

Processing Biometric Data under Encryption

Challenges and Opportunities for Cryptographers

Dr. Zeki Erkin

z.erkin@tudelft.nl

Cybersecurity Section
Department of Intelligent Systems
Delft University of Technology

About me...

Assist. Prof. @ TU Delft, Cyber Security Group

PostDoc @ TU Delft, 2010-2014

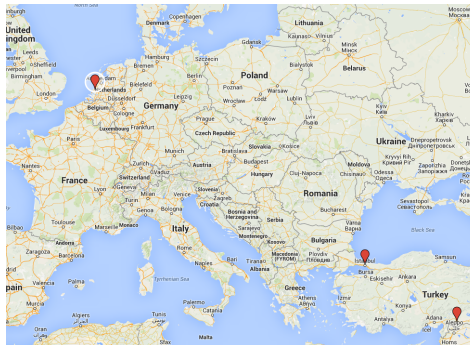
PhD @TU Delft, 2010

BSc and MSc @ITU, Istanbul, 2002, 2005

Secure Signal Processing, Privacy Enhancing Technologies
MPC, Applied Cryptography

CSng and ICTng core member
Blockchain Lab

- Blockchain and Logistics
- 3TU Big Software on the Run
- FET Signal Processing in the Encrypted Domain
- STW Kindred Spirits
- Dutch/COMMIT Trusted Healthcare and Extreme Wireless Sensor Networks



Outline

Biometric Data and Privacy

Case Study: Secure Face Recognition

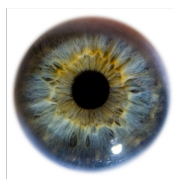
Homomorphic Encryption

Secure Comparison Protocol

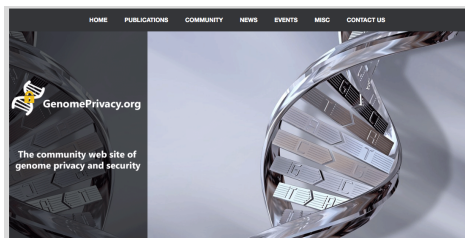
Cryptographic Challenges

Opportunities

Biometric Data?



- Surveillance for security
- Automated healthcare monitoring
- Identification/Detection
- DNA sequencing



Privacy Problems

Is Samsung's Galaxy S5 'leaking' YOUR fingerprints? Flaw means hackers can intercept and steal biometric data

- Experts have discovered a flaw in older versions of the Android system
- Once a hacker has access to a phone they can monitor data from sensors
- From this, they can potentially intercept a fingerprint from the scanner
- Vulnerability has been tested and confirmed on the Samsung Galaxy S5

Selfie as Source of Biometric Data Leakage

18.01.2017

[BACK TO NEWS](#)

Via cameras in today's smartphones, it is possible to leak papillary pictures of fingers with accuracy great enough for frauds to use other person's fingerprints for their own benefit.

Biometric authentication is a common way to protect applications and devices. Having obtained fingerprints, strangers can unlock a notebook or smartphone and trick biometric systems of access into any building.

Is Nadra keeping your biometric data safe?

The simple fact is that biometric data management is yet to mature.

SHABEERA JALIL ALBAHAT — UPDATED Oct 17, 2016 02:24pm

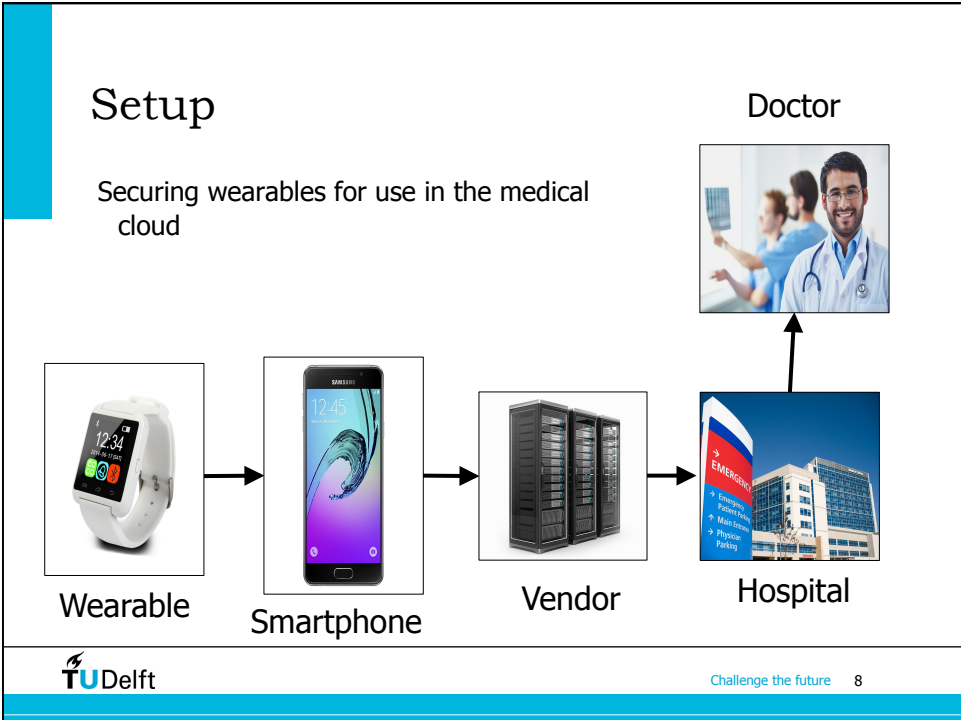
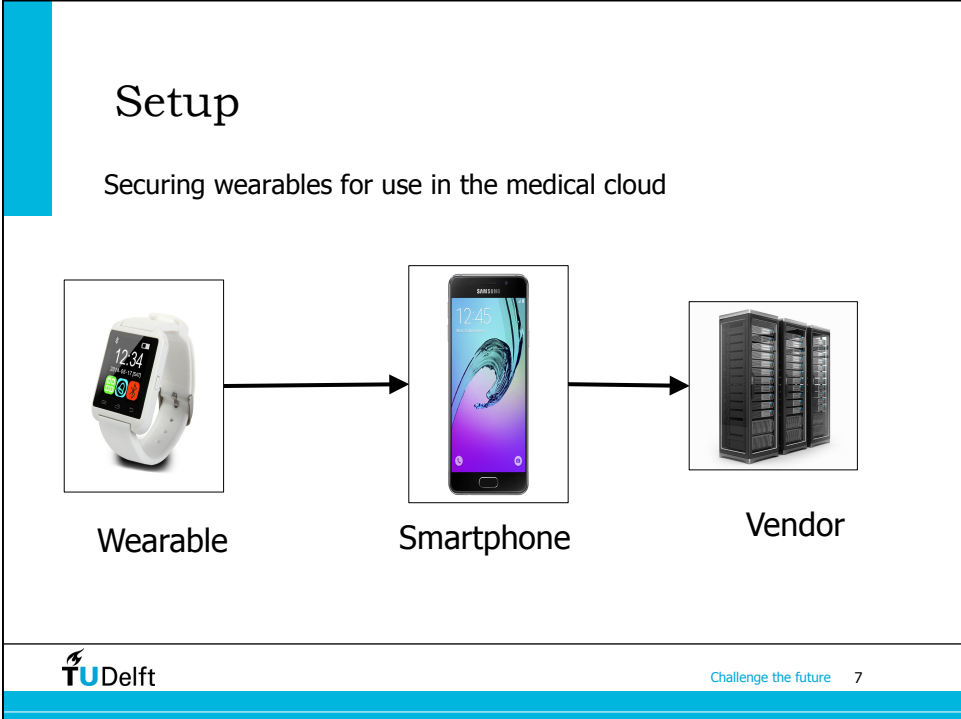
Pakistan maintains one of the world's largest centralised citizen databases, which continues to expand at an unprecedented rate. This mammoth task sounds impressive, but it also raises concerns about the vulnerability of our data.

The Philippines election hack is 'freaking huge'



Wearable Devices





Privacy Recipe!

- Awareness
- Education
- Laws and Regulations
- Scientific Solutions
 - Anonymization
 - Physical security
 - Access control
 - Cryptography



Privacy: New problem?

- Different applications with a different security risk
 - **Past:**
 - (Confidentiality-Integrity-Authenticity)
 - Alice and Bob want to communicate securely
 - **Present:**
 - Alice and Bob want to work together but do not **trust** each other
- Alice has private data, Bob has an (private) algorithm

Secure Face Recognition

©CBS NEWS CORRESPONDENT
SUSAN KOEPPEN

NEW YORK, June 30, 2010
Surveillance Camera Privacy Debate Widens

The New York Times

Europe

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH
AFRICA AMERICAS ASIA PACIFIC EUROPE MIDDLE EAST

Warning over 'surveillance state'

Electronic surveillance and collection of personal data are "pervasive" in British society and threaten to undermine democracy, peers have warned.



British Police Offer Apology to Muslim Spy Cameras

By THE ASSOCIATED PRESS
Published: October 1, 2010

LONDON (AP) — The British police on Thursday apologized for a counterterrorism program that featured surveillance cameras that were installed

OPINION Surveillance Cameras: Crime Prevention Or Violation Of Privacy?

by Yuliya Talmazan | August 25, 2009 at 09:45 am

Share:



CHICAGO, Aug. 13, 2010

Surveillance Cameras and the Right to Privacy

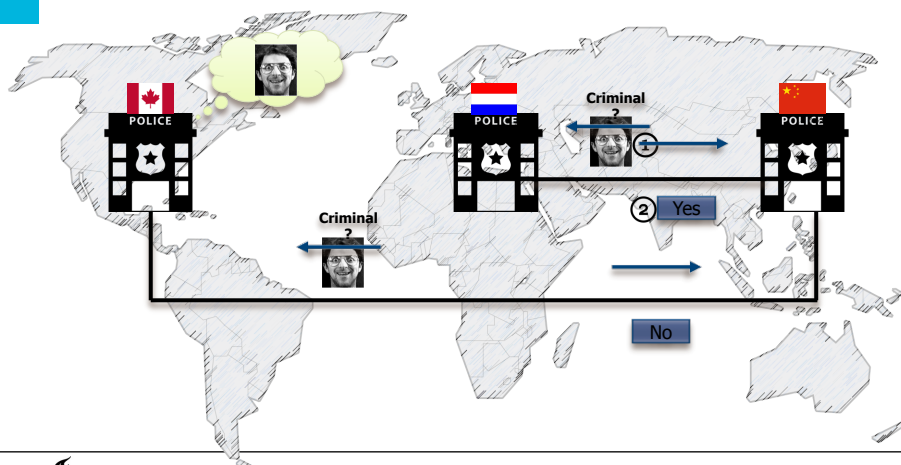
CBS Reports: Where America Stands on Fighting Crime in the High-Tech Era
By Erin Moriarty

Font size Print E-mail Share

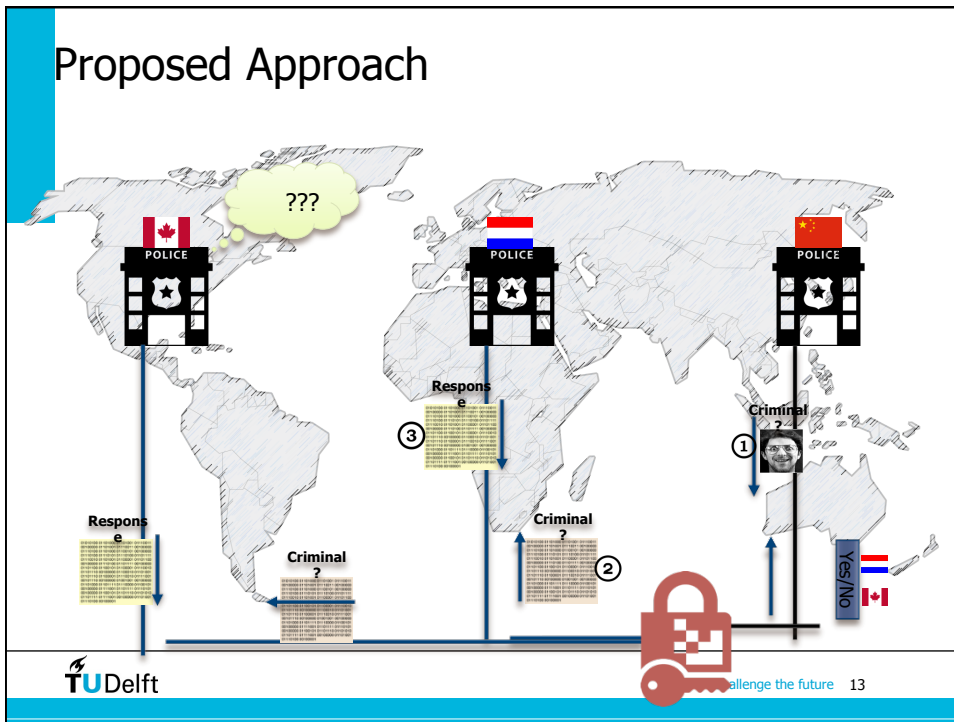


Challenge the future 11

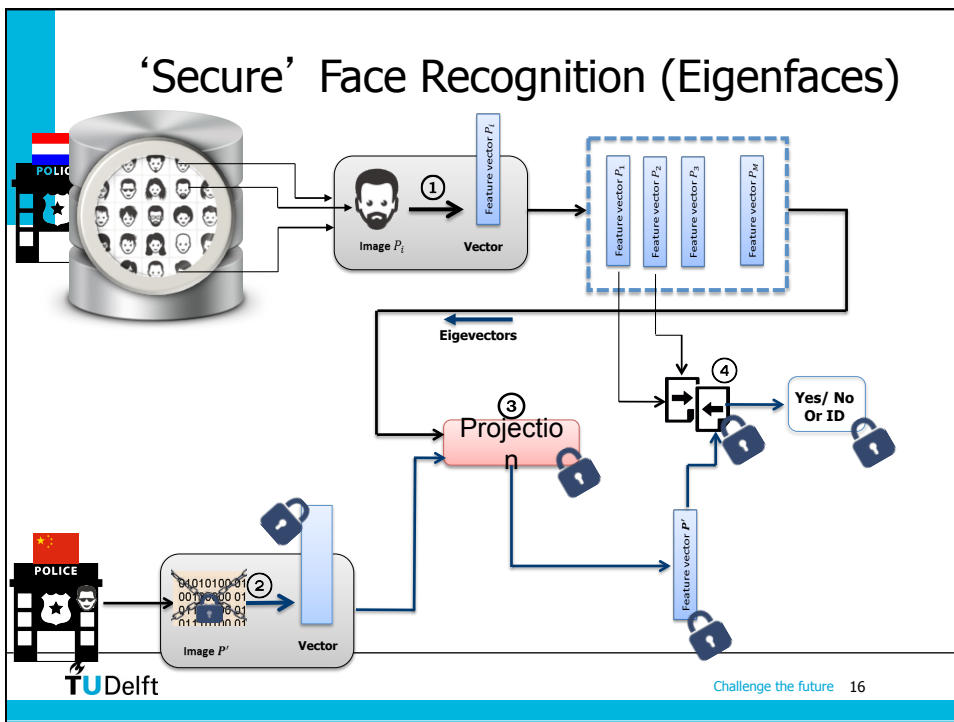
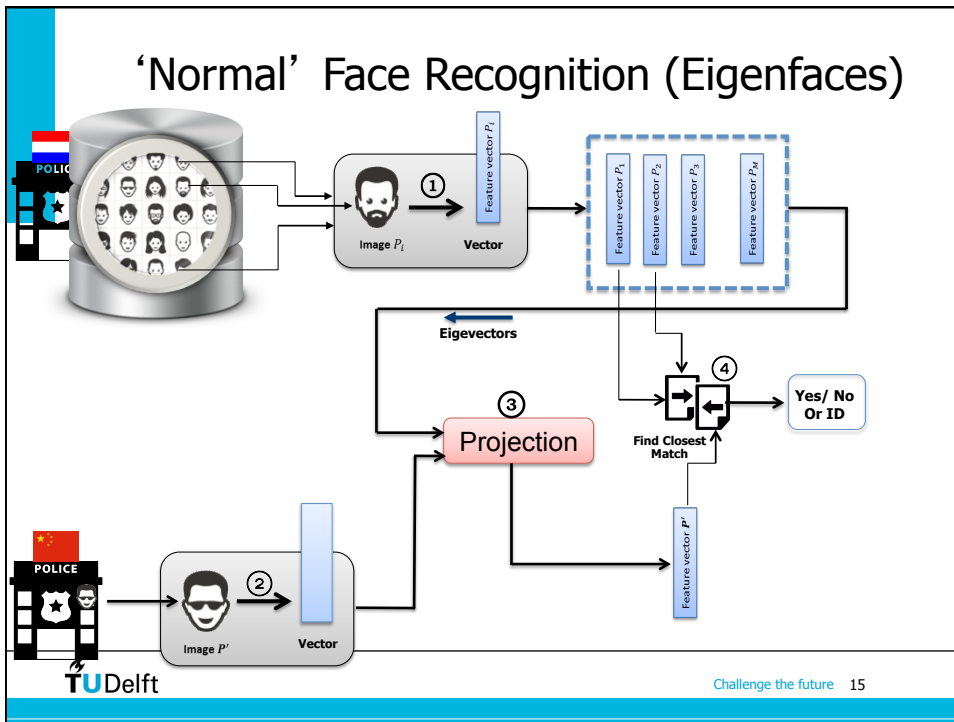
Face Recognition



Challenge the future 12



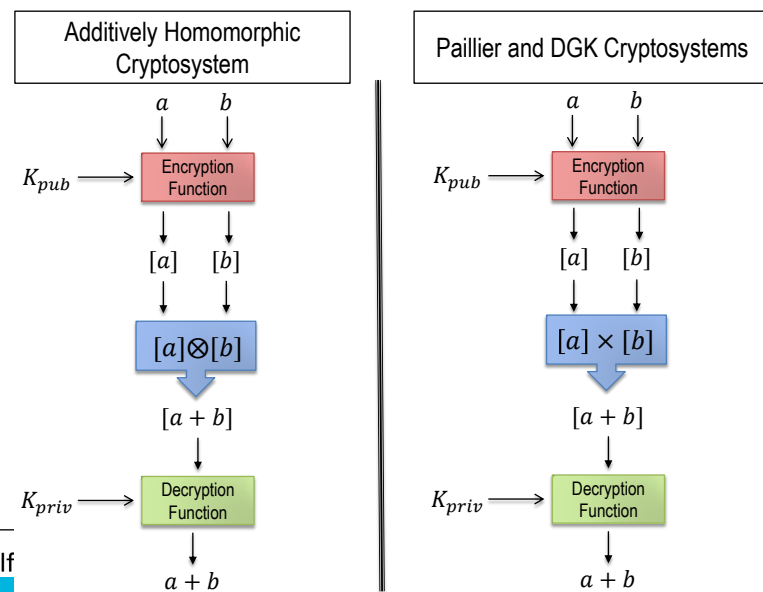
- ## How?
- Trusted third party
 - Cryptography
 - Cryptography 2.0
- TU Delft challenge the future 14



Encryption

- Destroys structure
- Random looking data
- Decryption key is required
- Homomorphic Encryption
 - Public key cryptosystems do reserve some structure

Homomorphic Encryption



Paillier And DGK Cryptosystems

$$[a] \times [b] = [a + b]$$

$$D_{K_{Priv}}([a] \times [b]) = a + b$$

$$[a]^c = [a] \times \dots \times [a] =$$

$$[a + \dots + a] = [a \cdot c]$$

$$[a]^c = [a \cdot c]$$

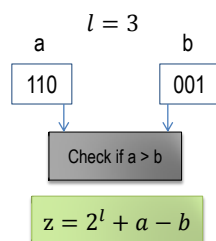
Example:

$$10 + (3 \times a) - b + a$$

Decryption

$$[10] \times [a]^3 \times [b]^{-1} \times [a]$$

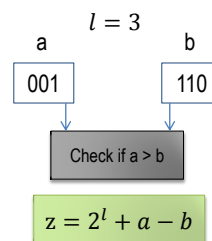
Secure Comparison Protocol



$$(1) z = 1000 + 110 - 001 = 1101$$

$$(2) t = 1101 - (1101 \bmod 1000) \\ = 1101 - 0101 \\ = 1000$$

$$\text{Answer} = 2^{-l} * 1000 = 1$$



$$z = 1000 + 001 - 110 \\ = 0100$$

$$t = 0100 - (0100 \bmod 1000) \\ = 0100 - 0100 \\ = 0000$$

$$\text{Answer} = 2^{-l} * 0000 = 0$$

Secure Comparison Protocol (Cont.)

a: 110, b: 001

Check if a > b

$z = 2^l + a - b$

(1) $z = 1000 + 110 - 001 = 1101$

(2) $t = 1101 - (1101 \bmod 1000)$

Answer = $2^{-l} * 1000 = 1$

a: [110], b: [001]


Check if a > b

$[z] = [2^l] * [a] * [b]^{-1}$

$z = [1000] * [110] * [001]^{-1} = [1101]$

$t = [1101] * [1101 \bmod 1000]^{-1}$

Needs private key -> MPC



Challenge the future 21

Secure Comparison Protocol (Cont.)

Alice

$k_{pub}, [z] = [1101], [z \bmod 1000] = ?$

random number $r = 110$

(1) $[d] = [1101 + 110] = [10011]$

(2) $[z \bmod 1000] = [d - r] = [011] * [110]^{-1} = [-011]$

Need to check if $d < r$

If $d < r$ then $[z \bmod 1000] = [d - r + 1000] = [-011 + 1000] = [0101]$

Bob

k_{priv}, k_{pub}


Decrypt $_{k_{priv}} [d]$ to 10011

$10011 \bmod 1000 = 011$

Encrypt(011) = [011] = d


[10011] →

← d = [011]





Secure Multi-party Computation

Yao's Millionaires' problem
Which one has more money!



A = how much money user1 has






B = how much money user2 has

$f(A,B)=$

- User1 if $A > B$
- Equal if $A = B$
- User2 if $A < B$



Challenge the future 23


Improved DGK By T. Veugen^[*] (Cont.)

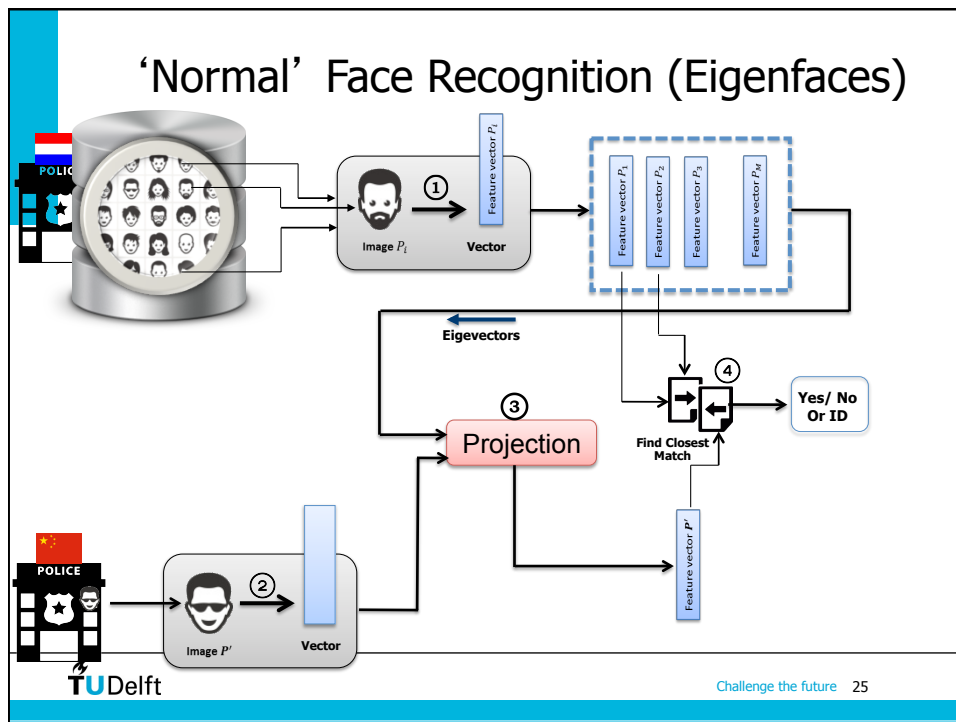
Improved DGK_[2]

Function	Time (second)	Percent (%)
Server		
Computing $[[c_i]]$	15	70
$[[e_i]] \leftarrow$ Masking $[[c_i]]$	3.15 → 2	15
Other	3.15	15
Client		
DGK zero-check	27.3	38
Paillier decryption	44.4	62
Total	93	

EPPCP

Function	Time (second)	Improvement
Server		
Computing $[[c_i]]$	1.40	91%
$[[e_i]] \leftarrow$ Masking $[[c_i]]$	3.15	0
Other	3.15	0
Client		
DGK zero-check	27.3	0
Paillier decryption	6.40	85%
Total	41.4	





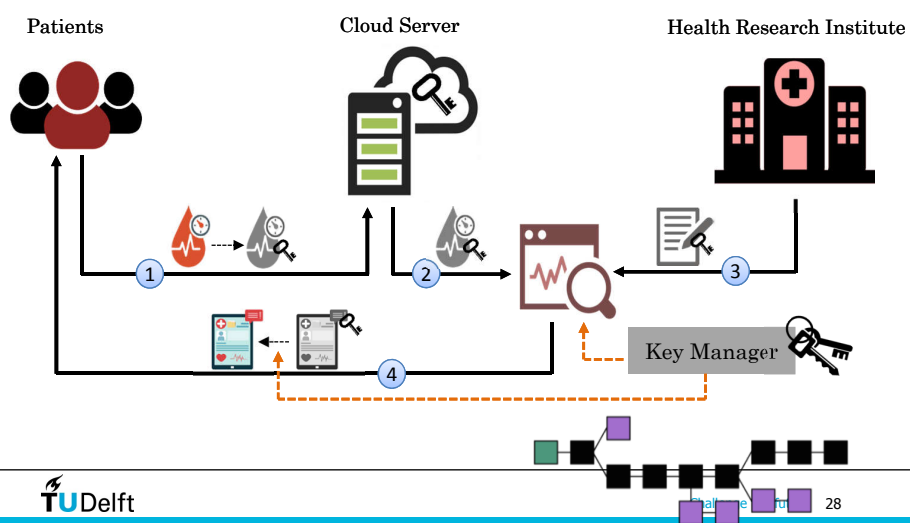
Challenges Privacy Engineering

- Application setting:
 - Server-client
 - Multiple servers-clients
 - Cloud
 - Different roles/parties
- Cryptographic challenge
 - Primitives: FHE, SHE, AHE, GC, SS
 - Key management
 - Dynamic environments
 - Semi-honest, covert, malicious

Privacy Engineering

- Integers vs real numbers
- Data expansion
- Communication
 - bandwidth
- Computation
 - expensive operations (thousand of bits)
- Business model
 - semi-trusted third party, auditing company...

Cloud Services



Thanks

Special Thanks to

Majid Nateghizad, Roderick Treskes, Thijs Veugen and Tomas Toft