How to get out of the e-caves!

or

Secure computation in untrusted world

Mohammad Hasan Samadani
Isfahan University of Technology
samadani@morvarid.io

September 17, 2016

CRYPTO HISTORY

ACCESS CRYPTO SUMMIT 2015
#CRYPTOSUMMIT

WHAT ARE PEOPLE LOOKING FOR?

WAS ORWELL RIGHT?

1984

FOUNDATION FOR ECPA

CONCERNS ABOUT BIG BROTHER

1987 COMPUTER SECURITY ACT

NSA OUT OF IT'S CENTRAL ROLE

SECURITY OUT IN THE OPEN

FBI

LAW ENFORCEMENT HAS LEGITIMATE CONCERNS!

DATA IS KEY

NEED NEW TOOLS

OPERATION "ROOT CANAL"

BACK DOOR

STORIES MATTER!

FREAKOUT OVER AT&T ENCRYPTION DEVICE

MILITARY GRADE!

1990's CLIPPER CHIP

HARDWARE-BASED

FRONT DOOR

EASE of USE IS KEY

TRUST

TRANSPARENCY

KEY ESCROW

CAN WE CLOSE THE GAP?

EXPORT CONTROLS

PRIVACY

SECURITY

BALANCE

HOW to STRIKE IT? SAME ENDS, DIFFERENT MEANS

ENCRYPTION IS THE FOUNDATION

EVEN the CAPABILITY TO CREATE YOUR OWN CRYPTOGRAPHY IS EXPORTING

PROBLEMS SHOULD NOT LEAD to OVERREACTION!

GOVERNMENT & INDUSTRY PARTNERSHIPS

COMMERCE PLAYED A LEADING ROLE

NEEDS TO BE TECHNICALLY GROUNDED

REALITY OF GLOBAL INTERCONNECTIVITY

FBI:

TAPPABILITY PRINCIPLE

DO UNBREAKABLE LOCKS LEAD TO SECURITY OR ANARCHY?

EVIDENCE: BIG DATA BREACHES

WEAK ENCRYPTION FACILITATES CRIME

EES KEY ESCROW

WHO GETS TO HOLD THE KEY?

1999 ISSUE of CLEARANCE!

DOJ FBI NSA ⟷ COMMERCE SILICON VALLEY

FEAR THAT EXPORT CONTROLS WOULD LEAVE US WEAK

OTHERS WOULD LEAD!

POLICY SHOULD PROTECT PUBLIC SAFETY

ANDREW FEDERMAN

WHERE DOES ENCRYPTION HAPPEN?

ACCESS CRYPTO SUMMIT 2015

#CRYPTOSUMMIT

INFORMATION IS BROADCAST AT EVERY STAGE

AND ENCRYPTED AND DECRYPTED AT EVERY STAGE

OVER 90% OF THE INTERNET IS UNENCRYPTED!

PHYSICAL CONNECTIONS

IX

SPS

TOWER

LTE/3G

BIG ROUTER

ROUTER

IPSEC

DATA CENTER

PHONE

PHONE ENCRYPTION SOFTWARE

ANY EXCHANGE LEAKS DATA!

LOCK CODE

BIOMETRICS

EASY to BREAK!

802.11

PC

ENCRYPTION SOFTWARE

UNIQUE KEY

NETWORK OF NETWORKS

IP

COMMON LANGUAGE

WHY CARE?

- SAFETY
- SECURITY
- PRIVACY

LOG OUT!

SHUT DOWN

TRUST

CAN'T DO MUCH WITH ENCRYPTED DATA

KEY MANAGEMENT IS THE HARD PART!

KEYBASE SERVICE

OFF THE RECORD

OTR

TIME STAMPS

IP ADDRESS

HEADERS

LOCATION

METADATA

Tor

TARGET: POPULAR, WIDELY ADOPTED SOLUTIONS

THINGS YOU CAN USE TO GET MORE SECURE

VPN

VIRTUAL PRIVATE NETWORK

END to END ENCRYPTION

CAN'T WE JUST FLIP A SWITCH?

HTTP → HTTPS

MONEY, LEGACY SYSTEMS, INFRASTRUCTURE ARE HOLDING US BACK!

LAYERS

- OVERLAY
- APP
- NETWORK

GAPS

- → INTERNET OF THINGS → METADATA
- → ENCRYPTION WITH LESS PROCESSING POWER
- → ENCRYPTION WITH LITTLE/NO INTERFACE
- → USER EDUCATION! BEYOND BROWSERS

ANDREW FEDERMAN

What can we do?

With the well-known crypto

- Encrypt/Decrypt
- Hash
- Sign/Verify
- Key exchange
- End-to-end encryption
- …

With the well-known security tools

- Protection (physical, digital, legal)
- Access control
- Intrusion detection
- Policy enforcement
- Audit
- …

Till the end of this talk, consider all of them in the ideal form.
Your data is protected, channels are secure, intrusion is impossible,…
Use your imagination!

Is it enough? No! It is just a secure e-cave!

We are safe here, making money.

Why should we get out of our secure e-caves?

What can we do now?

- What can you do with encrypted data? Just decrypting them!!?
- How can you share your secret data with others? Using your lawyer!!?
- How can you legally access other's useful data? By commanding or bribing them!!?
- How can you effectively use your encrypted data in the cloud? Oh, we do not use the cloud at all!
- How can you use other's private data in your computation and analysis?
- …

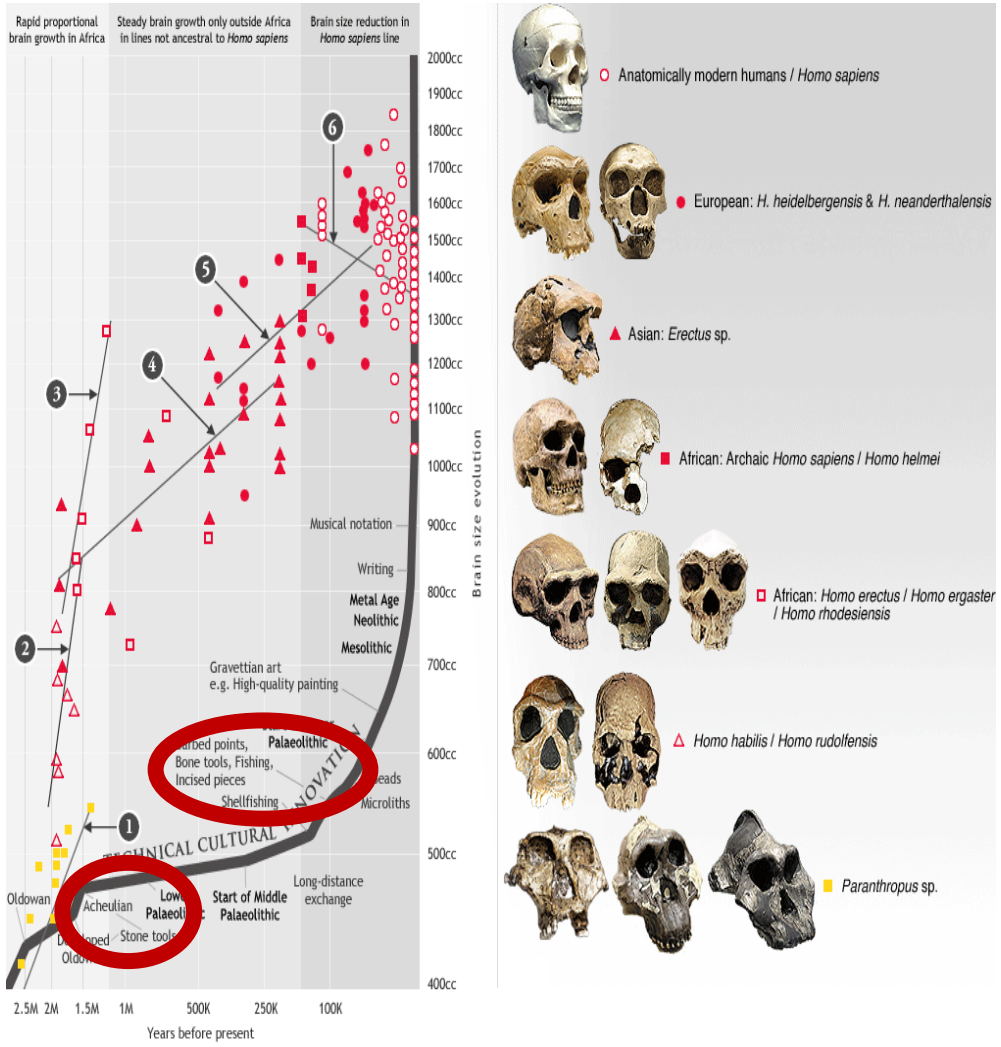
Is it possible to compute on encrypted data?
Is it possible to join a computation and find out the output without revealing the private inputs?

Origins of human intelligence: The chain of tool-making and brain evolution

Kwang Hyun Ko
Hanyang University, kwhyunko@gmail.com

Abstract

Although the definition of intelligence is debatable, it can be allocated to only one anatomical location: the brain. Arguments regarding general measures of animal intelligence and discussions of its evolution up to the Neanderthals arise only because hominids have evolved to have larger brains; i.e., they have become more "intelligent". Hominids clearly evolved in the past, but whether evolution is still ongoing is debated. Ironically, because hominids have created technologies and innovations to aid their survival, their evolution has included adaptation to the environment generated by their inventions. Similar to the recent evolution of ADHD traits or gluten tolerance, the hominid brain has undergone major changes over the past seven million years due to man-made habitats and technologies. Tool-making creates an environment conducive to increased social interactions, as it facilitates increased provisioning and protection, while increased opportunities for interactions and observations lead to advances in tool-making. These changes have been offset by the concurrent evolution of language and tool-making. Biologically, hominid brains have increased in size in areas where tool-making and language-processing coincide. This increase in brain size allowed advanced provisioning and tools, including the use of fire, and the technological advances during the Palaeolithic that stood on the shoulders of the previous evolutionary innovations of bipedalism and versatile hands enhanced the momentum of brain evolution. The beginnings of the reciprocal cause and effect between brain evolution and tool-making cannot be identified. The applicability of the hunting and fire hypotheses to the evolution of human intelligence is further discussed.



How secure your cave is, you need to get out.
But, that requires tools!

Let’s see what’s out there?

We <u>do not</u> concern about eavesdroppers, Man-In-The-Middle, …

We concern about other parties in the joint computation

Semi-honest adversaries

- Follow the protocol
- Try to learn anything more

Malicious adversaries

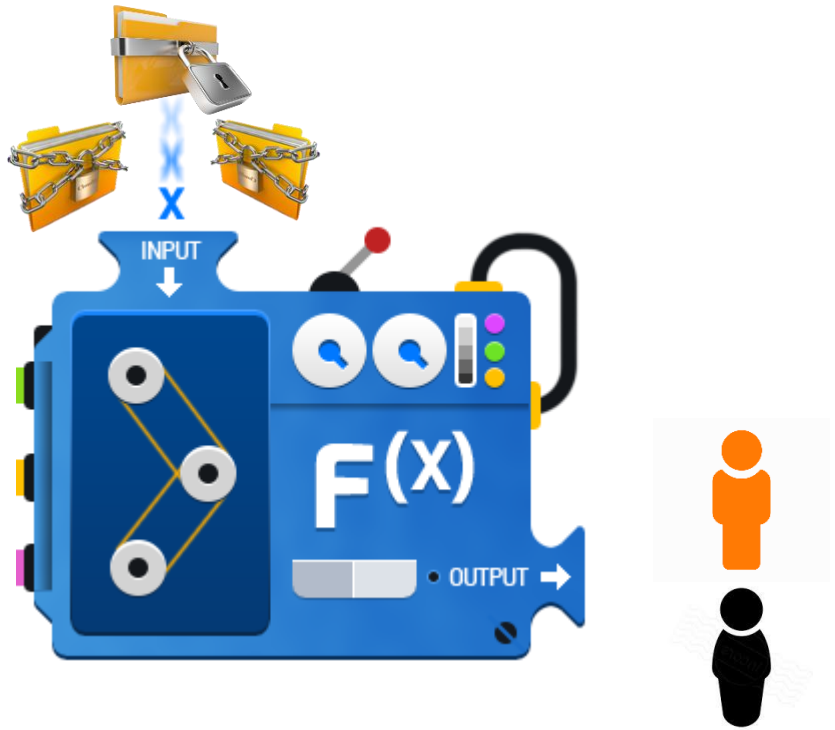
- Arbitrarily misbehave
- Abort

What we have? What we want?

Each party has a private input

A function of the private inputs is needed

(output might be different for each party)

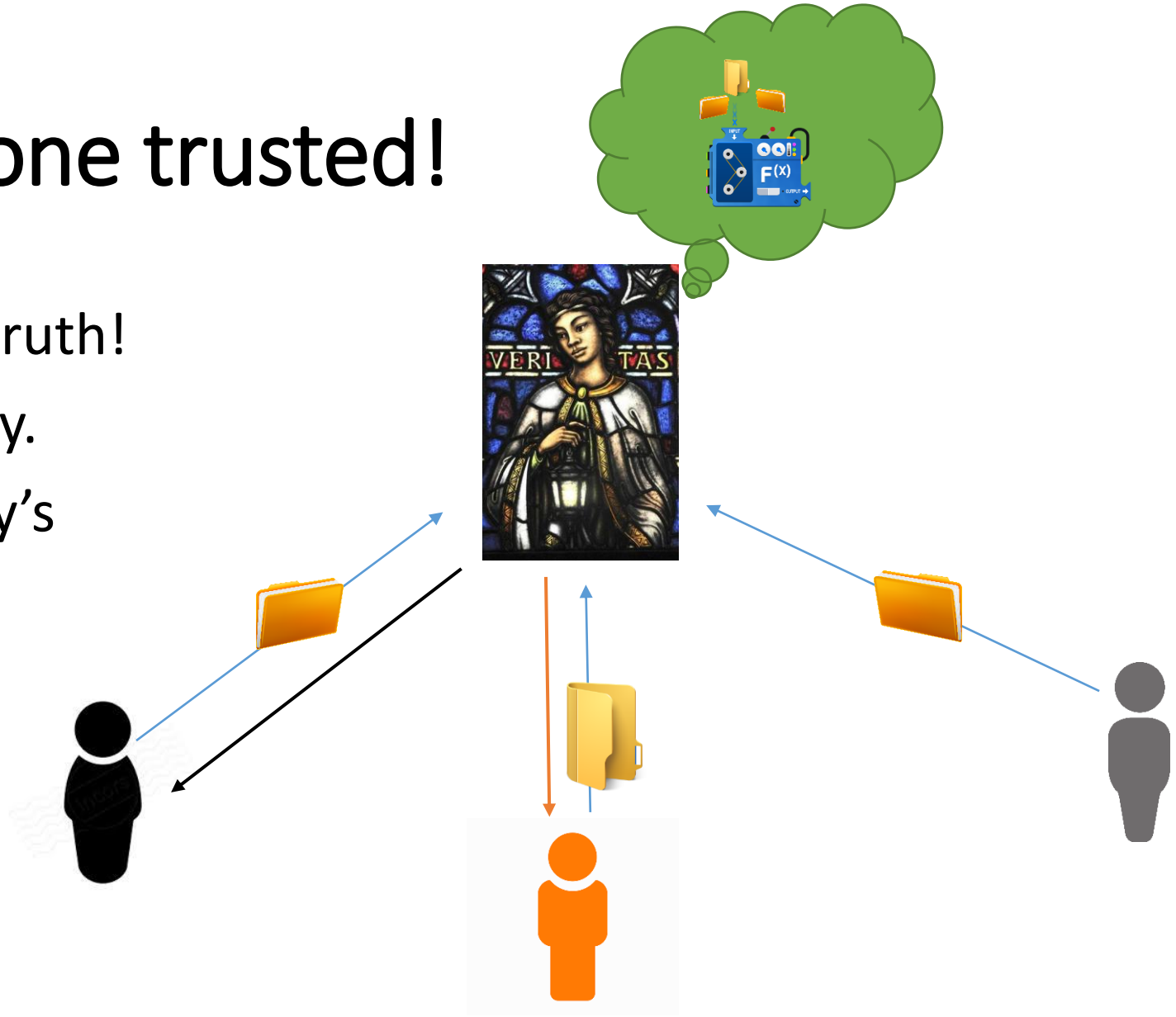


Examples

- Cross-checking two lists of suspicious persons
- Comparing two genomes or finding a genome in a genome DB
- Private email, search,…
- Secure and private cloud services
- Private location based services
- Voting
- IDS with private signatures on private traffic
- Outsourcing any task on private data
- …

Let’s find someone trusted!

- She is the goddess of truth!
- She computes correctly.
- She delivers each party’s output honestly.



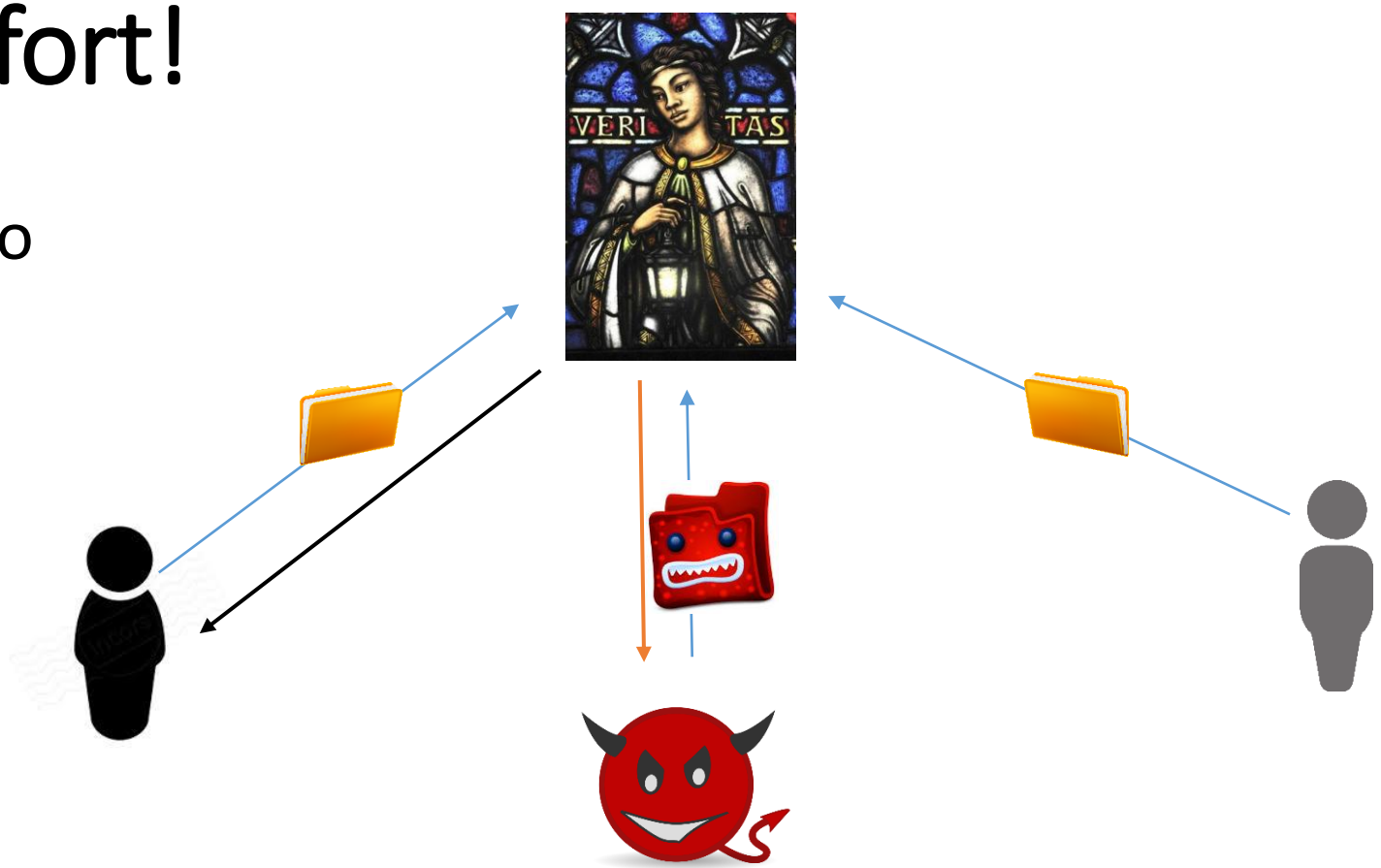
Adversary's best effort!

The adversary is just able to choose his own input.

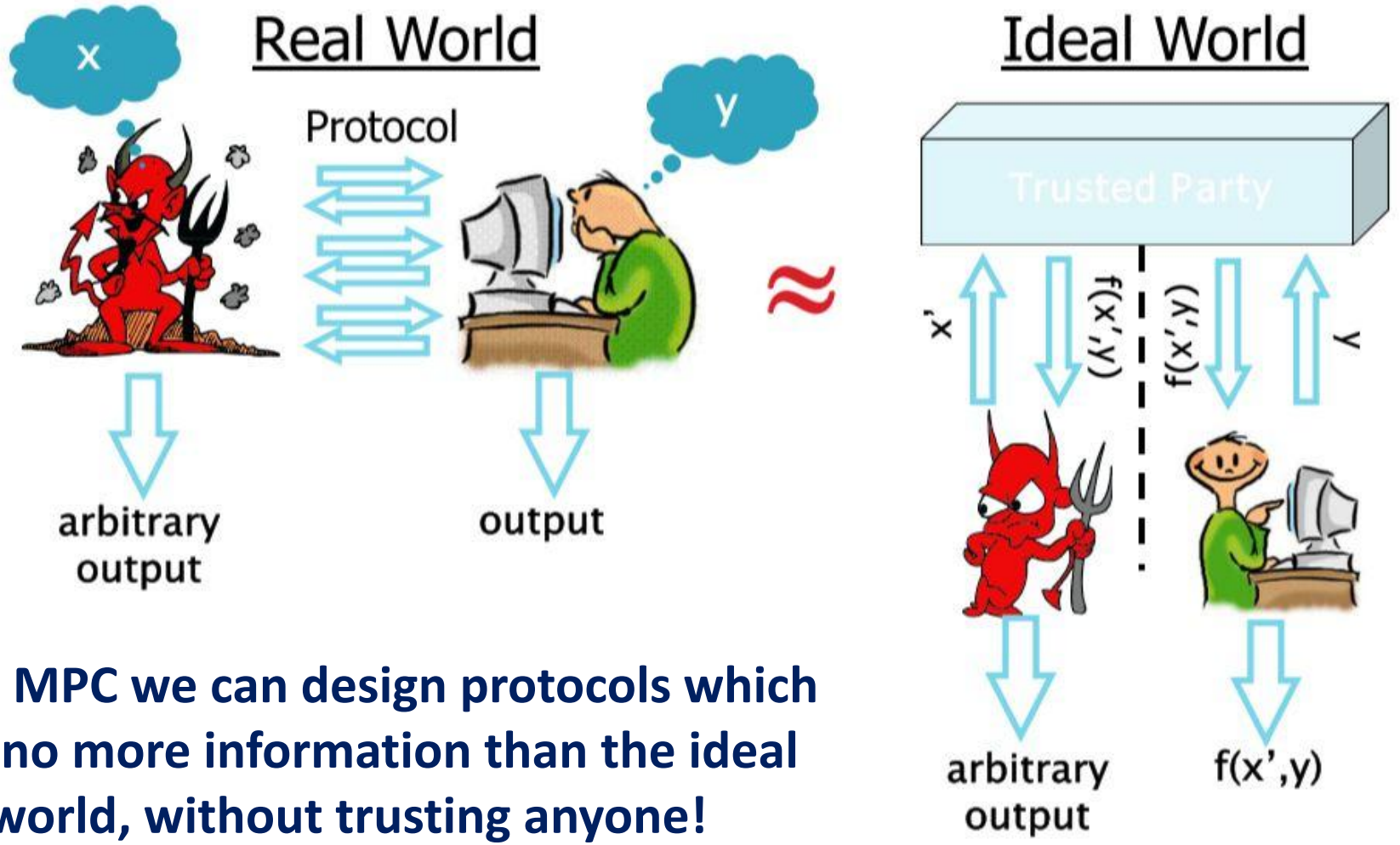
More security cannot be imagined!

It is secure by definition!

Bad news; there is no such goddess.



Good news; Multi-Party Computation



Using MPC we can design protocols which leak no more information than the ideal world, without trusting anyone!

Two and Multi Party Computation

Specific Constructions

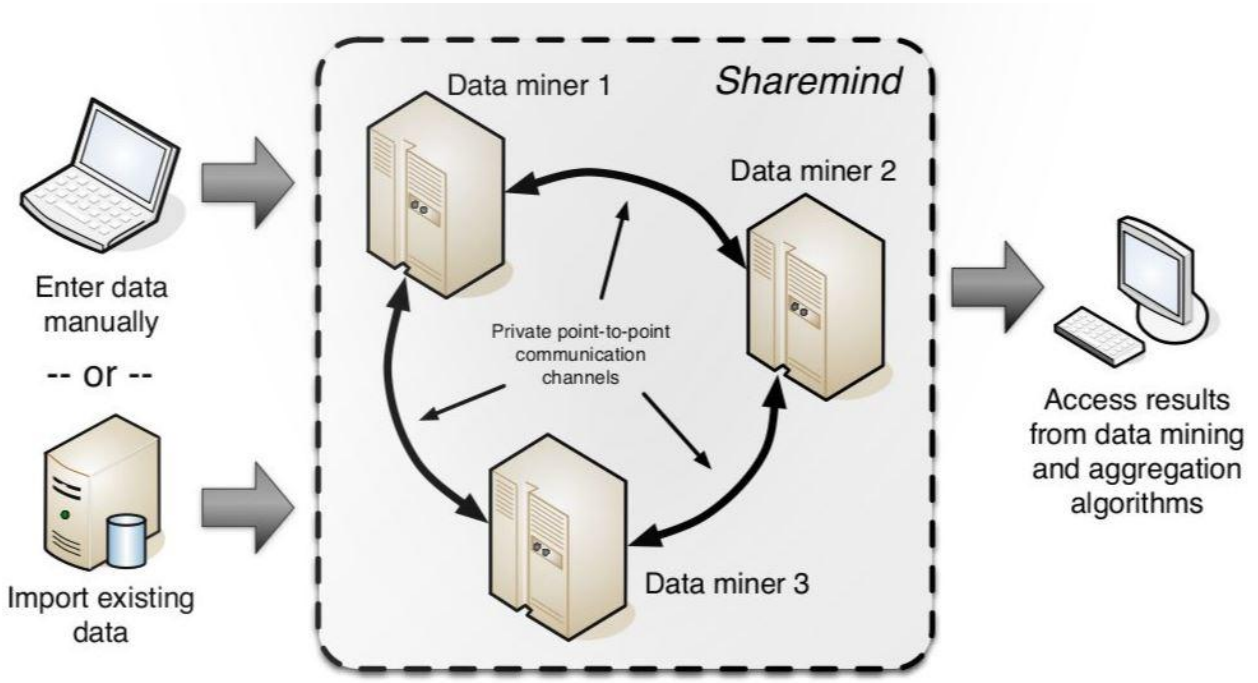
- Using the function's properties to design efficient protocols
- Very efficient protocols can be designed for semi-honest setting
- It is possible (but difficult) for malicious setting

General Constructions

- Any efficiently computable function can be evaluated securely
- Both two and multi party settings
- Communication and round complexity is very high
- Inefficient when number of parties is large

General Constructions in practice

- Consider any (1 or more) number of input owners
- We usually use 3-5 parties to run the protocol
- Practical and efficient for many functions
- Computation parties might be considered semi-honest or malicious



There is also Fully Homomorphic Encryption

It is possible to evaluate any function on encrypted data

1. Alice encrypts her data using a FHE scheme
2. Sends it to Bob
3. Bob evaluates any desired function on encrypted data and finds outs the encrypted result
4. Encrypted result is sent back to Alice
5. Alice decrypts and finds out the result

- 80s, existence proved
- 2009, First instance proposed

- Secure computation in **one round**
- Communication and round complexity is efficient
- Computation is very high!

- Now, cannot be used in practice!
  - But for very simple functions

MPC in action

- Sugar beet biding in Denmark since 2009
- Cross matching of suspicious persons in Israel
- Virtual HSM in Israel
- Survey on Tax information in Estonia
- Survey on IT companies in Estonia
- Location based services in Estonia
- Private satellite collision prediction, NASA, ESA,…
- Collaborative medical research between several drug companies
- Private supply chain management by SAP
- Emerging cloud services by Microsoft

"Any sufficiently advanced technology is indistinguishable from magic."
– Arthur C. Clarke

Be the magician.

Our magic

- Secret sharing schemes
- Sigma protocols and Zero-knowledge proof of knowledge
- Commitment protocols
- Oblivious Transfer protocols
- Homomorphic Encryption schemes
- Functional Encryption schemes

Thank you.