

# Global cyber surveillance: how to defend against?

A sample of a few cryptographic techniques



*Giuseppe Bianchi*  
May 6, 2021



consorzio nazionale  
interuniversitario  
per le telecomunicazioni

# What we will learn today?

## → **Perfect forward Secrecy**

⇒ Must-have post-Snowden requirement

## → **Certificate transparency**

⇒ blockchain-type data structures for public verification

## → **«trivial» Secure Multiparty Computation**

⇒ How to compute over encrypted data

# mass surveillance: who?

## List of government mass surveillance projects

From Wikipedia, the free encyclopedia

*Main article: [Mass surveillance](#)*

*This list is [incomplete](#); you can help by [adding missing items](#) with [reliable sources](#).*

This is a **list of known government surveillance projects** and related databases throughout the world.

### Contents [\[hide\]](#)

- [International](#)
  - [European Union](#)
- [National](#)
  - [Australia](#)
  - [China](#)
  - [France](#)
  - [Germany](#)
  - [India](#)
  - [Russia](#)
  - [Sweden](#)
  - [Switzerland](#)
  - [United Kingdom](#)
  - [United States](#)
- [Unclear origin](#)
- [Recently discontinued](#)
- [See also](#)
- [References](#)

WIKIPEDIA  
The Free Encyclopedia

[Main page](#)  
[Contents](#)  
[Current events](#)  
[Random article](#)  
[About Wikipedia](#)  
[Contact us](#)  
[Donate](#)

[Contribute](#)

[Help](#)  
[Learn to edit](#)  
[Community portal](#)  
[Recent changes](#)  
[Upload file](#)

[Tools](#)

[What links here](#)  
[Related changes](#)  
[Special pages](#)  
[Permanent link](#)  
[Page information](#)  
[Cite this page](#)  
[Wikidata item](#)

[Print/export](#)  
[Download as PDF](#)

# mass surveillance: who?

## List of government mass surveillance projects

WIKIPEDIA  
The Free Encyclopedia

[Main page](#)  
[Contents](#)

### Australia [\[ edit \]](#)

*Main article: [Mass surveillance in Australia](#)*

- In August 2014 it was reported that the Australian Security Intelligence Organisation (ASIO) had been conducting surveillance on a large number of people without a warrant.
- It was reported<sup>[3]</sup>

### China [\[ edit \]](#)

*Main article: [Mass surveillance in China](#)*

- **Golden Shield Project**: A division of the government that gathers biometric data on all Chinese citizens.
- **Monitoring Bureau**: A division of the government that monitors the activities of all Chinese citizens.
- **Public Information System**: A system that collects and analyzes data on all Chinese citizens.
- **Social Credit System**: A system that evaluates the creditworthiness of all Chinese citizens.

### France [\[ edit \]](#)

- **Frenchelon**: A data collection system used by the French government to monitor internet and telephone communication.

### Russia [\[ edit \]](#)

- **SORM**: A technical system used by the [Federal Security Service of the Russian Federation](#) to monitor internet and telephone communication.
- **Yarovaya Law** is a piece of anti-terrorist legislation that includes a requirement to store all phone call and text messaging data, as well as providing cryptographic backdoors for security services.

### Sweden [\[ edit \]](#)

- **Titan traffic database**: A database established by the [Swedish National Defence Radio Establishment](#) (Swedish: Försvarets radioanstalt, FRA) where call detail records (CDRs) of telephony and internet traffic and transaction data (IPDRs) concerning international telecommunications are stored.<sup>[13]</sup>
- **X-Keyscore**: A system used by the United States National Security Agency for searching and analysing internet data about foreign nationals. FRA has been granted access to the program.<sup>[14]</sup>

### Switzerland [\[ edit \]](#)

- **Onyx**: A data gathering system maintained by several [Swiss intelligence agencies](#) to monitor military and civilian communications, such as e-mails, telefax and telephone calls. In 2001, Onyx received its second nomination for the ironically-named "[Big Brother Award](#)".<sup>[15]</sup>

### United Kingdom [\[ edit \]](#)

*Further information: [Mass surveillance in the United Kingdom](#)*

- **Impact Nominal Index**: The Impact Nominal Index or INI is a computer system that enables the UK police force to establish whether other relevant authorities are holding information regarding a person of interest.<sup>[16]</sup>
- **Interception Modernisation Programme**: An initiative to extend the UK government's capability to lawfully intercept and store communications data in a central database.<sup>[17]</sup>
- **Mastering the Internet** (MTI): A clandestine mass surveillance program led by the British intelligence agency GCHQ. Data gathered by the GCHQ include the contents of email messages, entries on the social networking platform Facebook and the web browsing history of internet users.<sup>[18]</sup>
- **UK National DNA Database** (NDNAD): It is also the oldest national DNA database in the world.<sup>[19]</sup> Since its establishment in 1995, the database has grown to include DNA samples from 2.7 million individuals, or 5.2% of the UK's population, many of whom have neither been charged with, or convicted of, any offence.<sup>[19]</sup>
- **Tempora**: Launched in the autumn of 2011, this initiative allows the GCHQ to set up a large-scale buffer that is capable of storing internet content for 3 days and



# Remember Snowden's revelations, 2013

WIKIPEDIA  
The Free Encyclopedia

[Main page](#)

[Contents](#)

**Australia** [\[ edit \]](#)

*Main article: [Mass surveillance in Australia](#)*

- In August 2014 it was reported that the Australian Security Intelligence Organisation had intercepted communications from the United States without a warrant.
- It was reported<sup>[3]</sup> that the Australian Security Intelligence Organisation had intercepted communications from the United States without a warrant.

**China** [\[ edit \]](#)

*Main article: [Mass surveillance in China](#)*

- **Golden Shield Project**: A division of the government that monitors internet activity.
- The **Integrated Joint Operations Command** gathers biometric data from citizens.
- **Monitoring Bureau**: A bureau of the Ministry of State Security that monitors internet activity.
- **Public Information Service**: A service that provides information to the public.
- **Social Credit System**: A system that evaluates the creditworthiness of citizens.

**France** [\[ edit \]](#)

- **Frenchelon**: A data collection program by the French government.

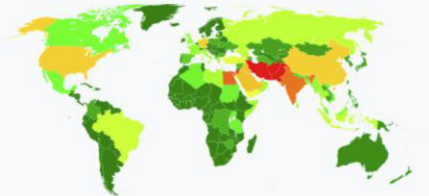
**United States** [\[ edit \]](#)

*Further information: [Mass surveillance in the United States](#)*

- **Boundless Informant**: A system deployed by the [National Security Agency](#) to analyze global electronic information. In March 2013, Boundless Informant gathered 14 billion data reports from [Iran](#), 6.3 billion from [India](#), and 2.8 billion from the [United States](#).<sup>[23]</sup>
- **BULLRUN**: a highly classified U.S. [National Security Agency](#) program to preserve its ability to eavesdrop on encrypted communications by influencing and weakening encryption standards, by obtaining master encryption keys, and by gaining access to data before or after it is encrypted either by agreement, by force of law, or by computer network exploitation (hacking).
- **Carnivore**: A system implemented by the Federal Bureau of Investigation that was designed to monitor email and electronic communications. Apparently replaced by commercial software such as [NarusInsight](#).
- **Comprehensive National Cybersecurity Initiative**
- **DCSNet**: The [Federal Bureau of Investigation](#) (FBI)'s [point-and-click](#) surveillance system that can perform instant wiretaps on any telecommunications device located in the [United States](#).<sup>[24]</sup>
- **Fairview**: A [mass surveillance](#) program directed at foreign mobile phone users.
- **Financial Crimes Enforcement Network**: A bureau of the [Department of the Treasury](#) that collects and analyzes financial transactions in order to combat [financial crimes](#).
- **ICREACH**: Surveillance [frontend GUI](#) that is shared with 23 government agencies, including the [CIA](#), [DEA](#), and [FBI](#), to search illegally collected personal records.
- **Magic Lantern**: A [keystroke logging software](#) deployed by the FBI in the form of an [e-mail attachment](#). When activated, it acts as a [trojan horse](#) and allows the FBI to decrypt user communications.<sup>[25]</sup>
- **Main Core**: A personal and financial database storing information of millions of U.S. citizens believed to be threats to [national security](#).<sup>[26]</sup> The data mostly comes from the [NSA](#), [FBI](#), [CIA](#), as well as other government sources.<sup>[26]</sup>
- **MAINWAY**: NSA database containing [metadata](#) for hundreds of billions of [telephone calls](#) made through the four largest [telephone carriers](#) in the United States.
- **Monitoring of email messages**: Entries on the social networking platform [Facebook](#) and the [web browsing history](#) of internet users.
- **UK National DNA Database** (NDNAD): It is also the oldest national DNA database in the world.<sup>[19]</sup> Since its establishment in 1994, it has grown to include DNA samples from 2.7 million individuals, or 5.2% of the UK's population, many of whom have neither been charged with nor convicted of a crime.
- **Tempora**: Launched in the autumn of 2011, this initiative allows the [GCHQ](#) to set up a large-scale [buffer](#) that is capable of storing vast amounts of data for future analysis.



## National Security Agency surveillance



Map of global NSA data collection, with countries subject to the most data collection shown in red

### Programs

[\[hide\]](#)

#### Pre-1978

[ECHELON](#) · [MINARET](#) · [SHAMROCK](#) · [PROMIS](#)

#### Since 1978

[Upstream collection](#) · [BLARNEY](#) · [FAIRVIEW](#) · [Main Core](#) · [ThinThread](#) · [Genoa](#)

#### Since 1990

##### RAMPART-A

#### Since 2001

[OAKSTAR](#) · [STORMBREW](#) · [Trailblazer](#) · [Turbulence](#) · [Genoa II](#) · [Total Information Awareness](#) · [President's Surveillance Program](#) ([Terrorist Surveillance Program](#))

#### Since 2007

[PRISM](#) · [Dropmire](#) · [Stateroom](#) · [Bullrun](#) · [MYSTIC](#) · [MonsterMind](#) (alleged)

#### Databases, tools etc.

[PINWALE](#) · [MARINA](#) · [Main Core](#) · [MAINWAY](#) · [TRAFFICTHIEF](#) · [DISHFIRE](#) · [XKeyscore](#) · [ICREACH](#) · [BOUNDLESSINFORMANT](#)



# And of course surveillance from big OTT as well!

## “Surveillance is the business model of the Internet.”

Everyone is under constant surveillance by many companies, ranging from social networks like Facebook to cellphone providers. This data is collected, compiled, analyzed, and used to try to sell us stuff. Personalized advertising is how these companies make money, and is why so much of the internet is free to users. **We're the product, not the customer.**

### Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google - Bruce Schneier

[privacy-be-very-scared-analyst-suggests/](#)

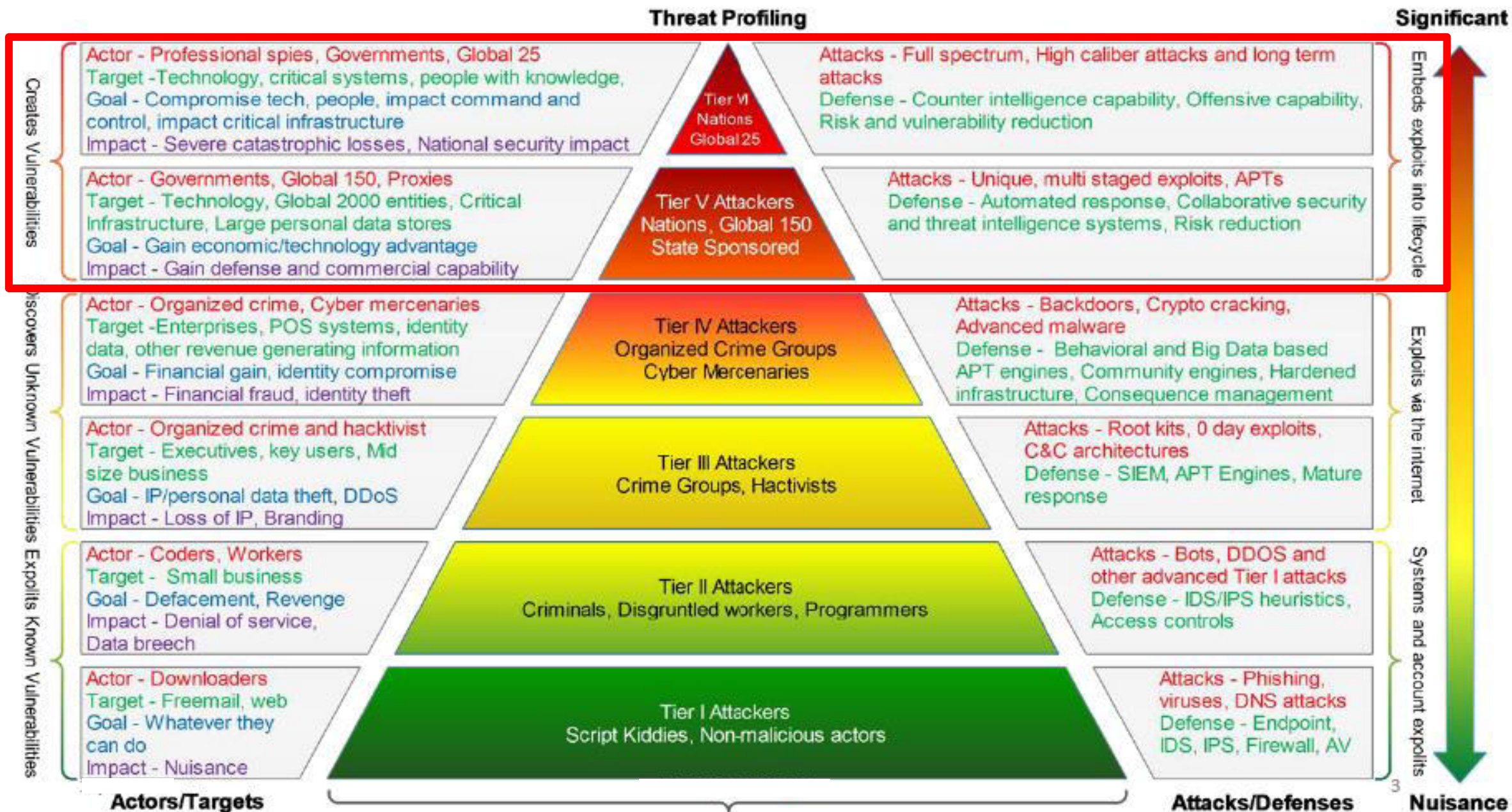
Douglas J. Leith  
School of Computer Science & Statistics,  
Trinity College Dublin, Ireland  
25<sup>th</sup> March, 2021

**Abstract**—We investigate what data iOS on an iPhone shares with Apple and what data Google Android on a Pixel phone shares with Google. We find that even when minimally configured and the handset is idle both iOS and Google Android share data with Apple/Google on average every 4.5 mins. The phone IMEI, hardware serial number, SIM serial number and IMSI, handset phone number etc are shared with Apple and Google. Both iOS and Google Android transmit telemetry, despite the user explicitly opting out of this. When a SIM is inserted both iOS and Google Android send details to Apple/Google. iOS sends the MAC addresses of nearby devices, e.g. other handsets and the home gateway, to Apple together with their GPS location. Users have no opt out from this and currently there are few, if any, realistic options for preventing this data sharing.

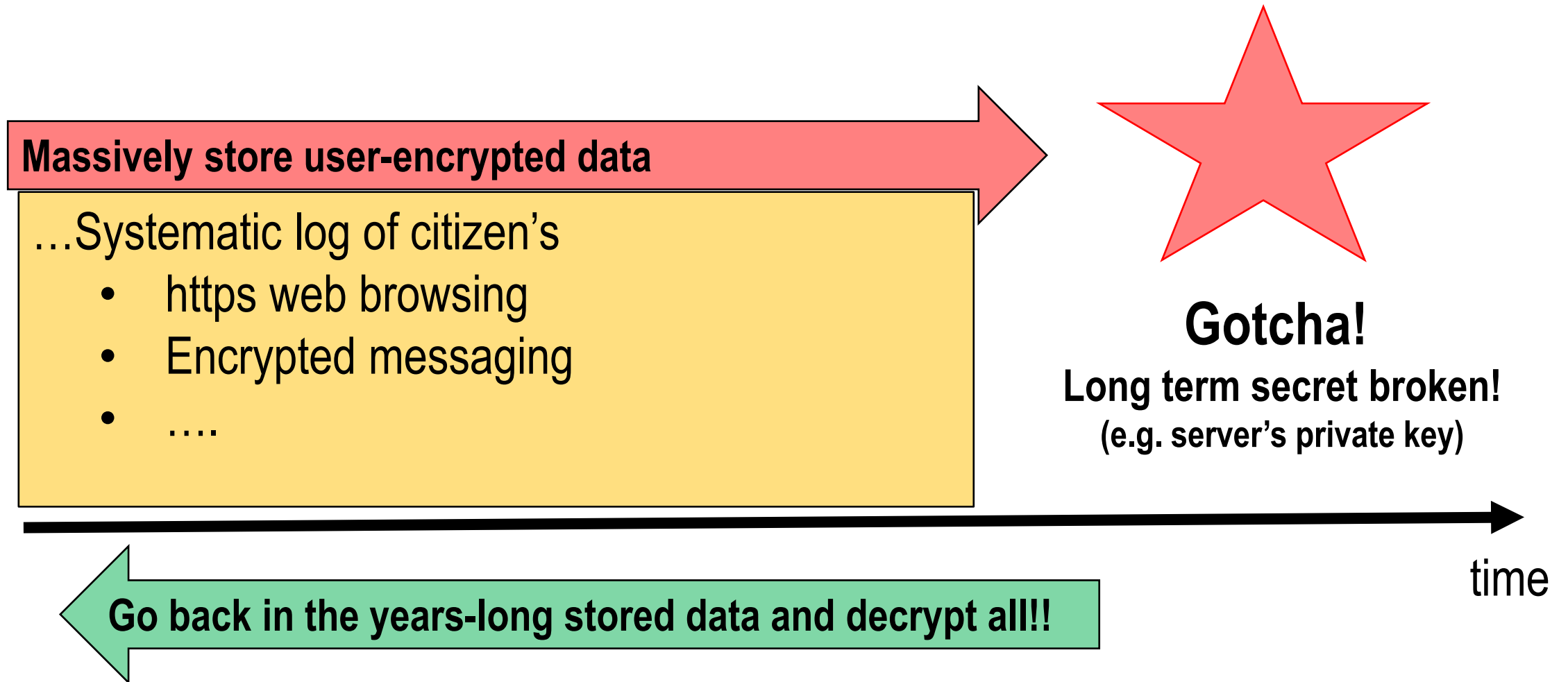
===== Giuseppe Bianchi =====



# High tier adversary's model!



# **Time not an issue for «them» a.k.a.: standard encryption is NOT enough**





# **A must today: (Perfect) Forward Secrecy**

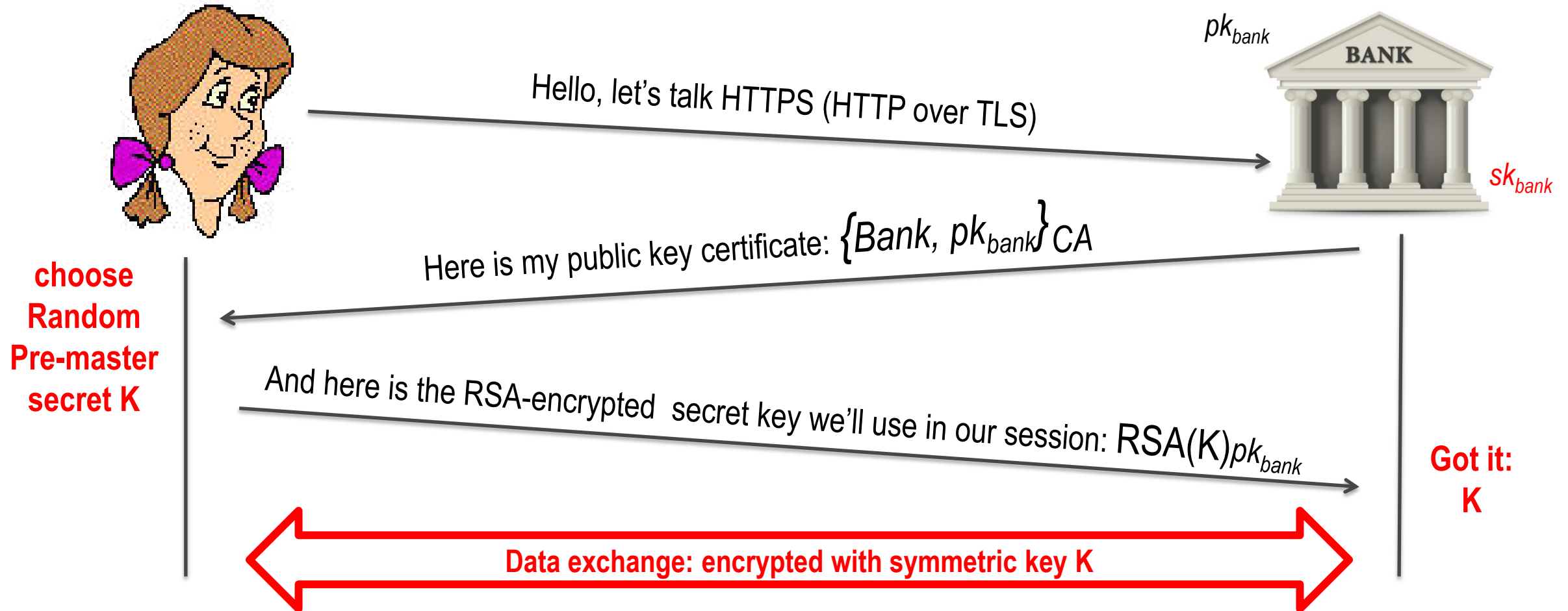
## **Informally:**

if a long-term private key (e.g. of the server) is compromised at some time, this should NOT affect data delivered **BEFORE** such time!

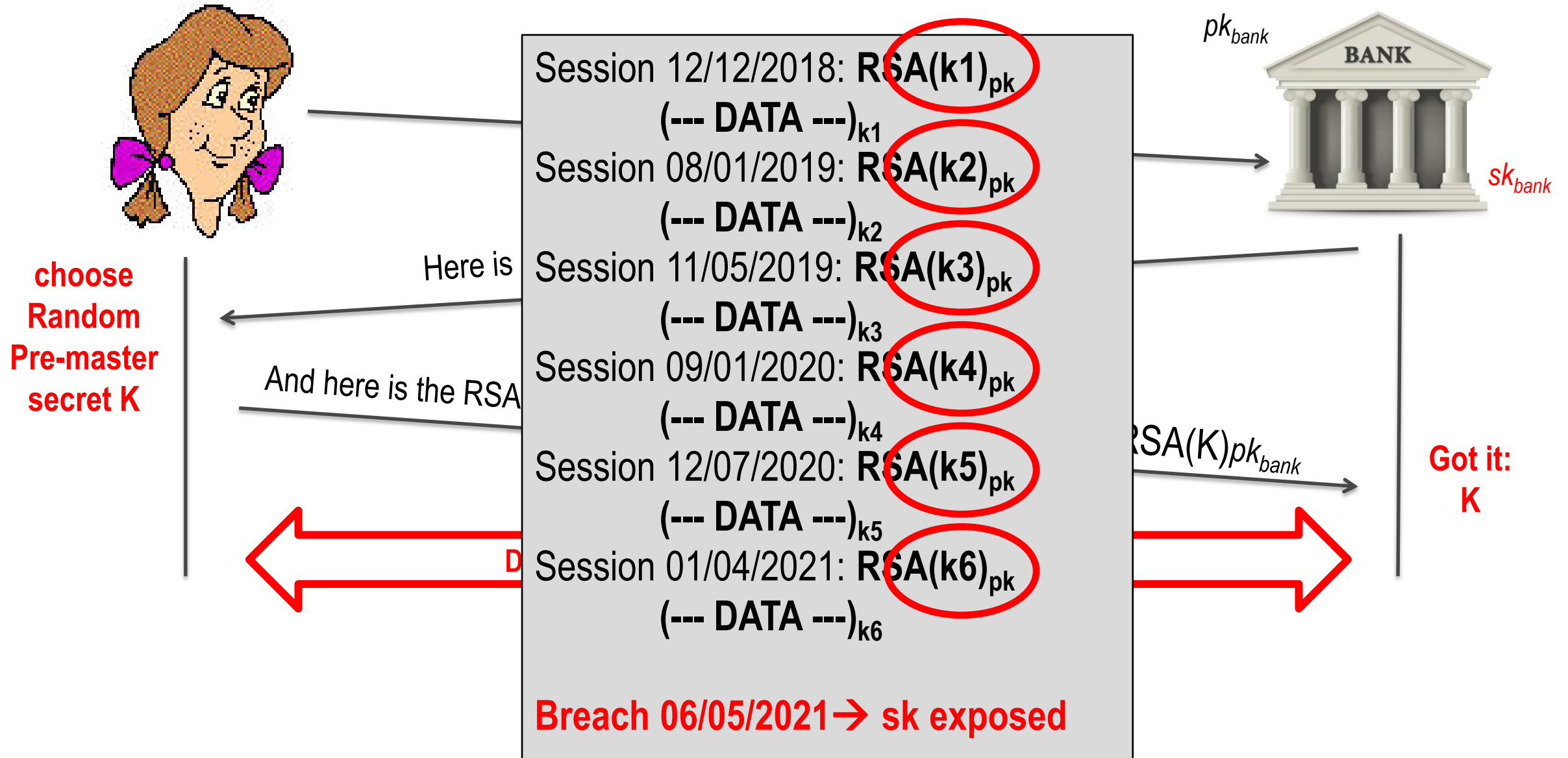
## **More technically:**

session keys will not be compromised even if long-term secrets used in the session key exchange are compromised

# Traditional TLS: RSA key transport, no PFS

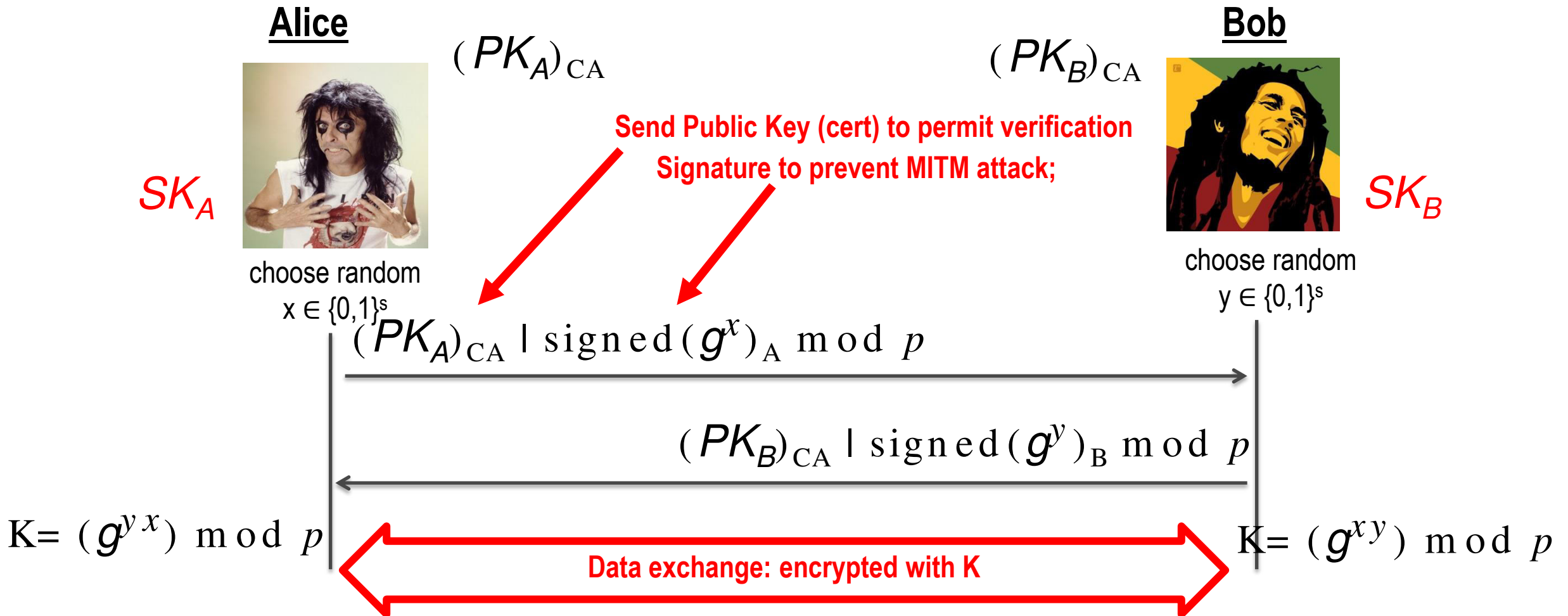


# Traditional TLS: RSA key transport, no PFS





# PFS - how to? Ephemeral Diffie-Hellman!



**If SK breaks, (ephemeral) session keys are not revealed! Forward Secrecy!**

# **Why you should upgrade to TLSv1.3?**

## **Perfect Forward Secrecy becomes mandatory!**

### **→ TLS1.2: four key handshake methods supported**

- ⇒ RSA key transport (most common, no PFS))
- ⇒ Diffie-Hellman Anonymous (vulnerable to MITM)
- ⇒ Diffie-Hellman Fixed (no PFS)
- ⇒ Diffie-Hellman Ephemeral

### **→ TLS1.2: removed all, except one!**

- ⇒ Diffie-Hellman Ephemeral
- ⇒ Moreover, Authenticated Encryption mandatory as well
  - To clear the original MAC-then-Encrypt flaw (e.g. POODLE attack)

# What about PFS vs pre-shared key?

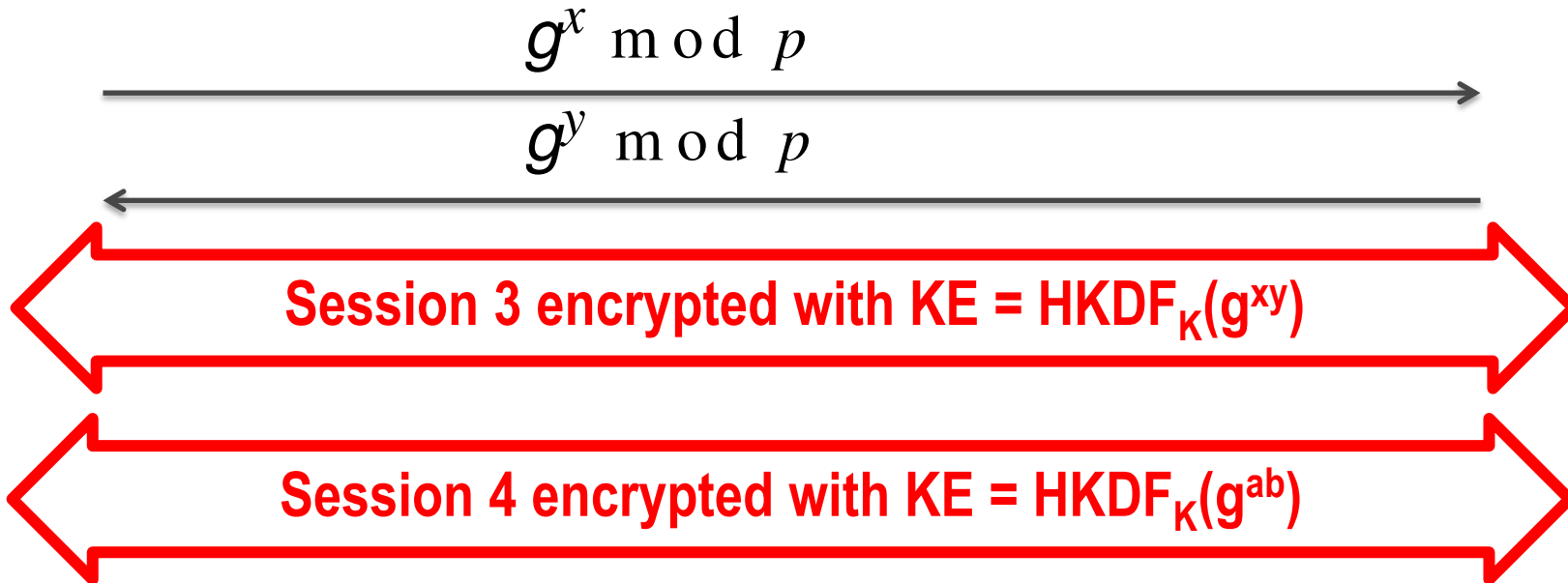
WPA2 key  
 $K = 31EF21456$



WPA2 key  
 $K = 31EF21456$



**We must use same static K... how to get PFS then???**

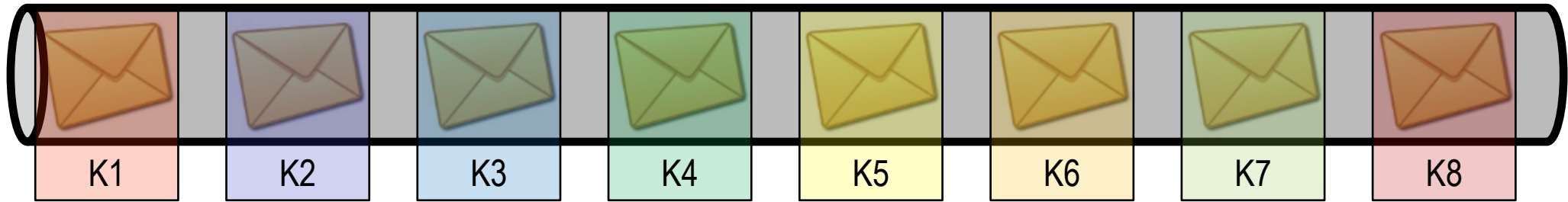


... ..



# Does your messaging app guarantee PFS?

~~E2e encryption: not even your provider can see~~



E2e encryption **with PFS**: Not only your provider cannot see,  
But **even if it logs all data and gets access later on to your  
key, he cannot decrypt past messages!**



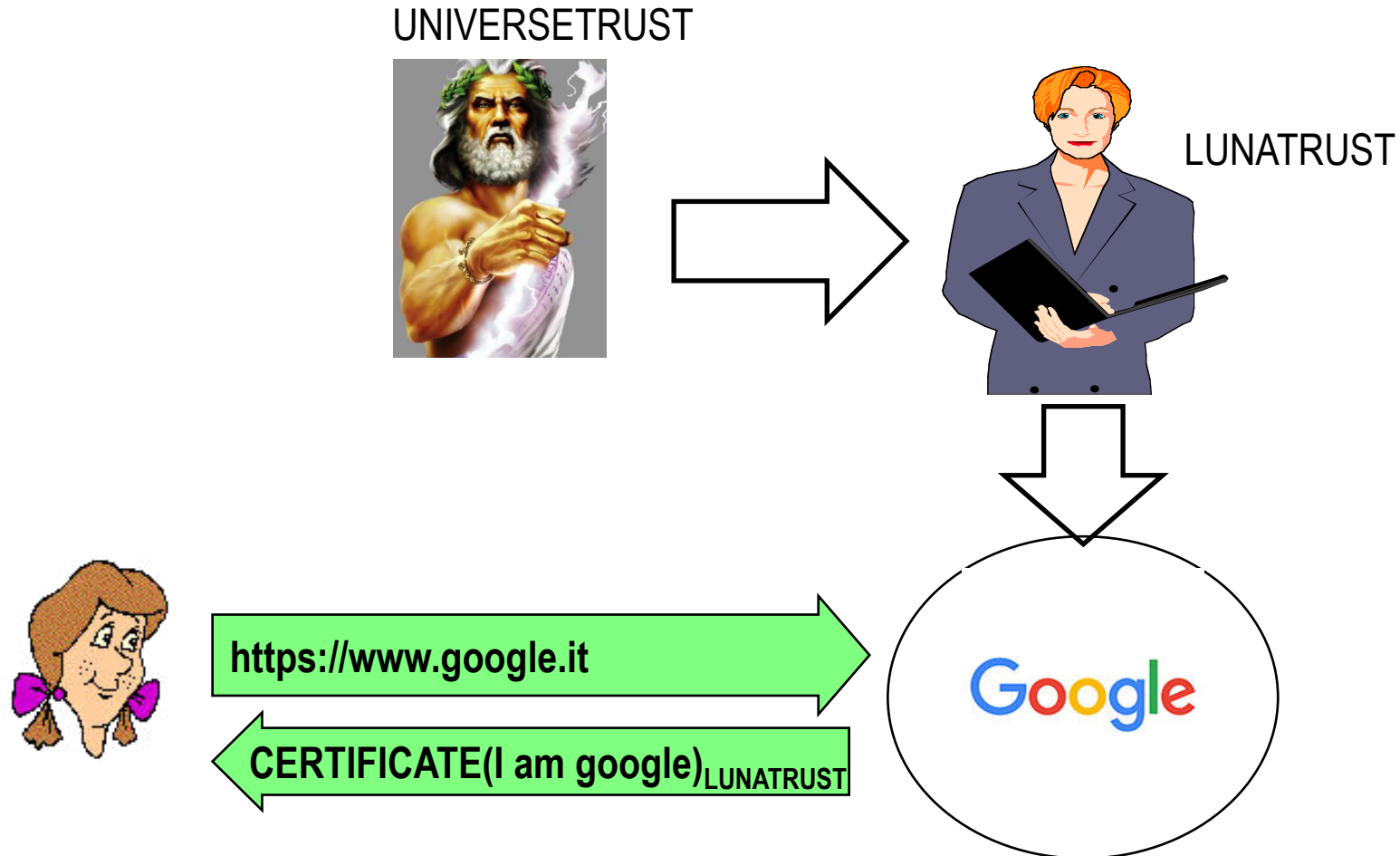
**Signal's Double Ratchet: brilliant solution!**  
(too tech for today)



# Back to mass surveillance: What about fake certificates?

a.k.a.: how transparency can help solving security problems

# Web security pillar: Certificate Authorities ARE trusted!





# Fact: trusted CA assumption at stake

With powerful threats (governments),  
and many players which can «make mistakes»  
the security of the PKI model is getting weaker and weaker

Published: 09 Jan 2015

re  
SS  
at

Netcraft has found dozens of fa  
Some of these certificates may  
customers. Successful attacks  
and forwarding it to the bank.  
authentication credentials, or n

## Enhancing digital certificate security

The fake certificates bear com  
As the certificates are not sign

Posted: Thursday, January 3, 2013

g+1 183

Tweet 300

Facebook Mi piace

Sections

Why 'b  
SSL ce

- **Google's VALID fake Certificates mistakenly (?) issued**
  - by TurkTrust (2012), ANSSI France (2013), etc
- **Smaller CAs: compromised**
  - ⇒ Holland: Dgnotar
  - ⇒ Malaysia: DigiCert sdn. Bhd.
  - ⇒ etc

Engineer

ected and blocked an unauthorized digital certificate for the "\*.google.com"  
ly and found the certificate was issued by an [intermediate certificate authority](#)  
a Turkish certificate authority. Intermediate CA certificates carry the full  
has one can use it to create a certificate for any website they wish to

certificate revocation metadata on December 25 to block that intermediate CA,  
other browser vendors. TURKTRUST told us that based on our information,

## TLS Proxies: Friend or Foe?

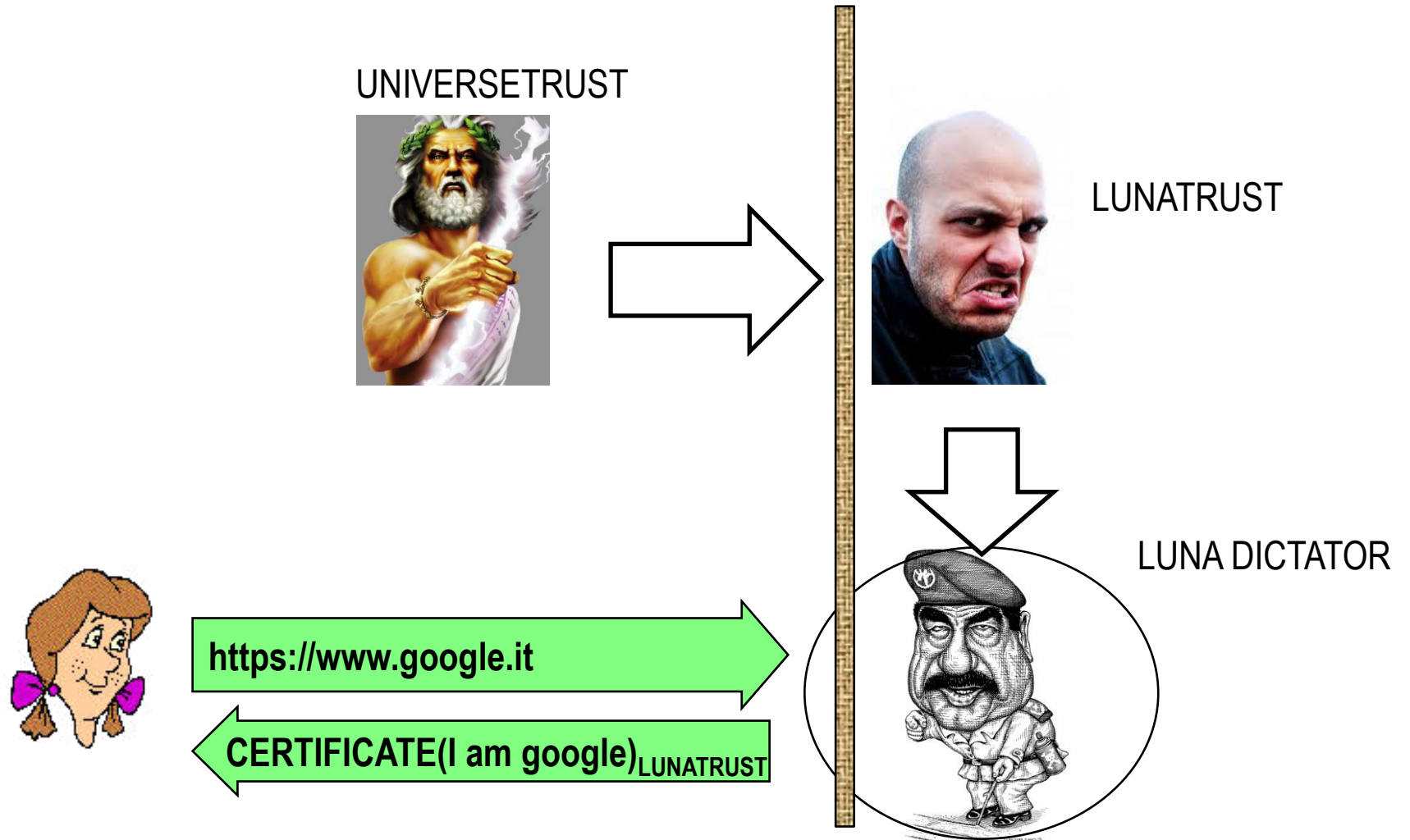
Online banking apps for mobile  
is far from trivial, and mobile  
of iOS-based banking apps test  
authenticity of SSL certificates  
manual tests by Leibniz Univer  
may also be vulnerable if a us

Our actions add  
Chrome again in  
though connecti

Since our priorit  
further discussion and careful consideration.

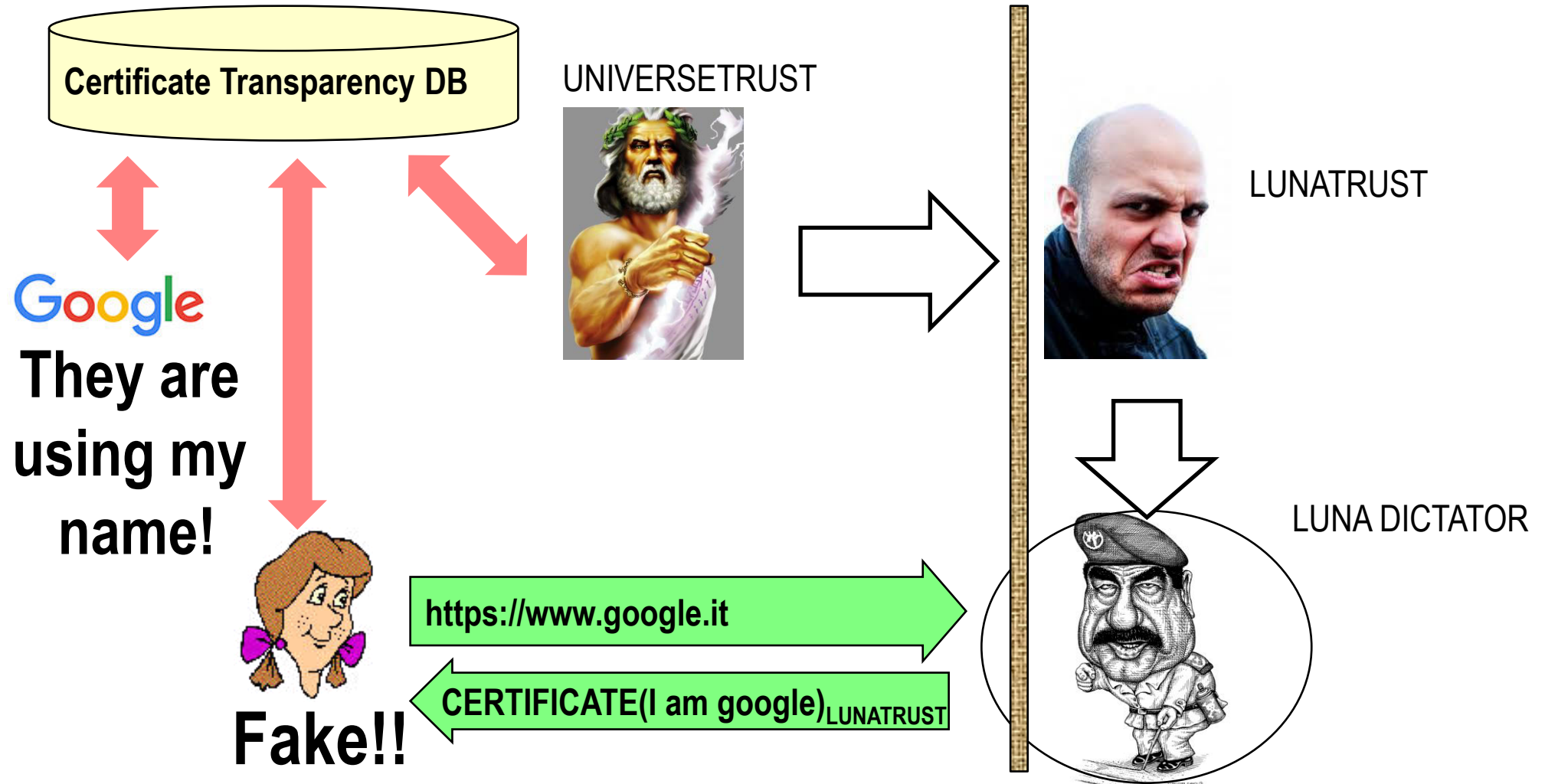
Mark O'Neill, Scott Ruoti, Kent Seamons, Daniel Zappala  
Brigham Young University  
Department of Computer Science  
Provo, UT 84602

# Mass surveillance with fake certificates...



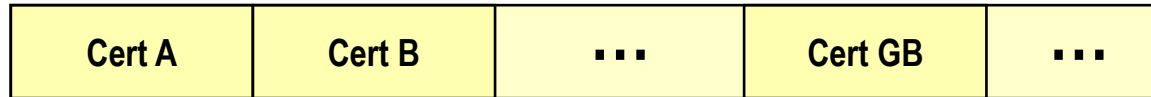
# How to cope with malicious CAs?

Idea: gigantic worldwide DB which anyone can check!



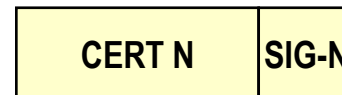
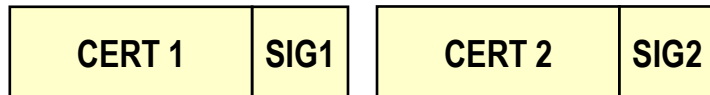


# How to implement such gigantic Database of certificates?



**Req. 1**  
**Verify one cert at a time**

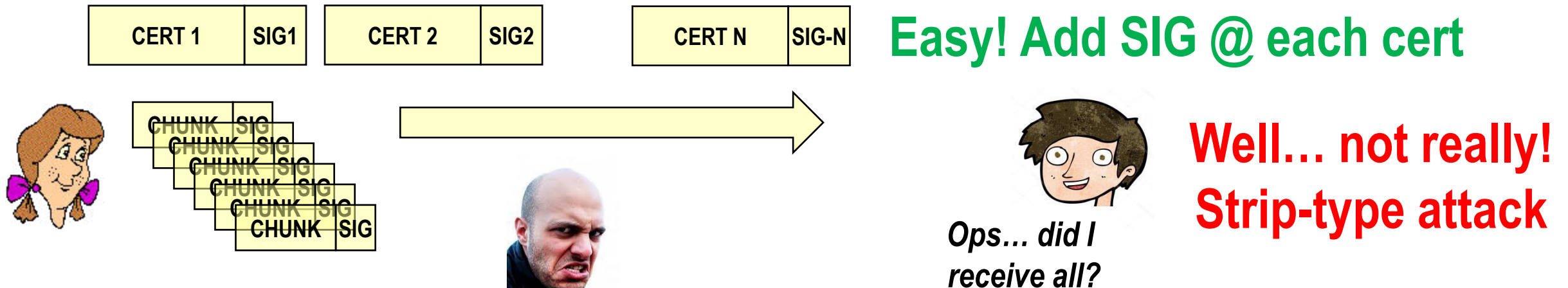
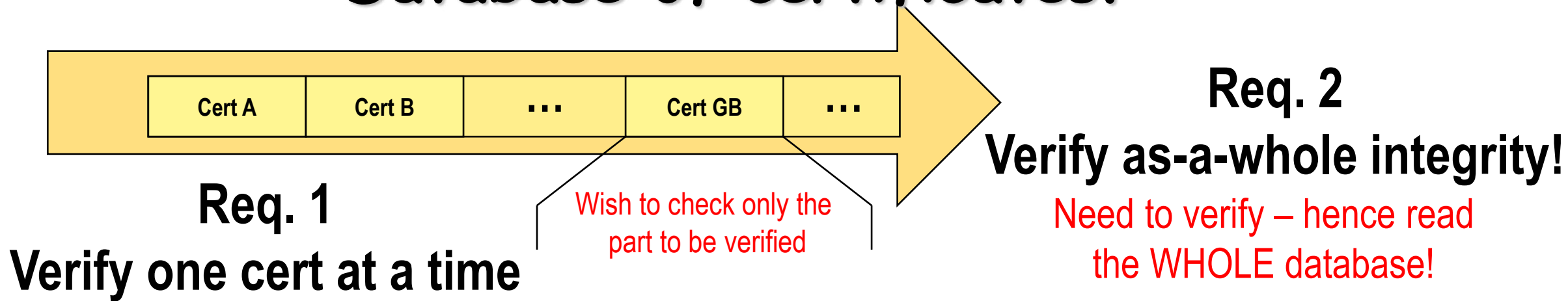
Wish to check only the  
part to be verified



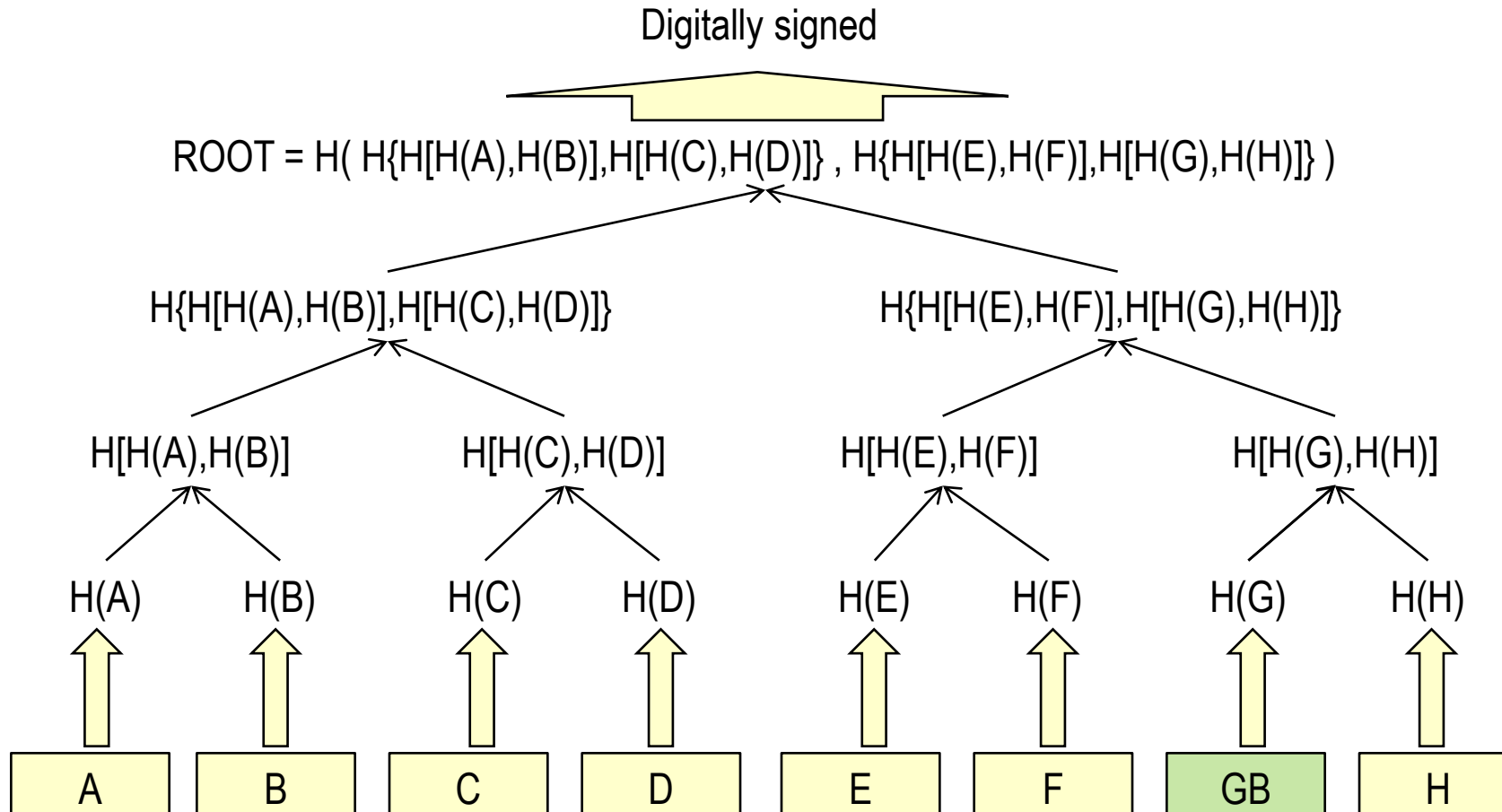
**Easy! Add SIG @ each cert**

**Well... not really!**  
**Strip-type attack**

# How to implement such gigantic Database of certificates?



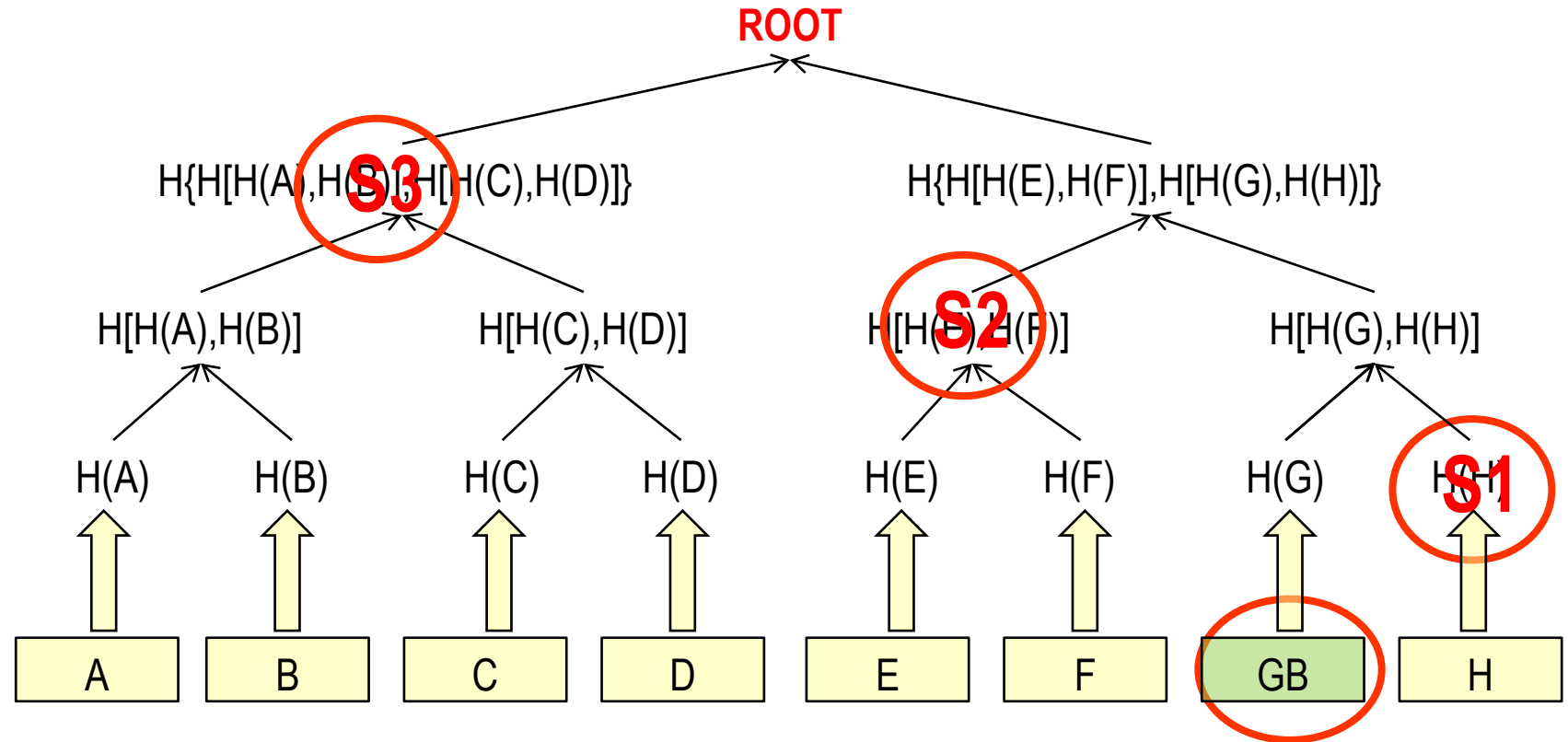
# You can have them both! Merkle's trees (1979)



# Single CERT verification: fast with “siblings”!

Give me:

- Cert GB
- Sibling S1
- Sibling S2
- Sibling S3

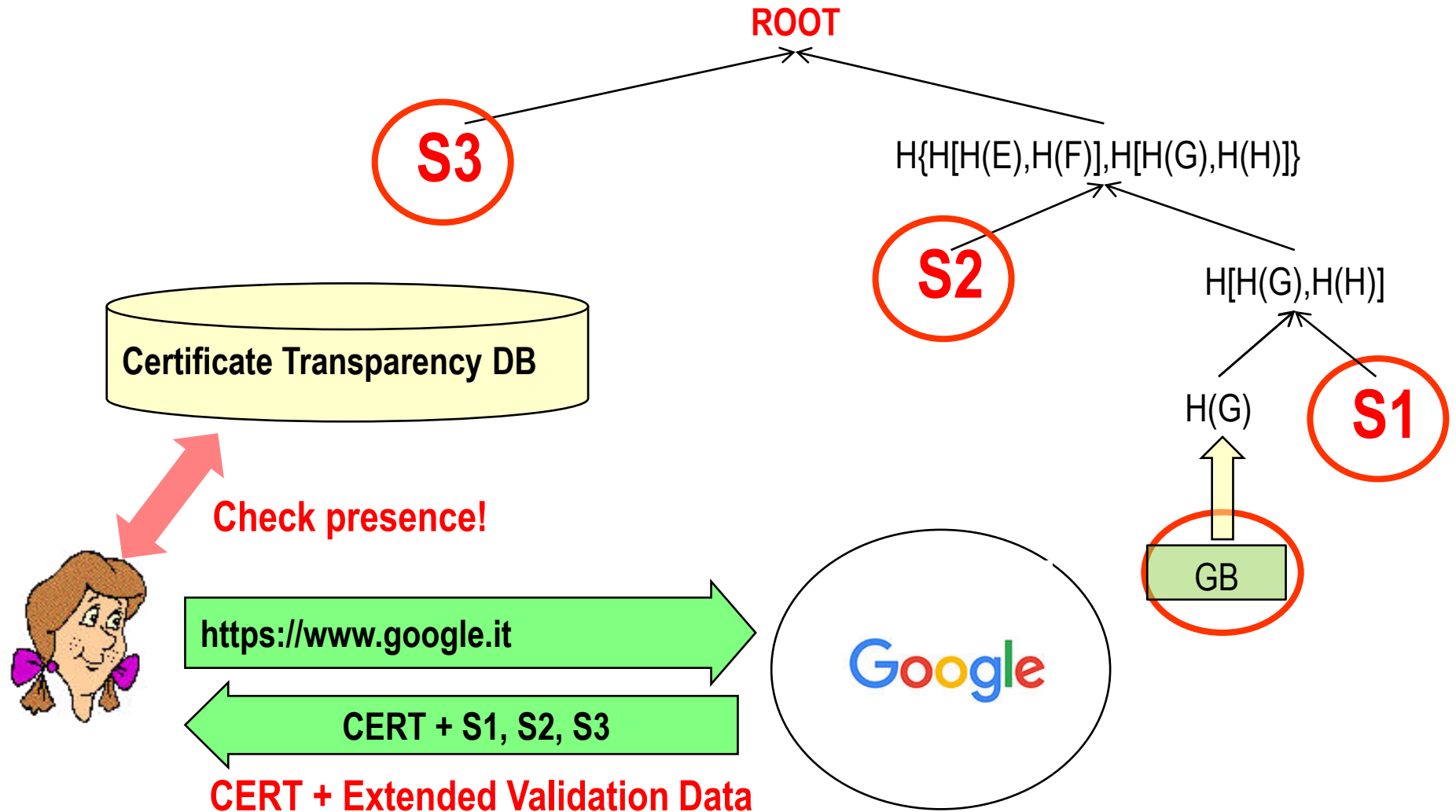




# Single CERT verification: fast with “siblings”!

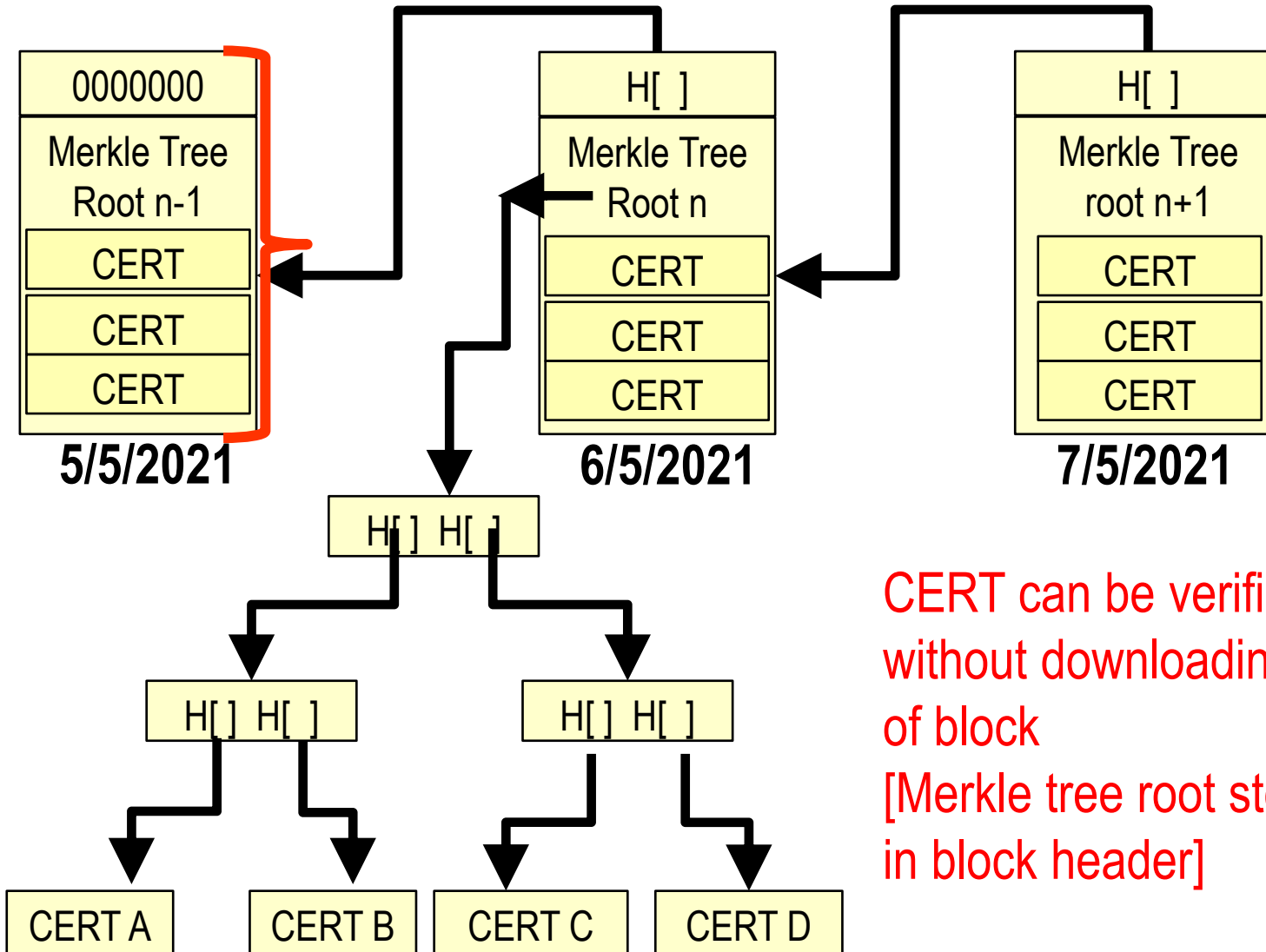
Give me:

- Cert GB
- Sibling S1
- Sibling S2
- Sibling S3



# Merkle trees vs time? Blockchain-type DB!

Hash pointers:  
Integrity of the  
Whole history  
From block 0!



Does this  
look familiar?



CERT can be verified  
without downloading content  
of block  
[Merkle tree root stored  
in block header]

# Done for real: Certificate Transparency

→ Launched in july 2013 by Google

→ experimental IETF RFC 6962

→ IETF WG «trans»

→ Specified processes and protocols

→ Integrated in all major browsers

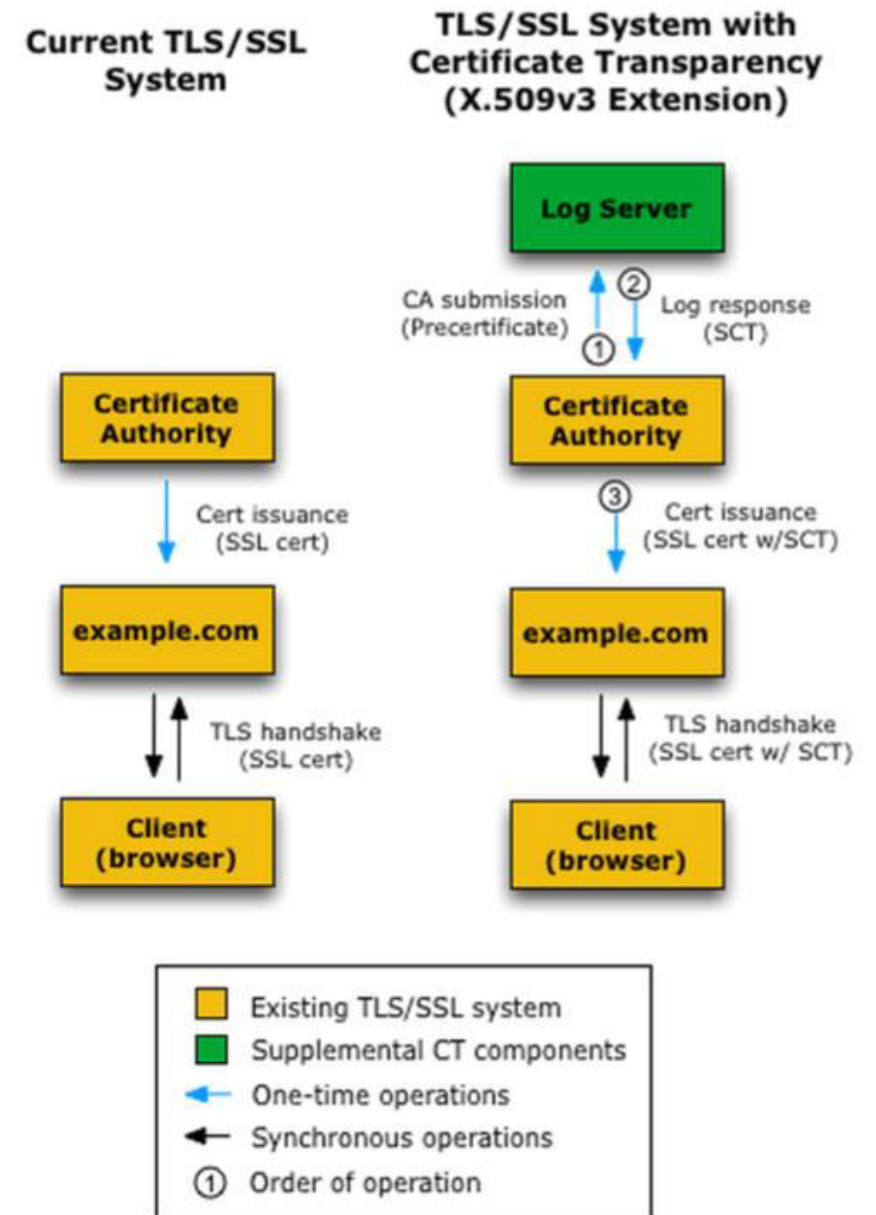
→ Supported by major sites

→ Paypal, CertSign, etc

→ Multiple pilot logs

→ Google, Cloudflare, DigiCert, etc

→ <https://certificate.transparency.dev/logs/>



# Done for real:

## Certif

→ Launched in ju

→ experimental

→ IETF WG «trans

→ Specified proce

→ Integrated in

→ Supported by

→ Paypal, CertSig

→ Multiple pilot

→ Google, Cloudfl

→ <https://certificate>

Current TLS/SSL  
System

TLS/SSL System with  
Certificate Transparency  
(X.509v3 Extension)

PayPal, Inc. [US] <https://www.paypal.com/it/webapps/mpp/home>

PayPal, Inc.

La tua connessione a questo sito è privata.

Autorizzazioni Connessione

L'identità di PayPal, Inc. a San Jose, California US è stata verificata da Symantec Class 3 EV SSL CA - G2 e può essere controllata pubblicamente.

[Informazioni sulla trasparenza](#)

La connessione a [www.paypal.com](https://www.paypal.com) è crittografata tramite crittografia obsoleta.

La connessione utilizza TLS 1.2.

La connessione è stata crittografata utilizzando AES\_256\_CBC, con SHA1 per l'autenticazione dei messaggi e RSA come meccanismo principale di scambio delle chiavi.

Informazioni sito

Non hai mai visitato questo sito prima di oggi.

[Che cosa significano?](#)

Visualizzatore timestamp certificato firmato

1: Integrato, Verificato

Stato di convalida	Verificato
Origine	Integrato
Versione	V1
Nome log	Google 'Pilot' log
ID log	A4 B9 09 90 B4 18 58 14 87 BB 13 A2 CC 67 70 0A 3C 35 98 04 F9 1B DF B8 E3 77 CD 0E C8 0D DC 10
Emesso alle ore	giovedì 23 aprile 2015 00:28:58
Algoritmo di hash	SHA-256
Algoritmo di firma	ECDSA
Dati della firma	30 45 02 20 5B E3 52 37 1B 84 B4 48 D1 CD 8F 53 34 D5 31 22 2D 46 C1 91 B2 86 6A 77 3E 37 DF FD CC 9D 78 A5 02 21 00 DE 96 80 20 B6 82 09 1E 8E 4A 9F C7 EE 3B 35 47 82 31 B1 D0 B1 63 F7 7D 52 1C C5 C5 41 5E BF 1A

Log Server

Log response (SCT)

Certificate Authority

Cert issuance (SSL cert w/SCT)

le.com

TLS handshake (SSL cert w/ SCT)

ent server)

Chiudi



# Cert Trans → is a Blockchain?

## → It definitely looks like

⇒ Identical (!) architecture as Bitcoin's ledger

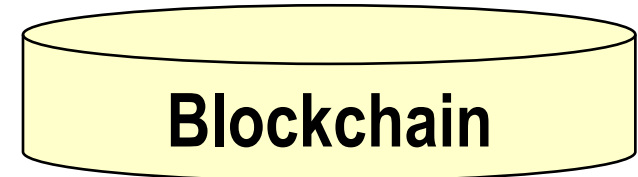
## → It could be distributed as well

⇒ Instead of different logs, make it a same «consensus» log

## → But it is NOT a Blockchain

⇒ It does NOT necessarily contain only VALID certificates!

→ As a Blockchain mandates; also Google being crystal clear on this!



If stored,  
NOT fake!



# Cert Trans → is a Blockchain?

## → It definitely looks like

⇒ Identical (!) architecture as Bitcoin's ledger

## → It could be distributed as well

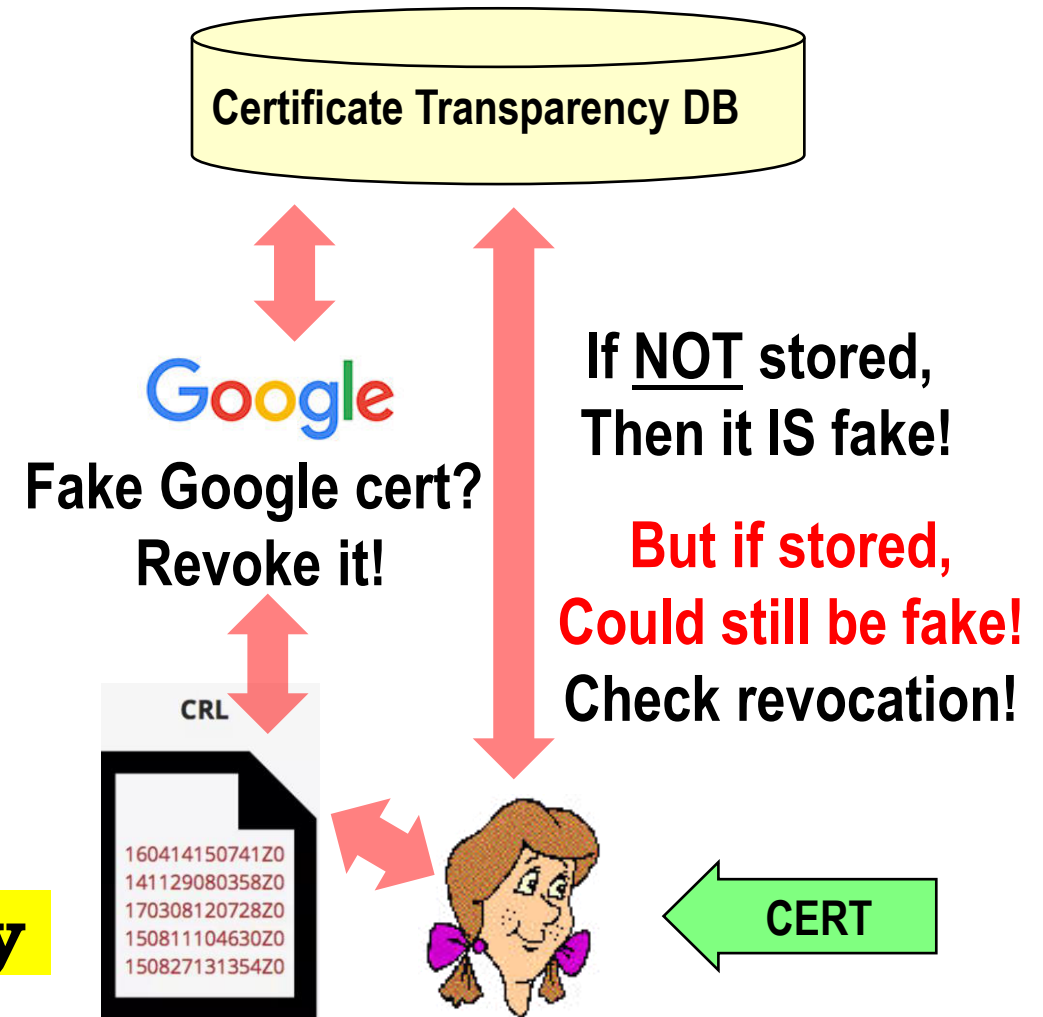
⇒ Instead of different logs, make it a same «consensus» log

## → But it is NOT a Blockchain

⇒ It does NOT necessarily contain only VALID certificates!

→ As a Blockchain mandates; also Google being crystal clear on this!

## → Security comes from transparency



# And what about cloud privacy? We must get rid of it?

a.k.a.: how to compute on encrypted data - ultra-brief intro to  
SECURE MULTIPARTY COMPUTATION  
(next slides in Italian)

# Cominciamo dalle conclusioni!

## Elaborazione di dati cifrati:



**ovvero: elaborare dati condivisi da più persone  
senza che nessuno possa «vedere» i dati di origine**

*Risultati scientifici disponibili da quasi 40 anni!*

*Falsità della dicotomia*

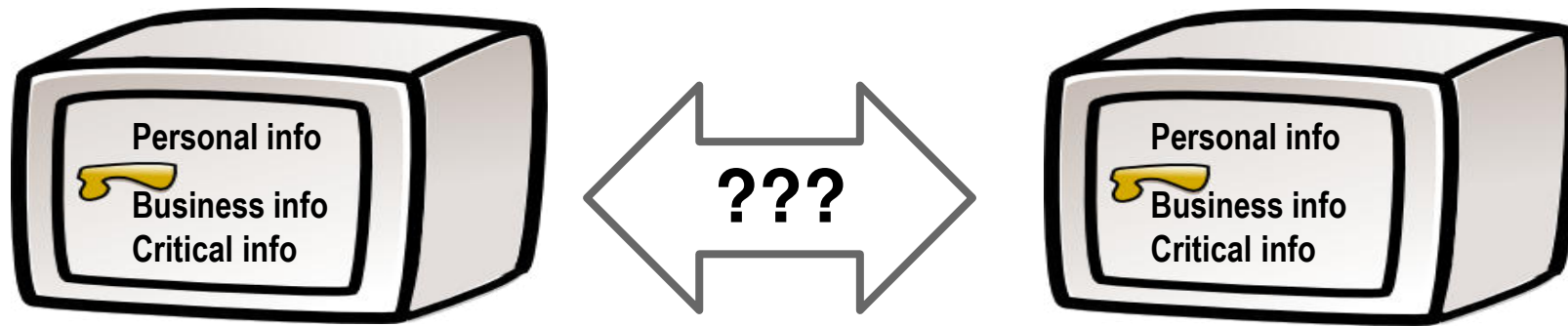
***confidenzialità ↔ utilità dei dati***

Ma perché pochi sono informati? E perché le applicazioni sono praticamente inesistenti? potremmo fare molto di più...



# «The sharing dilemma»

## Condividere o non condividere?



**Caso critico:**  
**NO autorità o**  
**intermediario fidato**

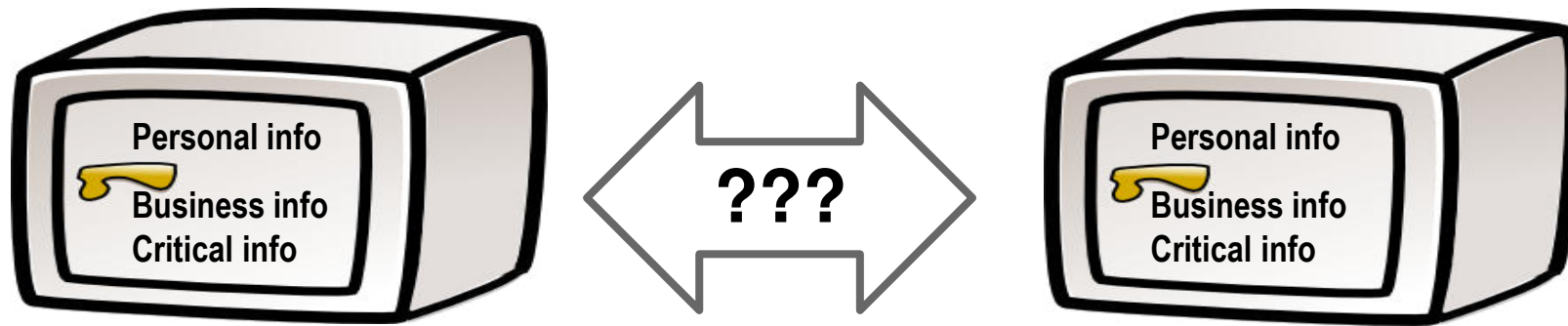
**Internet AS, Stati,**  
**Aziende**

...



# «The sharing dilemma»

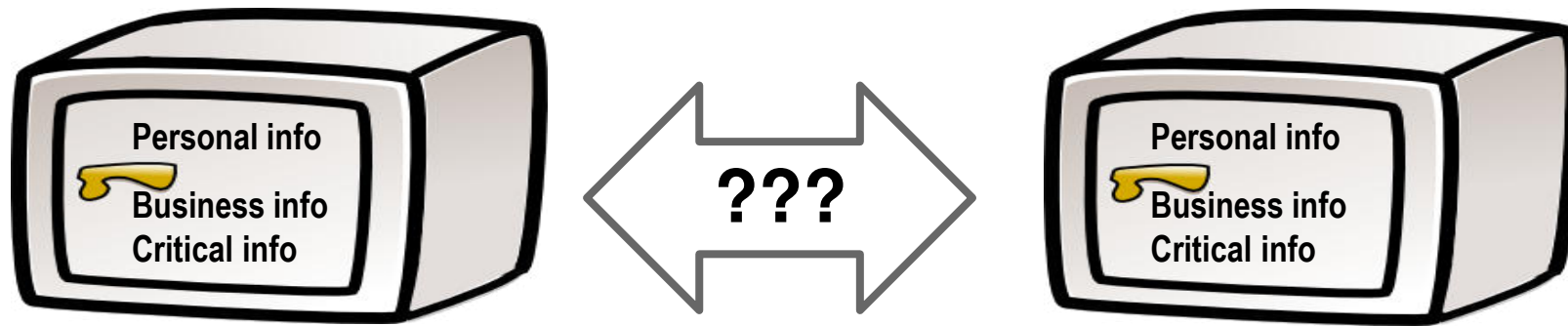
## Condividere o non condividere?



Condividere (minacce, attacchi, dati):  
collaborazione → più sicurezza,  
più efficienza, servizi migliori

# «The sharing dilemma»

## Condividere o non condividere?

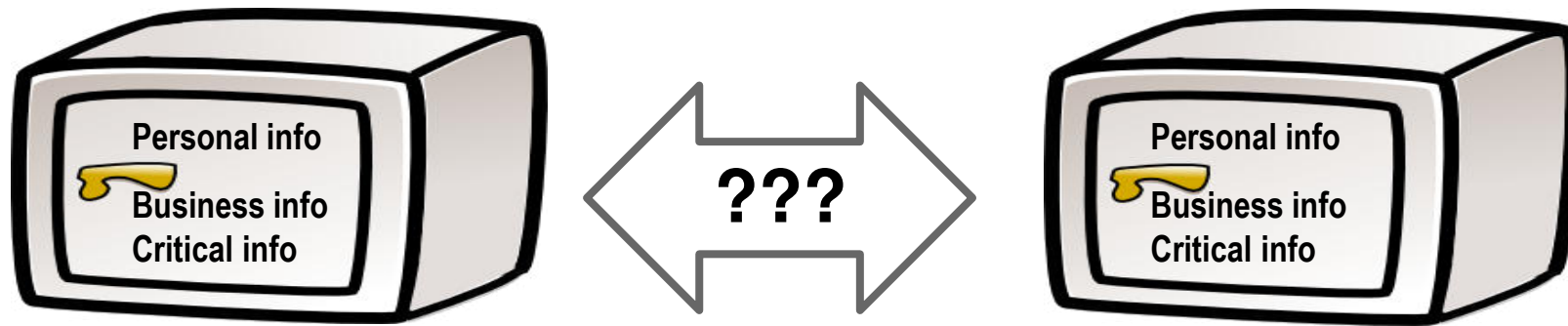


Condividere (minacce, attacchi, dati):  
**Meno privacy, meno confidenzialità  
del business, maggior esposizione**



# «The sharing dilemma»

## Condividere o non condividere?



*Percezione da parte del «non tecnico»:  
**DEVE** essere un gioco a somma zero  
Dobbiamo **per forza** cercare un trade-off*

# «The sharing dilemma»

## Una terza via: Win-Win!

Homeland Security Department, stato 1
<b>Lista Sospetti</b> -BNCGPP75T10H5091 -RSSFRC82S21X5091 -...

Airline, stato 2
<b>Lista Passeggeri</b> -VRDRBT65T10B157X -BNCGPP75T10H5091 -...

- ➔ **C'è qualche sospetto su questo volo?**
- ➔ **Soluzione 1: fornire lista sospetti a compagnia aerea**
  - ⇒ No way!!
- ➔ **Soluzione 2: obbligare airline a fornire lista passeggeri**
  - ⇒ In mancanza di meglio... ma.... (passeggeri in transito? privacy?)



# «The sharing dilemma»

## Una terza via: Win-Win!

Homeland Security Department, stato 1
<b>Lista Sospetti</b> -BNCGPP75T10H5091 -RSSFRC82S21X5091 -...

Airline, stato 2
<b>Lista Passeggeri</b> -VRDRBT65T10B157X -BNCGPP75T10H5091 -...

→ **C'è qualche sospetto su questo volo?**

→ **Soluzione Win-Win: Private Set Intersection!**

⇒ Freedman et. Al. 2004, Ateniese et al. 2011, GB 2016, etc

# Nulla di nuovo! (per i crittografi)

## → **Secure Multi Party Computation (e variazioni sul tema)**

- ⇒ *private information retrieval*,
- ⇒ *Homomorphic encryption*
- ⇒ *Conditional encryption*
- ⇒ *etc*

## → **SOLO interessato al risultato, NON ai dati di input?**

- ⇒ **MPC is for you!** (dati input rimangono confidenziali)

## → **Ricerca estremamente consolidata, da quasi 40 anni!**

- ⇒ Andrew Yao, 1982, problema del Milionario
- ⇒ Migliaia (!) di lavori scientifici e di applicazioni, da allora

# Si, ma...

## → **Troppo difficile, per nulla scalabile**

⇒ Inizialmente vero

⇒ *garbled circuits, oblivious transfer, Pailler Encryption, ...*

## → **Ma ora è BEN diverso! Tecniche moderne ESTREMAMENTE efficienti e pratiche!**

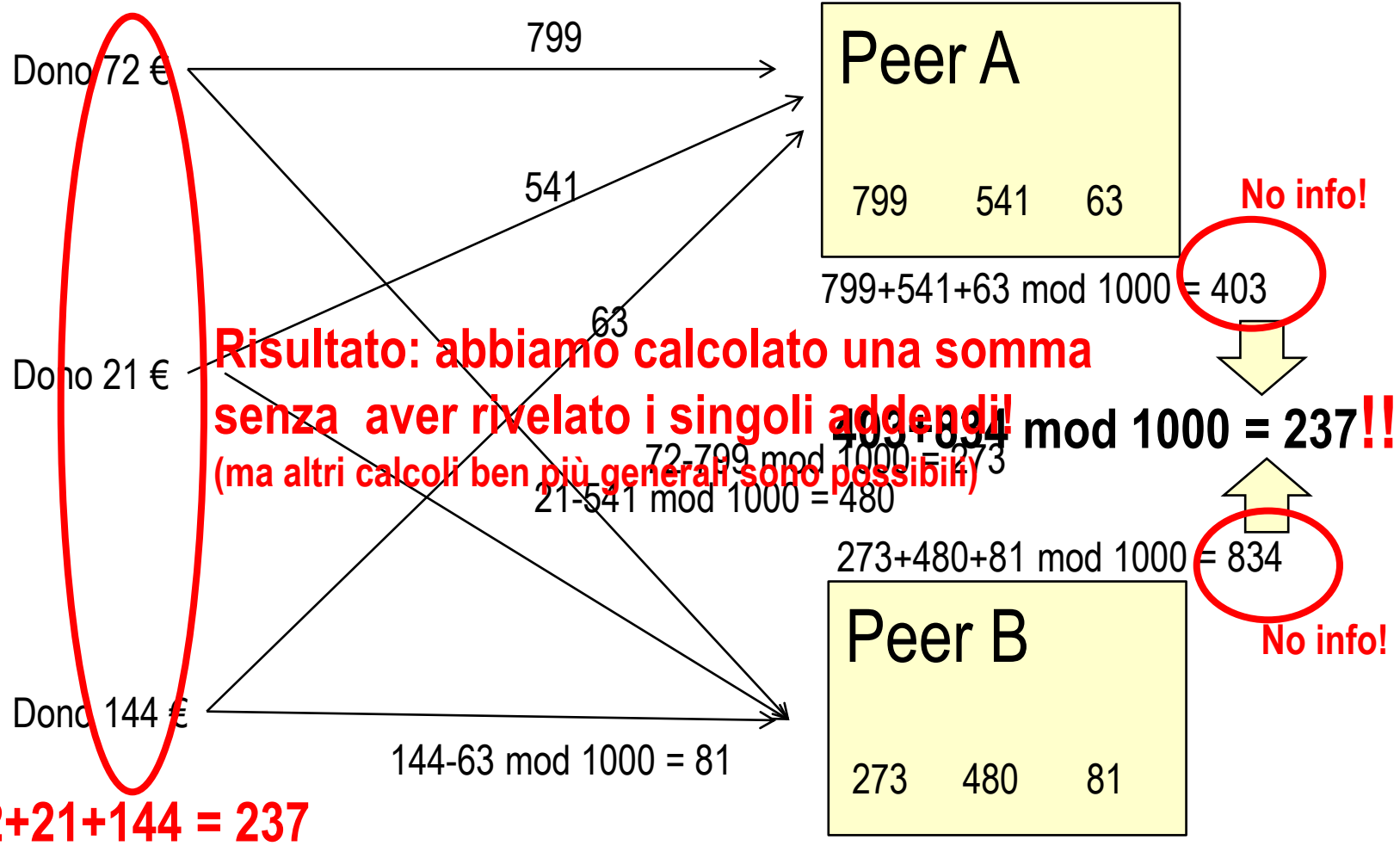
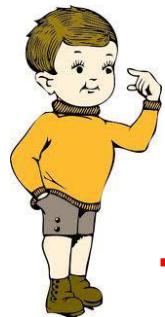
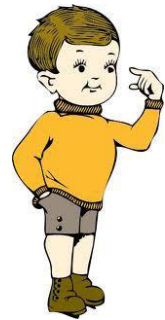
⇒ Post-2010, basate su secret sharing

⇒ Nigel Smart: ERC → Dyadic → Unbound

## → **E molto flessibili**

⇒ Gentry's doubly-homomorphic encryption

# Estremamente pratiche?! Un semplicissimo esempio!



# **Altri «layman examples» (casi realmente accaduti!!)**

- **Valutazione docenti: da cartacea a web**
  - Studenti: non ci fidiamo!
  - Centro di calcolo: garantisco io!
    - (ma se qualcuno poi attacca il server?)
  - server docenti + server studenti + MPC:
    - Fiducia non più necessaria!
- **Commissione valutazione best PhD award**
  - 5 commissari, 1 aggregatore sapeva voti di tutti
  - MPC distribuito!
    - Nessuno saprà nulla
    - Ma tutti conosceremo media voti.



# Applicazioni: tante! Esempi:

- **Key segregation/isolation, signature-splitting, ...**
  - Segreti MAI usati in chiaro → più sicurezza, anti-tampering, ...
  - **Modello di business principale di Unbound Security – Israele!**
- **Inter-domain data sharing**
  - Scambio dati tra unità operative in domini differenti
  - monitoring & security → più privacy, business confidentiality
- **Cloud Systems, auction bid systems**
  - Permettere al cloud di operare sui miei dati → senza rivelarli
- **Bio-informatica, genetica, e-health, ...**
  - Elaborazione su dati sensibili cifrati, minima disclosure → privacy
- ...

# Ma perché MPC è ancora una nicchia?

A maggior ragione visto che è in giro da quasi 40 anni...

- **Non ne sapevo nulla!!**
  - MPC non nei corsi base; crittografi poco divulgatori
- **Ma è «solo» privacy... e privacy non ci interessa (ooops)**
  - **Falso!** E' anche business confidentiality, data protection, system security hardening, key protection in BYOD, etc!
- **Scarsa interdisciplinarietà, gap tra problemi e soluzioni**
  - “...*Most research papers give imaginary applications...*”
  - Ma qualcosa sta cambiando (bio-informatica, start-ups, ...)
- **MPC non scala, costa, richiede riprogrammazione**
  - Non più (dal 2010 in poi): prestazioni + buona flessibilità
    - SS-MPC per algo non banali quali PCA, SVD, vari ML, K-means, etc

# Commercial MPC in 2018...

The screenshot shows a web browser window displaying the Unbound Tech website. The browser's address bar shows the URL <https://www.unboundtech.com/company/about/>. The website's header includes the Unbound logo with the tagline "(MATH OVER MATTER)" and a navigation menu with links to PRODUCTS, USE CASES, SOLUTIONS, TECHNOLOGY, RESOURCES, COMPANY, and BLOG. A "LET'S TALK" button and a search icon are also present. The main content area features a section titled "Developing Novel MPC Applications, Privacy and Beyond" with a paragraph about innovation and data privacy. A dark blue overlay box lists various MPC applications: Database Encryption, App-Level Encryption, Secure Manufacturing, Code Signing, Blockchain Key Management, Secure Authentication on BYOD, Replace Hardware Tokens with BYOD, Secure Mobile PKI, PCI-DSS Compliance, and DFS Compliance. To the right, a graphic titled "The Unbound Horizon" depicts a globe with a purple dot and a trail of orange particles. The Windows taskbar at the bottom shows the search bar, task view, and several application icons, with the system clock indicating 23:55 on 17/04/2018.

Leading the revolution in

giuseppe

Unbound Tech LTD [IL] | <https://www.unboundtech.com/company/about/>

App The Future of Networ Governor of Poker 3 BTC-Tech | Class Profil HPSR2018 - Google Windsurf. Mercatino Stazione meteo Mari Altri Preferiti

UNBOUND  
(MATH OVER MATTER)

PRODUCTS USE CASES SOLUTIONS TECHNOLOGY RESOURCES COMPANY BLOG

LET'S TALK

Developing Novel MPC Applications, Privacy and Beyond

Innovation is increasingly dependent on analyzing masses of data. This often comes at the expense of privacy. Unbound is developing practical applications of MPC to safeguard privacy, opening the doors for organizations to perform analytics on shared data sources without jeopardizing the privacy of each contributor.

- Database Encryption
- App-Level Encryption
- Secure Manufacturing
- Code Signing
- Blockchain Key Management
- Secure Authentication on BYOD
- Replace Hardware Tokens with BYOD
- Secure Mobile PKI
- PCI-DSS Compliance
- DFS Compliance

The Unbound Horizon

23:55  
17/04/2018

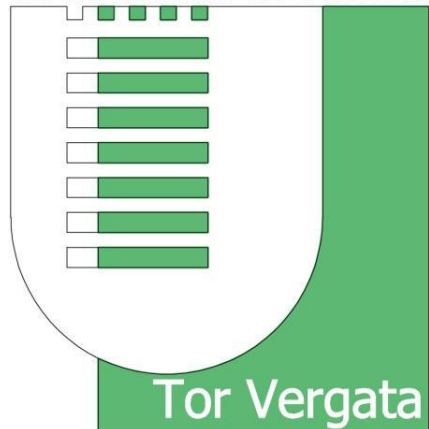
# Commercial MPC in 2021... security!

The screenshot displays the homepage of unbound security. The navigation bar includes links for Solutions, Partners, Resources, Blog, and Company, along with a 'BOOK A DEMO' button and a search icon. The main content area is divided into four sections, each with an icon and a description:

- Crypto Agility**: Achieve agility, scalability, and automation using a pure-software platform designed for modern IT. (Icon: A padlock inside a circle with circuit lines radiating outwards.)
- No Hardware Dependency**: Eliminate the single cryptographic key and with it the complex and cumbersome security measures used to protect it. (Icon: A cloud with a folder icon inside.)
- Key Misuse Prevention**: Gain complete visibility and control by unifying protection and management of all keys, on any infrastructure, across the organization. (Icon: A globe with location pins.)
- Seamless Usability**: Take usability to a whole new level, with applications that streamline workflows, support automation and enhance simplicity and efficiency. (Icon: Two interlocking gears.)

A chat bubble icon is visible in the bottom right corner of the website. The Windows taskbar at the bottom shows the search bar with the text 'Scrivi qui per eseguire la ricerca', several application icons, and the system clock displaying 19:47 on 04/05/2021.

Università di Roma



consorzio nazionale  
interuniversitario  
per le telecomunicazioni

# ***Thank you***

**Giuseppe Bianchi**

Professor of networking and network security  
University of Roma «Tor Vergata»

*giuseppe.bianchi@uniroma2.it*

