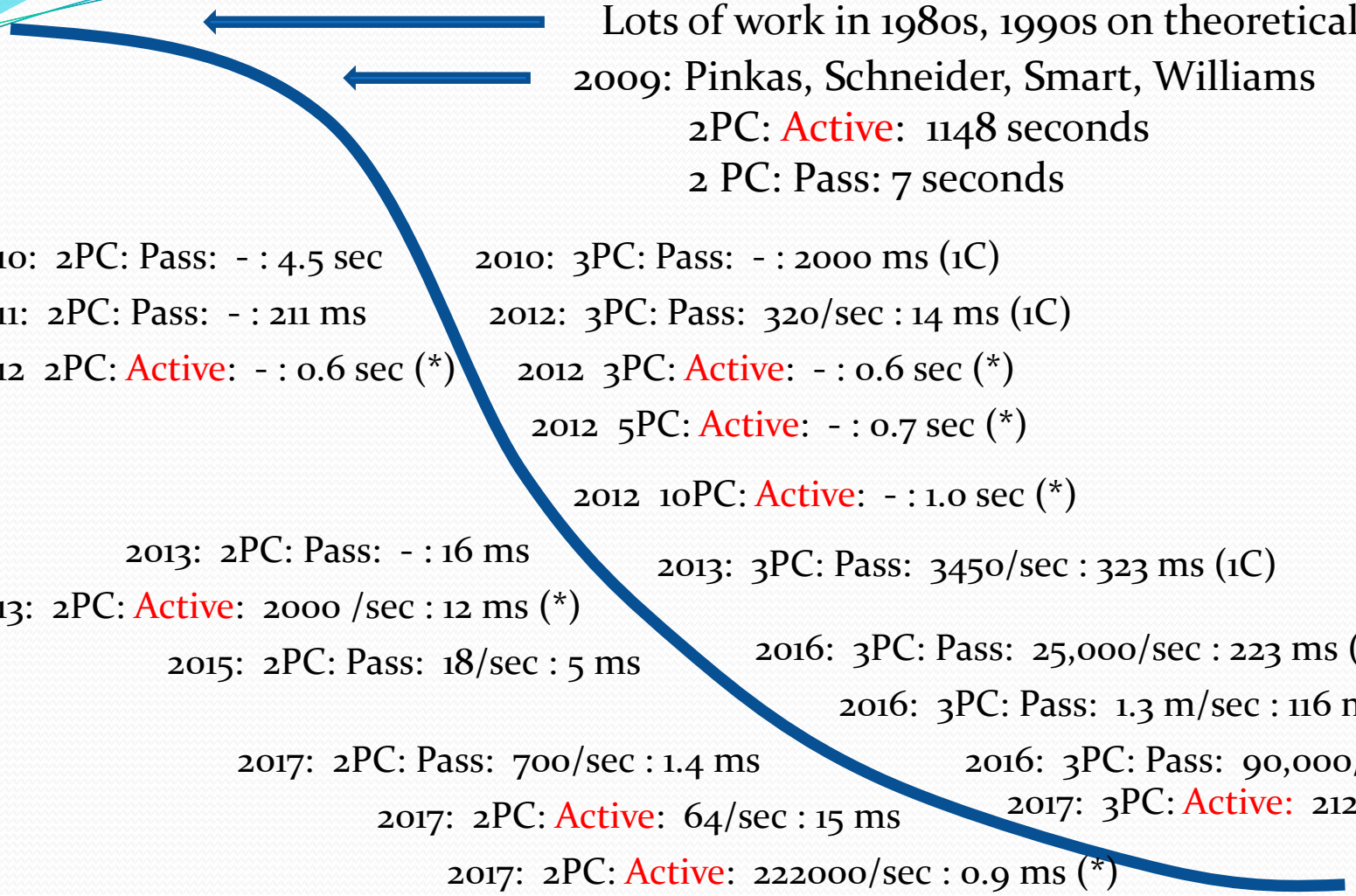
2009: Pinkas, Schneider, Smart, Williams

2PC: Active: 1148 seconds

2 PC: Pass: 7 seconds

1C = Tolerate one corruption

* = Online runtimes only



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

MPC

But AES is not a typical example of block cipher usage

- Now have PRF designs which are MPC friendly (MiMC, Leg)
- Working on modes of operation which are MPC friendly
  - Why do we need these?

ML algorithms in MPC

- Long history (Lindell/Pinkas in 2008)
- But now a practical reality in some examples
- Looking at MPC friendly neural networks, and other structures

MPC The Future is Bright

Lots of investment in area

- DARPA/IARPA Probably > $100 million investment in last decade
  - (Brandeis, PROCEED, SPAR,…)
- ERC: Lot of investment mentioning MPC
  - (Cramer, Damgard, Lindell, Nielsen, Pointcheval, Smart, ….)
- EU H2020 Projects
  - (CACE, PRACTICE, SODA, UaESMC, PRIST, SUNFISH, ….)
- VC funding
- Loads of EU based national funding

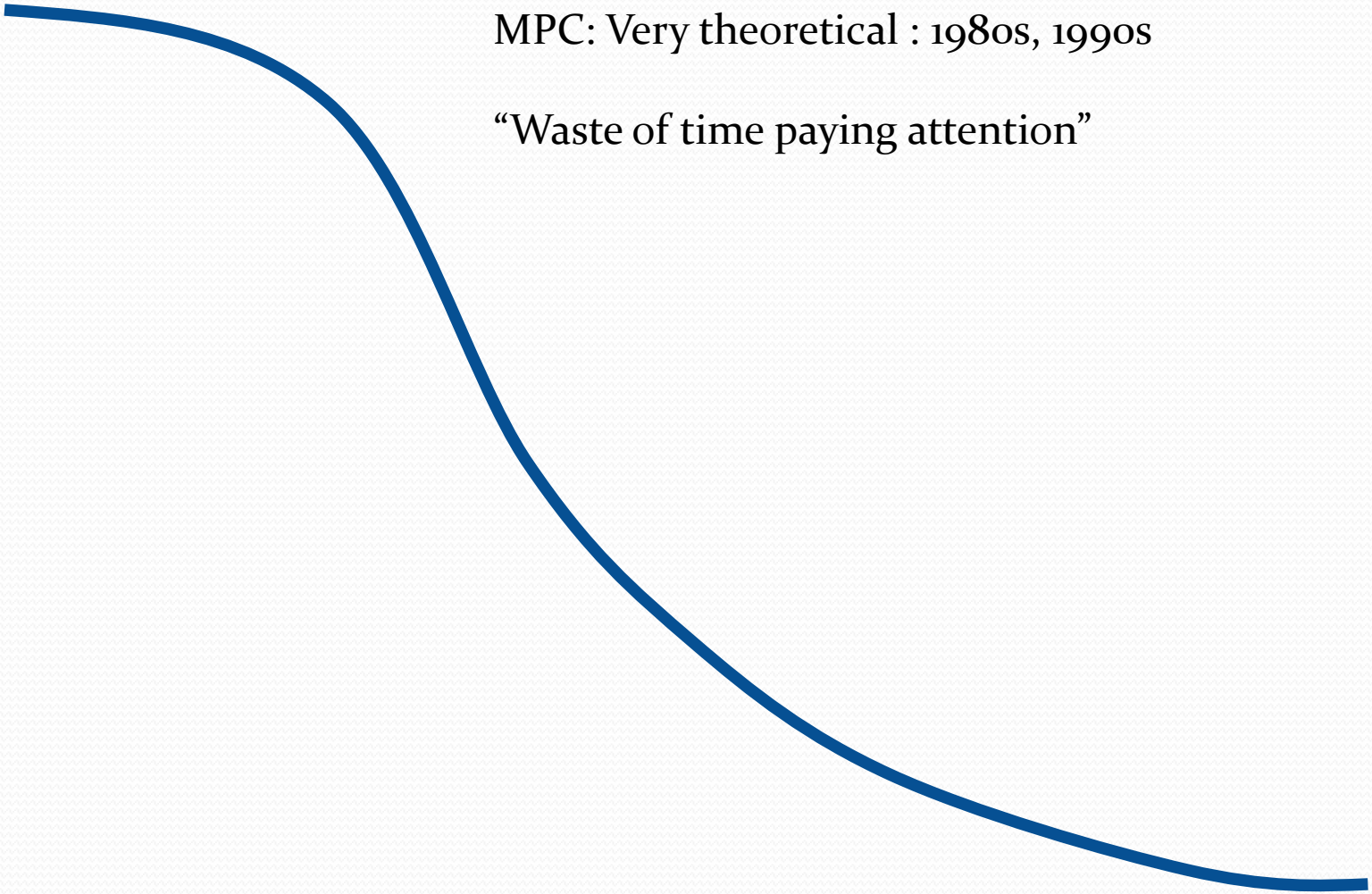
Other Applications…

- **Masking** in side channel research is also MPC in some sense
  - Computing on secret shared data
- Strong linkage between TCC and CHES communities
  - Wire-probe-model (Ishai, Sahai, Wagner)
  - TI multipliers (Rijmen, Nikova and others)

- Lots of potential new research
  - Could apply more MPC theory to CHES style problems
  - Could apply more side-channel style analysis to MPC style problems.

MPC: Very theoretical : 1980s, 1990s

“Waste of time paying attention”



MPC: Very theoretical : 1980s, 1990s

"Waste of time paying attention"

Lesson:

Always pay attention to ALL talks

Now various companies in this space

Summary

Try to **implement** theoretical stuff

- Theory will stay theory unless someone does this.
- Theoreticians should welcome it as showing someone care
- Practical people should welcome it as expanding their problem space

This processs tests how far practice is away from theory

Summary

This process also turns up

The “correct” theoretical problems /metrics to look at

New practical/implementation problems

DARPA programs PROCEED, Brandeis and SafeWare are good examples of this

- Unlike Phil Rogaway I see this “military” funding of crypto having been for the good.

Summary

There is a huge amount of work to do in the MPC area.

Its a great mix of theory and practice

We need more people to work in this area

- If interested in getting involved come and see me

Summary

There is a huge amount of work to do in the MPC area.

Its a great mix of theory and practice

We need more people to work in this area

If interested in getting involved come and see me

Usual Bristol jobs advert

Questions?