coinbase

The MPC Journey from Theoretical Foundations to Commercial Technology

Yehuda Lindell

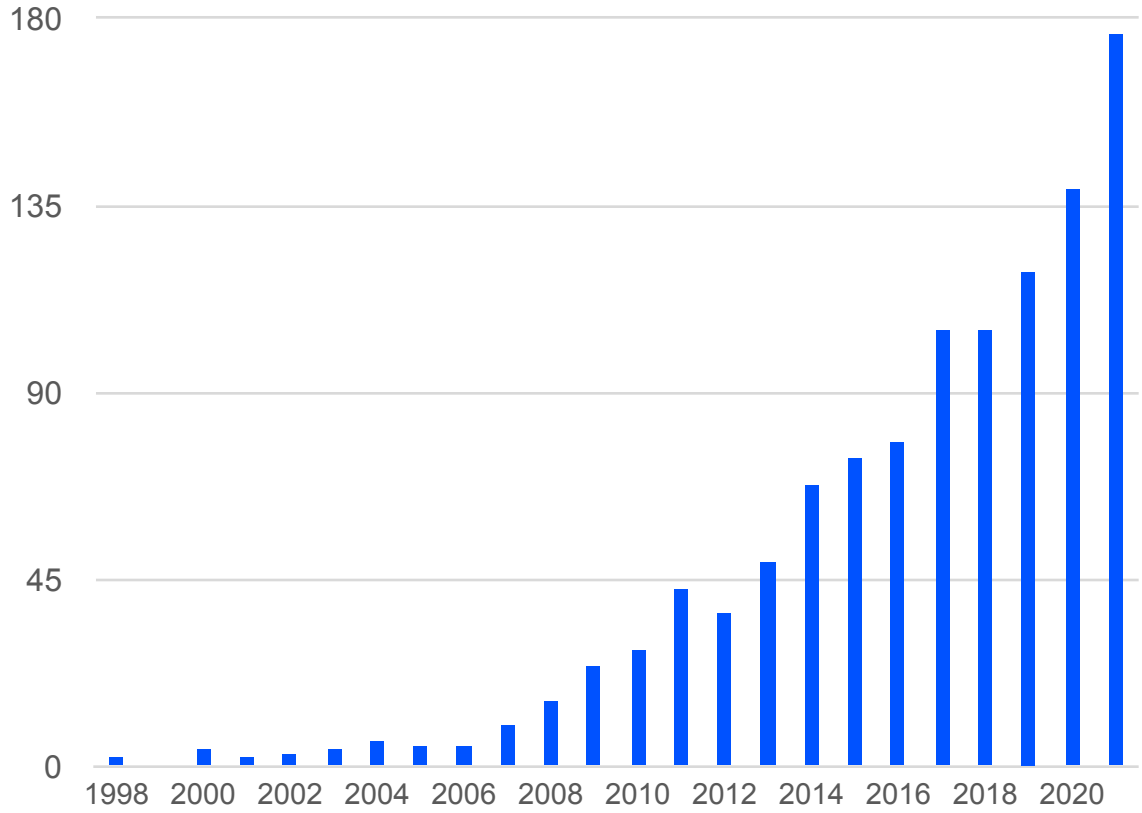
Coinbase

Retrospection on the MPC Journey

- **The stages of its scientific evolution and what we can learn from it**
- **Commercialization process and challenges**
  - What we can learn in general
  - What still needs to be achieved

Papers in ePrint Referencing MPC, two-party computation, secure computation and multiparty computation

Of course it's not complete, since threshold signing, PSI, and other topics are also MPC but may not use this terminology



Scientific Evolution – Summary of Stages

- **Stage 1: the idea stage** (approx mid 1980s to mid 1990s)
- **Stage 2: theoretical foundations** (1990s and 2000s, and ongoing)
- **Stage 3: algorithmic research** (mid 2000s to mid 2010s, and ongoing)
- **Stage 4: applied research** (mid 2010s to today)

- **Notes**:
  - There are many counter-examples of things that worked "out of order" (e.g., threshold cryptography was studied intensively in the 1990s, also from an efficiency perspective)
  - There are too many relevant works to cite (and I'm afraid I'll omit many important things)

Stage 1 – The Idea Stage (1986 – 1995)

- **Initial breakthrough ideas**
  - Basic feasibility of 2-party and multiparty computation
  - Information-theoretic MPC
  - Oblivious transfer and OT extension
  - Multiplication triples
  - MPC based on threshold secret sharing (mult and degree reduction)
  - Garbled circuits
  - Semi-honest to malicious compilation

Some Interesting Observations

- **Many of these initial ideas and protocols were around before we even knew how to define security**
  - But there was enough intuition to “get it right” (even to the extent of things like BGW being UC secure)
- **Many initial feasibility proofs used techniques that are used in practice today (with optimizations)**
  - Garbled circuits, OT extension, multiplication triples, ZK compilation and much more

Stage 2 – Theoretical Foundations

- **Study of the feasibility of MPC**
  - How to define security
  - Adversary models:
    - Information theoretic vs computational
    - Semi-honest, malicious, covert
    - Stand-alone (sequential) versus concurrent composition
    - Static, adaptive, proactive
  - How to prove security
  - Under what setup and/or computational assumptions

Important Observations

- **In this stage, the motivation is not applications or usage**
  - Indeed, it's very unclear if this will ever be usable or used
- **Why study it?**
  - Motivation is primarily mathematical elegance and beauty, and part of "understanding the world"
  - A natural question needs no motivation!
    - Proving a theorem without revealing anything is an amazing idea within itself; the fact that this is possible is important to understanding computation

Theoretical Research

- **There are many benefits of theoretical research**
  - Understanding our world (in this case, computation)
  - Techniques and knowledge
    - The adversarial mindset can make a theoretical cryptographer a very successful consultant
  - And it can lead to practical usage – MPC is an example of that
    - But in the late 1990s and early 2000s, that wasn't what we thought about

Stage 3 – Algorithmic Research

- **The feasibility results provide protocols, but they can't be implemented**
  - Prove in ZK that your next message in a protocol is correct, via a Karp reduction to an NP-complete problem
  - Use multiple asymmetric operations for every AND gate in a circuit
- **The next stage in development is to try to make it more efficient**
- **This is very challenging -**
  - You are moving from impractical to impractical
  - Theoreticians aren't always interested and practitioners look at it and still see something wildly impractical
- **There was an MPC low at this time (in my subjective memory)**

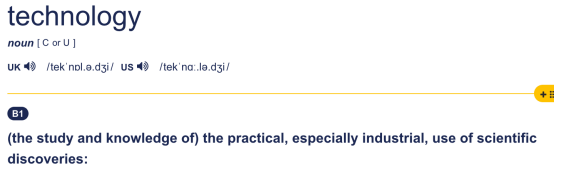
An Important Lesson

- **As a researcher, it's important to believe in the scientific process**
- **When your research areas loses popularity, what do you do?**
  - Sometimes it really makes sense to change, since the topic has exhausted itself
  - Sometimes it's a matter of fads, and you should stay
- **How do you decide?**
  - I think that researchers should work on what they are passionate about
    - This makes for the best research, and goes in both directions (you don't have to follow the latest fads if you're not interested in them)
  - As a community overall, we will move forward – it's OK and even best to optimize for a community rather than an individual effort

Stage 4 – Applied Research

- **The focus is no longer the topic itself, but how it can be used to solve other problems**
- **There is a huge difference between a paper in 2001 that considered privacy-preserving machine learning and research today on that topic**
  - In 2001, the paper's statement was to motivate the field: this may actually be possible, and so it's important to study MPC
  - In 2021, papers on this topic are actually trying to solve the problem in a way that can be used
- **This often leads to new theoretical questions and so the process is intertwined and reactive, rather than sequential**

The Beginnings of Commercializatic


technology

noun [C or U]

UK /tekˈnɒl.ə.dʒi/ US /tekˈnɑː.lə.dʒi/

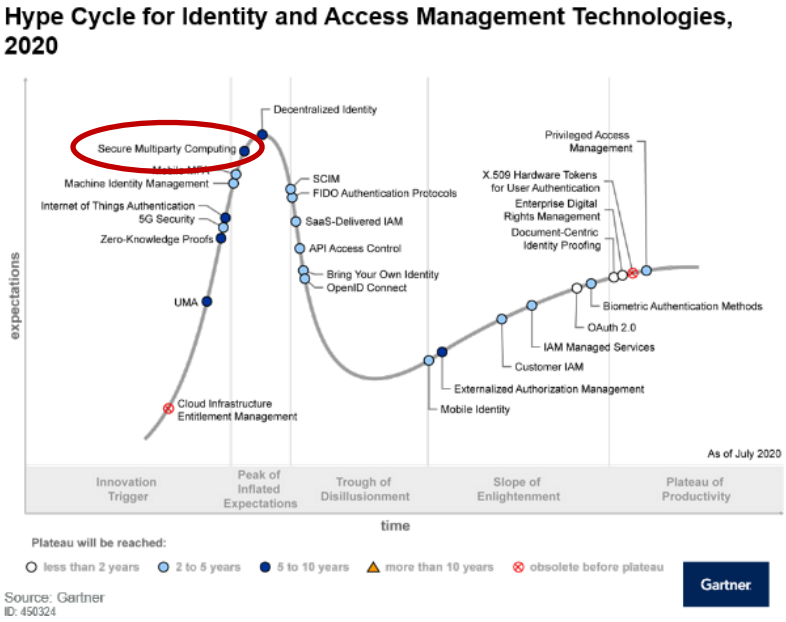
B1

(the study and knowledge of) the practical, especially industrial, use of scientific discoveries:

- **At some point, science becomes technology and it's ready for commercialization**
- **At this point, we have the tendency to wave from academia and say "come and take it", but that's not realistic**
- **If we don't make the effort to push it out, then it won't happen**
  - It requires great expertise at this time (it's very far from off the shelf technology)
- **Some researchers look actively to do this, but I didn't**
  - But when the idea came, I felt I couldn't ignore it
  - It takes a lot of commitment; it's lucky I didn't know how much!

Challenges of the Early Days

- **What is MPC? It sounds like snake oil.**
- **How do you overcome this?**
  - Academic reputation actually helps a lot!
  - Market education – it takes time and that should be factored in
  - FIPS certification
  - And analysts like Gartner help significantly
    - This can feel outrageous, but in a world of so much noise and fake news, how can you differentiate?



What Problem Do You Solve – a Scalable Product

- **Projects versus products**
  - How much customization is needed?
  - Do many people need the same problem solved?
- **The difference between a potentially healthy standard business and a startup with exponential growth (e.g., doubling revenue each year)**
- **Our focus at Unbound was on key protection and management – an existing problem with a budget**
  - Privacy is much harder, but without doing the work, it won't happen (the need isn't always apparent until the existence of a solution is known)

A Repeatable Use Case

- **A use case is not an “application”**
  - Protection of cryptographic keys is not a use case
  - Better machine learning for image analysis is not a use case
- **A repeatable use case – multiple customers doing the same thing with your product**
  - Replacing smartcards with MPC for mobile authentication is a use case
  - Better ML to detect flaws in a production plant is a use case
- **Repeatability helps with sales, marketing, education, and is the key to scaling**

The Double-Edge Sword of Deep Technology

- **Novel research results can be a huge asset, but they don't make a business**
  - Better technology with worse business execution will usually lose to inferior technology with better business execution
- **In the beginning there is a tendency to focus on the technology**
  - But **no one cares** about your cool technology – they only care about whether it makes the product better!
  - This may seem obvious but it's really hard – the technology is what makes the product better and is the differentiator
- **A hard question – can you demonstrate that your product is better? Is it better visibly or invisibly? Can you determine the ROI?**
  - Being more secure in an unclear way is not that helpful

Overcoming the Challenge

- **Finding your value proposition**
- **Determining the compelling event**

Value Proposition

- **It's not what we thought**
- **We started with replacing hardware (HSMs, smartcards)**
  - By being software we would be cheaper, faster to deploy, more agile!
  - It was all true, but compelling events were hard to find
- **In the end, our major value proposition was different**
  - Usability, orchestration, defragmentation
  - MPC was an important part, but very much under the hood
  - For security – key misuse resistance was a major benefit
    - Code signing (policies, sign after scan,…)
    - Cryptocurrencies

“It’s much easier to sell a product that

improves usability without sacrificing security

than a product that

improves security without sacrificing usability”

Bob Blakley

The Compelling Event

- **Why will I buy now?**
  - Regulatory compliance (e.g., GDPR) and its double-edged sword
  - Business enablement (move to cloud without sacrificing security)
  - Immediate cost saving

- **When you understand the compelling event, you can market to that problem and issue**

Today’s Fragmented Cryptographic Infrastructure

Different Environments

On-premise data centers

Different clouds for different business needs

Need for gradual migration and flexibility

Different Key Stores

Physical HSMs

Cloud HSMs

Cloud KMSs and vaults

Unprotected keys on servers

Different Interfaces

Many standard libraries (PKCS11, KMIP, JCA, CNG, OpenSSL) without universal support

Environment-specific REST APIs

Different Cryptographic Problems

Encryption – databases, storage, VMs

Application-level cryptography

PKI and certificates

Authentication

Code and document signing

Blockchain and crypto assets

Challenges

Management: different key stores in different environments (clouds and on-prem) have different management methods

Challenge to set company-wide policies

No single audit of all keys and operations

Time-costly to manage different solutions in different settings

Different authentication methods for administrators

Consumption: different key stores in different environments work differently

The same key store cannot be used in on-premise data center and cloud

- Different key stores offer different APIs
- Applications need to be refactored for different environments
- Client authentication uses different and proprietary methods

Existing infrastructure is rigid and slow to deploy

Key theft vs key misuse

Unified Orchestration

Single pane of glass for managing all keys in all key stores

Set companywide policies for cryptographic parameters, key rotation, access control, key usage limitations, and more

A single (tamper resistant) audit for all key stores

Synchronization between key stores and devices (virtual mesh)

Unified authentication and authorization (integration to OpenID connect / OAUTH)

Unified cryptographic consumption

Use different key stores in different environments in the same way

- Universal API - use any standard library and REST API, irrespective of key store support
- No need to refactor applications

Unified client authentication and authorization (integration to OpenID connect / OAUTH)

Achieve virtualized cryptography infrastructure

Virtual mesh provides synchronization of keys and admin settings

Crypto-agility – updates and fixes separated from actual key store

Unbound's software-based MPC key store

- Complement hardware with software key stores for fast deployment and agility
- Built-in high availability and on-demand deployment
- Cryptographic services at the edge, where applications run

Cryptography firewall for all key stores, to prevent key misuse

CORE Information Security

CORE Identity Security

CORE Crypto Asset Security

Unbound CORE Platform

CORE Virtual HSM

Virtualized cryptography mesh over all key stores

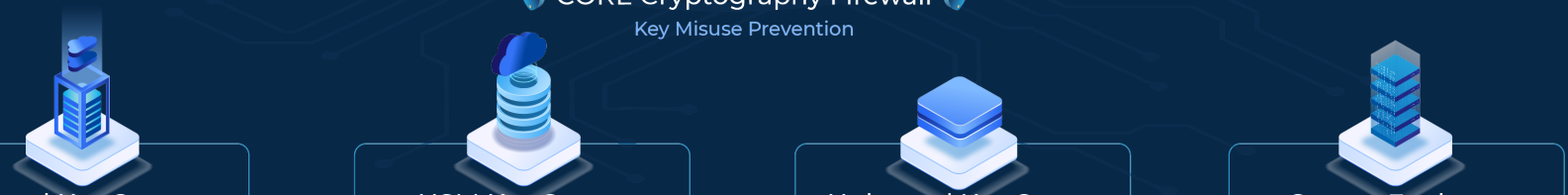
CORE Key Management

Single pane of glass for policies over all key stores

Authentication, Authorization, Policy, Quorum Approval, Tamper Proof Audit

CORE Cryptography Firewall

Key Misuse Prevention



Cloud Key Stores

AWS - Azure - Google

HSM Key Stores

Cloud - Physical

Unbound Key Stores

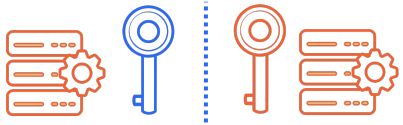
MPC Key Store

Secure Enclaves

AWS Nitro - SGX - IBM HPVS

Unbound CORE's MPC Key Store

1 Each private key is shared between at least two separate locations



2 Key shares are never combined at any point in time – not even when used or when created

3 The sharing of the keys is constantly refreshed so that the attacker must breach both simultaneously

Utilizes MPC technology based on decades of scientific research, and FIPS 140-2 Level 2 certified

Benefits

Support cloud migration and adoption; same key store for every environment

Cryptography at the edge, where your application runs

Built-in high availability and disaster recovery

Fully virtualized: supports cloud economy, replication, on-demand HSM services and fast deployment

Particularly suited for zero-trust environment with no single point of failure

Contrast to what we started with

Technology for securing corporations' applications and data from being breached, with a software-only solution

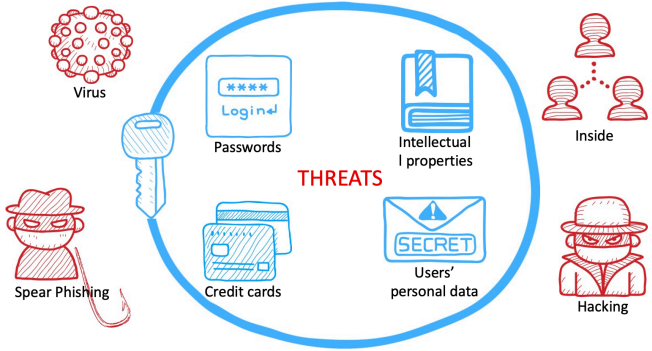
Strong Scientific Roots

Based **on years of deep research in computer science**, which has made distributed cryptography a practical reality

Multi-party Computation Solution

Using **cutting-edge research** from the field of **secure multiparty computation** to prevent attackers from getting to encryption keys, credentials, data and more

The Data Security Center Challenge



Challenge Currently not Met

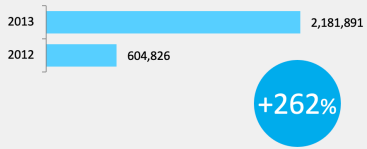
2013 THE YEAR OF DATA CENTER MEGA BREACH*

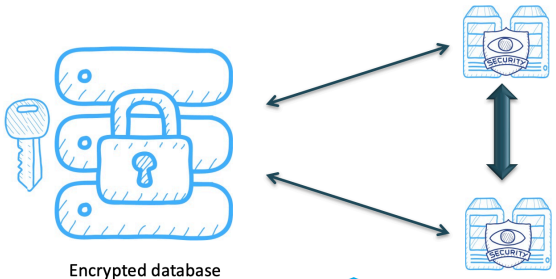
2013 showed 62% annual increase in breaches compared to 2012

550 million identities were breached in 2013-

- **Financial Data -** Consumer's credit card information, financial information
- **Personal data -** Birth dates, government ID numbers, home addresses, medical records, phone numbers, email addresses, login, passwords

Average Identities Exposed / Breach





Encrypted database

- Decryption takes place without ever bringing the key together
- The key is never in any single place to be stolen

There is much more to talk about

- **Product-market fit: what is it and how do you achieve it?**
- **Focus and why it’s critical**
- **The researcher/co-founder dilemma**

What Still Needs to be Achieved

- **MPC is still at the very early stages of commercialization**
- **The more that industry knows about it, the more new use cases we see (and even existing use cases are far from complete)**
- **But all this will remain limited unless we can move MPC from a mature technology requiring great expertise to a ubiquitous off-the-shelf solution**
  - This is a very hard problem and it's not even clear what it means
  - Deploying any cryptography is hard, even basic encryption
  - But we can't require a PhD in cryptography to deploy MPC (and today, even that isn't enough)

Important Lessons

- **Science can take a long time to become technology, and that's fine**
  - The role of academic research is to be years ahead of applications (this is not a flaw at all)
- **We have no idea what specific ideas will have impact and what won't, but as a community we have had huge impact, and continue to do so**
- **The roles of academia and industry are very mixed and intertwined today**
  - A lot of interaction and mutual exchange of ideas
  - People can move back and forth far more easily than before

Thank You

- I feel very fortunate to belong to this community
- The cryptography community is a friendly and supportive one
- I owe a lot to the community, and want to use this opportunity to express my gratitude

Product-Market Fit

- **When you sell what the market is desperately looking for**
- **How do you find it?**
  - It’s extremely hard and requires being very agile
  - The use cases we talk about in academia are often far off the mark (or at least, way ahead of their time)
  - It’s a process of listening and looking at trends: your customers, those who meet with you and say no, RFPs, etc.
- **When do you know if you have it?**
  - When customers are looking for what you have already
  - Sales…

Product-Market Fit

- **Early adopters are crucial, but they are often exceptional**
- **When you have product-market fit, customers buy and use now!**
  - Many people will tell you that your product is cool, much better than what they have now, etc., but it doesn't mean they will buy
    - This is especially true of technologists with a cool solution!
  - If you are replacing something, you need to be much better (10x ?)
  - If you are new, then where will the budget come from?

Focus

- **One of the hardest things as a startup is to say NO**
- **But if you don’t say no, you become a project company**
- **Focus comes in many flavours – the more focused everywhere, the better**
  - The use case
  - The vertical (i.e., types of companies / market segment)
    - Financial, technology, health, education…
    - Enterprises, mid-size companies, small businesses, end consumers
  - Geographical locations

Focus

- **Doesn’t too much focus reduce your market size?**
- **Yes, but:**
  - You don’t have the resources of your competition
    - Marketing – the message depends on your product/s and geography
    - Engineering – how thin do you spread your team; can you be the best?
    - Education – it’s hard to educate your employees (and certainly the market) and the less focus you have, the harder it is
  - You need to conquer a smaller market first, and you need to be **efficient**
- **We failed early at product focus, but eventually turned it to our advantage**
  - But we insisted on focus in other areas (financial and technology, enterprises)
  - Education was always extremely challenging