



PI lab
Privacy & Identity Lab

Radboud University

TILBURG UNIVERSITY
Law School

university of groningen

Privacy Seminar

Basic Techniques

Jaap-Henk Hoepman

Privacy & Identity Lab
Radboud University
Tilburg University
University of Groningen

✉ jhh@cs.ru.nl // 🌐 www.cs.ru.nl/~jhh // 📝 blog.xot.nl // @xotoxot

1

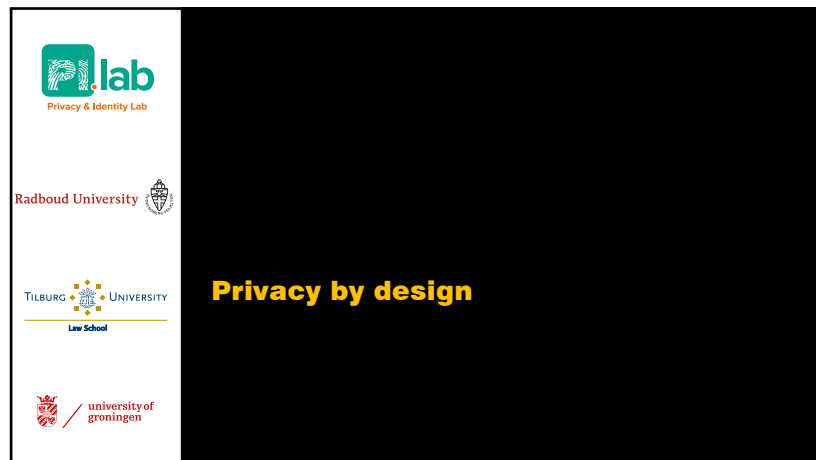


Agenda

- **Privacy by Design**
 - Principles
 - Privacy Design Strategies
- **Privacy Enhancing Technologies I**

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

2



PI lab
Privacy & Identity Lab

Radboud University

TILBURG UNIVERSITY
Law School

university of groningen

Privacy by design

3



Privacy by design

- **Protect privacy when developing new technology:**
 - From concept...
 - ... to realisation

Throughout the system development cycle

- **Privacy is a quality attribute (like security, performance,...)**
- **Privacy by design is a process!**


Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

4



5

Common engineering misconceptions #1


0/1 vs. 

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

6

6

Common engineering misconceptions #2

Data controller = 

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

7

7

Common engineering misconceptions #3

Privacy = Data minimisation

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

8

8

Personal data?

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **So...**
 - Name
 - Social security number
 - Email address
- **But also...**
 - License plate
 - IP Address
 - Likes
 - Tweets
 - Search terms

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 9


9

Aside: what is 'Data Processing'...

Action	Relevant GDPR Personal Data Processing Examples
Operate	Adaptation; Alteration; Retrieval; Consultation; Use; Alignment; Combination
Store	Organisation; Structuring; Storage
Retain	opposite to (Erasure; Destruction)
Collect	Collection; Recording
Share	Transmission; Dissemination; Making Available; opposite to (Restriction; Blocking)
Change	unauthorised third party (Adaptation; Alteration; Use; Alignment; Combination)
Breach	unauthorised third party (Retrieval; Consultation)

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 10

10



Radboud University

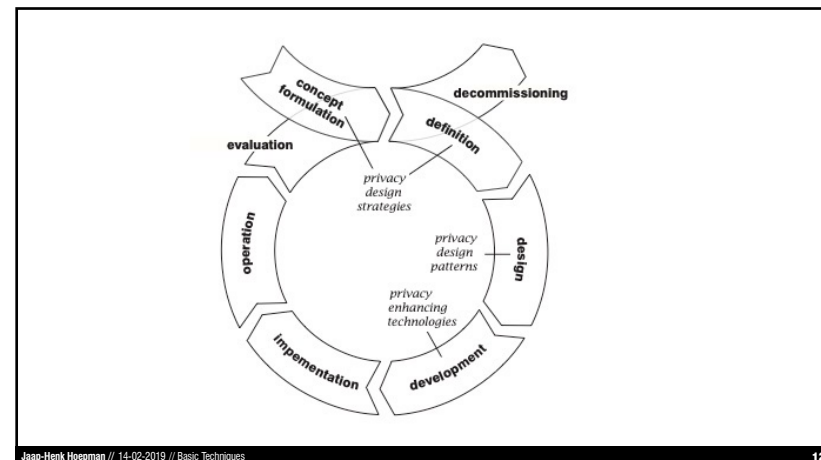
TILBURG UNIVERSITY Law School

university of groningen

Eight privacy design strategies

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 11

11



12

Privacy design strategies map fuzzy legal concepts to concrete data protection goals to help control data processing

Legal norms

(Technical) design requirements

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 13

13

Levels of abstraction

- **Design strategy**
 - “A basic method to achieve a particular design goal” - *that has certain properties that allow it to be distinguished from other basic design strategies*
- **Design pattern**
 - “Commonly recurring structure to solve a general design problem within a particular context”
- **(Privacy enhancing) technology**
 - “A coherent set of ICT measures that protects privacy” - *implemented using concrete technology*

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 14

14

Design pattern: example

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 15

15

Privacy design patterns

The “Aggregation over time” privacy design pattern

Jaap-Henk Hoepman

Name

Aggregation over time.

[Also Known As]

Summary

Instead of reporting immediately and continuously about resource consumption, a consumer of a resource keeps track of its consumption locally (using a trusted device) and periodically reports on its total consumption (over the last reporting period) to the provider of the resource. This prevents the provider to learn details about when exactly the consumer used the resource, while still informing the provider about the total amount of resources used by each individual consumer. Using *aggregation over time* protects the privacy of the consumer, while still allowing to charge consumers for their resource use (for example).

- **Describes a recurring pattern of communicating components that solve a general problem in a specific context**
 - Summary
 - Context
 - Problem
 - Solution
 - Structure
 - Consequences
 - Requirements
- <http://privacypatterns.org>
- <https://github.com/p4pnl/patterns>

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 16

16

Sources for the design strategies

- **Standards**
 - ISO 29100 Privacy framework
- **Principles**
 - OECD guidelines
 - Fair Information Practices (FIPs)
- **Law**
 - General Data Protection Regulation

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 17

17

Data protection law (core principles)

- **Legitimate Processing Grounds**
 - consent
 - necessity
- **Data Subject Rights**
 - Notification
 - Access
 - rectification
 - object to profiling
- **Data Protection Principles**
 - purpose limitation
 - data minimisation
 - duration of retention
 - accuracy of the data
- **Accountability**
 - risk based-approach
 - transparency of processing
 - data protection by design
 - data protection impact assessment

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 18

18

IT system = essentially a database, so...

The diagram illustrates the concept of an IT system as a database. It shows a grid of 'Individuals' (rows) and 'Attributes' (columns). An arrow points from this grid to a smaller grid, representing the application of data processing techniques: 'minimise', 'separate', 'abstract', and 'hide'.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 19

19

The diagram shows the interaction between a 'Data subject' and a 'Data controller'. The Data subject can 'inform' (indicated by an upward arrow) and 'control' (indicated by a downward arrow). The Data controller can 'demonstrate' (indicated by a document icon) and 'enforce' (indicated by a shield icon). The Data controller also performs actions like 'separate', 'abstract', 'hide', and 'minimise' (indicated by icons of a scissors, a magnifying glass, a crossed-out eye, and a scissors icon respectively).

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 20

20

Announcement

- **Due to the larger group size**
 - The student paper is expected to be roughly 12 pages long (excluding references, and using 10-11pt font, and reasonable margins)

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 21

21

#1 Minimize

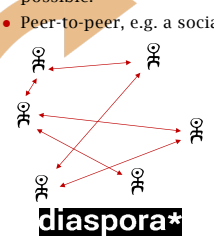
- **Definition**
 - *Limit as much as possible the processing of personal data.*
- **Associated tactics**
 - EXCLUDE: refrain from processing a data subject's personal data.
 - SELECT: decide on a case by case only relevant personal data.
- **Examples**
 - STRIP: partially remove unnecessary attributes.
 - DESTROY: completely remove all personal data as soon as they become unnecessary.
 - "Select before you collect".
 - Blacklist.
 - Whitelist.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 22

22

#2 Separate

- **Definition**
 - *Separate the processing of personal data as much as possible, to prevent correlation.*
- **Associated tactics**
 - ISOLATE: process personal data (for different purposes) independently in (logically) separate databases or systems.
 - DISTRIBUTE: process personal data (for one task) in physically separate locations.
- **Examples**
 - Edge computing: process data in the device of the user as much as possible.
 - Peer-to-peer, e.g. a social network.



Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 23

23

#3 Abstract

- **Definition**
 - *Limit as much as possible the detail in which personal data is processed.*
- **Associated tactics**
 - GROUP: aggregate data over groups of individuals, instead of processing data of each person separately.
 - SUMMARIZE: summarise detailed information into more abstract attributes.
 - PERTURB: add noise or approximate the real value of a data item.
- **Examples**
 - Process age instead of date of birth.
 - Aggregate data over time, in e.g. smart grids.
 - Pproximate the real location of a user (in e.g. 10 km² resolution).

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 24

24

#4 Hide

- **Definition**
 - Prevent personal data to become public or known.
- **Associated tactics**
 - RESTRICT: prevent unauthorized access to personal data.
 - ENCRYPT: encrypt data (in transit or when stored).
 - DISSOCIATE: remove the correlation between data subjects and their of personal data.
- **Examples**
 - MIX: process personal data randomly within a large enough group to reduce correlation.
 - OBFUSCATE: prevent understandability of personal data, e.g. by hashing them.
 - Mix networks, Tor.
 - Pseudonimisation.
 - Differential privacy.
 - Access control.
 - Attribute based credentials.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

25

25

#5 Inform

- **Definition**
 - Inform data subjects about the processing of their personal data.
- **Associated tactics**
 - SUPPLY: inform users which personal data is processed, including policies, processes, and potential risks.
 - EXPLAIN: provide this information in a concise and understandable form, and explain why the processing is necessary.
- **Examples**
 - NOTIFY: alert data subjects whenever their personal data are being used, or get breached.
 - Readable privacy policy.
 - Privacy icons.
 - Algorithmic transparency.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

26

26

#6 Control

- **Definition**
 - Provide data subjects control about the processing of their personal data.
- **Associated tactics**
 - CONSENT: only process personal data for which explicit, freely-given, and informed consent is received.
 - CHOOSE: allow data subjects to select which personal data will be processed.
- **Examples**
 - UPDATE: provide data subjects with the means to keep their personal data accurate and up to date.
 - RETRACT: honouring the data subject's right to the complete removal of any personal data in a timely fashion.
 - Opt-in (instead of opt-out).
 - Privacy dashboard.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

27

27

#7 Enforce

- **Definition**
 - Commit to processing personal data in a privacy friendly way, and enforce this.
- **Associated tactics**
 - CREATE: decide on a privacy policy that describes how you wish to protect personal data
 - MAINTAIN: maintain this policy, and
 - UPHOLD: ensuring that policies are adhered to by treating personal data as an asset, and privacy as a goal to incentivize as a critical feature.
- **Example**
 - Specify and enforce a privacy policy.
 - Assign responsibilities.
 - Check that the policy is effective, and adapt where necessary.
 - Take all necessary technical and organisational measures.

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques

28

28

#8 Demonstrate

Definition

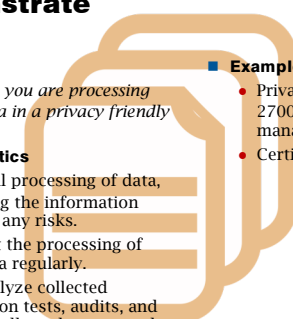
- Demonstrate you are processing personal data in a privacy friendly way.

Associated tactics

- LOG: track all processing of data, and reviewing the information gathered for any risks.
- AUDIT: audit the processing of personal data regularly.
- REPORT: analyze collected information on tests, audits, and logs periodically and report to the people responsible.

Example









- Privacy management system (cf. ISO 27001 information security management systems).
- Certification.



Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 29

29

Eight privacy design strategies

Data oriented	Process oriented
<p>MINIMIZE</p> <ul style="list-style-type: none"> • Limit as much as possible the processing of personal data.  	<p>INFORM</p> <ul style="list-style-type: none"> • Inform data subjects about the processing of their personal data. 
<p>SEPARATE</p> <ul style="list-style-type: none"> • Separate the processing of personal data as much as possible, to prevent correlation.  	<p>CONTROL</p> <ul style="list-style-type: none"> • Provide data subjects control about the processing of their personal data. 
<p>ABSTRACT</p> <ul style="list-style-type: none"> • Limit as much as possible the detail in which personal data is processed.  	<p>ENFORCE</p> <ul style="list-style-type: none"> • Commit to processing personal data in a privacy friendly way, and enforce this. 
<p>HIDE</p> <ul style="list-style-type: none"> • Prevent personal data to become public or known.  	<p>DEMONSTRATE</p> <ul style="list-style-type: none"> • Demonstrate you are processing personal data in a privacy friendly way. 

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 30

30

Tensions

- Privacy vs. Utility
- Privacy vs. Security
- Privacy vs. Usability
- Data protection vs privacy as norm
- Perception of the data subject vs data controller ininterests

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 31

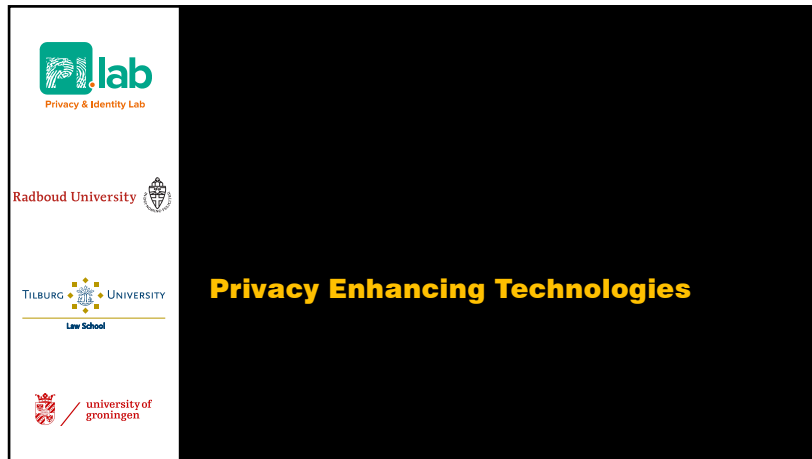
31




Further information

- G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tírtea, and S. Schiffner. Privacy and Data Protection by Design - from policy to engineering. Technical report, ENISA, December 2014. ISBN 978-92-9204-108-3, DOI 10.2824/38623. <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design>
- M. Colesky, J.-H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering - IWPE'16, San Jose, CA, USA, May 26 2016. <http://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf>

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 32

32



 Privacy & Identity Lab
 Radboud University
 TILBURG UNIVERSITY Law School
 university of groningen

Privacy Enhancing Technologies

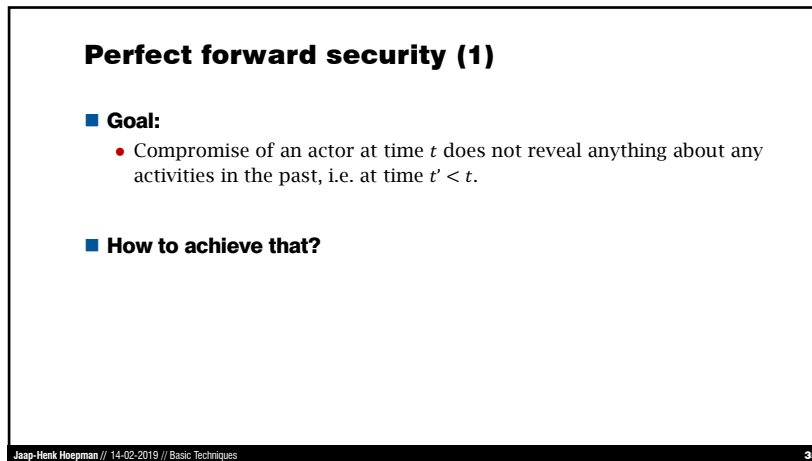
33



 Privacy & Identity Lab
 Radboud University
 TILBURG UNIVERSITY Law School
 university of groningen

PETS: forward and future secrecy

34

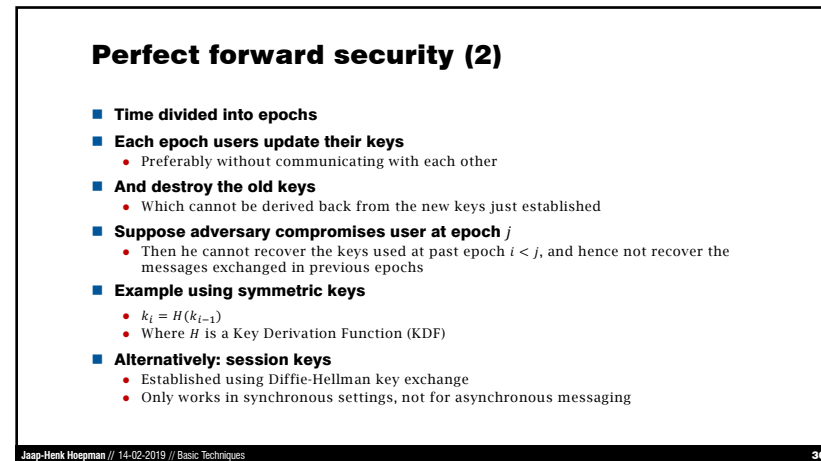


Perfect forward security (1)

- **Goal:**
 - Compromise of an actor at time t does not reveal anything about any activities in the past, i.e. at time $t' < t$.
- **How to achieve that?**

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 35

35



Perfect forward security (2)

- **Time divided into epochs**
- **Each epoch users update their keys**
 - Preferably without communicating with each other
- **And destroy the old keys**
 - Which cannot be derived back from the new keys just established
- **Suppose adversary compromises user at epoch j**
 - Then he cannot recover the keys used at past epoch $i < j$, and hence not recover the messages exchanged in previous epochs
- **Example using symmetric keys**
 - $k_t = H(k_{t-1})$
 - Where H is a Key Derivation Function (KDF)
- **Alternatively: session keys**
 - Established using Diffie-Hellman key exchange
 - Only works in synchronous settings, not for asynchronous messaging

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 36

36

Future secrecy (1)

- **Goal:**
 - Allow actors to recover from a compromise by an adversary
- **Observation**
 - Techniques for perfect forward security do **not** have this property
 - (Although for DH based techniques it depends on the threat model)
- **Again: how to achieve this?**

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 37

37

Future secrecy

- **'self-healing' property**
- **Suppose adversary compromised user at some epoch (or recovered keys used in this epoch), but user recovers at epoch i**
 - I.e. Adversary no longer controls user at epoch i
- **Then adversary**
 - cannot recover the keys used at future epoch $j > i$, and hence not recover the messages exchanged in future epochs
- **How to implement this: use OTR**
 - OTR advertises next key to use in a message, and sender will use this key as soon as recipient acknowledges this key

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 38

38

Forward security + Future secrecy

- **The Signal Ratchet**

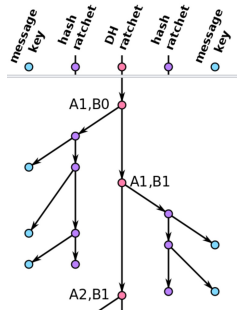


<https://signal.org/blog/advanced-ratcheting/>, <https://signal.org/docs/specifications/doublerratchet/>

Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 39

39

Signal's ratchet



- **Start with a root key R**
- **Alice uses ephemeral DH keys ($a_i, A_i = g^{a_i}$); Bob similarly**
 - Advertise A_i with every message
 - Generate next key A_{i+1} when receiving (correct) B_j from Bob
- **Whenever Alice generates new ephemeral key, advance the root**
 - $R' \leftarrow H(R, B_i^{a_{i+1}})$
 - Derive hash ratchet key $K = h(R')$
 - Hash this with every new message sent/received $K' = h(K)$
 - Derive message key $k = h(K)$

Jaap-Henk Hoepman // 30-01-2018 // Privacy by design 40

40

PETS: hiding metadata

41

Hiding metadata

- Mixnetworks
- Onion routing
- DC networks

■ Discussed in several other TRU/e courses...

Jaap-Henk Hoepman // 11-2-2016 // Privacy Enhancing Technologies 42

42

Homomorphic encryption

43

(Partial) Homomorphic encryption

- A public key encryption protocol $E_K: P \mapsto C$
 - From plaintext space P , with group operation $+$
 - To ciphertext space C , with group operation \times
- Such that
 - $E_K(a + b) = E_K(a) \times E_K(b)$ and hence also $c \times E_K(a) = E_K(a)^c$
- Example: Paillier (1999)
- What can you do with homomorphic encryption
 - Jointly compute the sum of private values, e.g. smart grid
 - Electronic voting

Jaap-Henk Hoepman // 11-2-2016 // Privacy Enhancing Technologies 44

44



Privacy & Identity Lab



Radboud University



TILBURG UNIVERSITY
Law School



university of
 groningen

Blind signatures

45

Blind signature

Alice public K Bob private k

$- r \in_R \mathbb{Z}_n^*$ $\xrightarrow{n \cdot r^k}$ sign with k

$- n$ $\xleftarrow{(n \cdot r^k)^k}$

divide by r


\Downarrow

n^k


Q: - different coin values?
- forgery?

Jaap-Henk Hoepman // 11-2-2016 // Privacy Enhancing Technologies 46


46




Privacy & Identity Lab



Radboud University



TILBURG UNIVERSITY
Law School



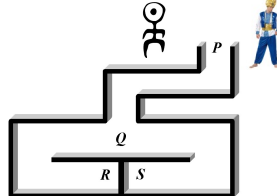
university of
 groningen

Zero-knowledge protocols

47

Zero knowledge

■ The cave of Ali Baba



How to Explain Zero-Knowledge Protocols to Your Children

QUISQUATER Jean-Jacques¹, Merlin, Michel, Michell

GELOUS Louis², Marie Annele, Gail, Anna, Gremel, Swing

in collaboration with Tom REESON³ for the English version

¹ Philips Research Laboratory, Avenue Van Broekelen, 3, B-1170 Brussels, Belgium

² OCEATECH, BP 59, F-35112 Combre Saint-James, France

³ Amazon Laboratories, P.O. Box 757, Palo Alto, CA 94301, USA

The Strange Cave of Ali Baba

Jaap-Henk Hoepman // 11-2-2016 // Privacy Enhancing Technologies 48

48

Vragen / discussie



[Monty Python's
Argument Clinic sketch]

jhh@cs.ru.nl www.cs.ru.nl/~jhh blog.xot.nl [twitter: @xotoxot](https://twitter.com/xotoxot)
Jaap-Henk Hoepman // 14-02-2019 // Basic Techniques 49