

# Advanced Computer Networks

---

Stephan Sigg

Georg-August-University Goettingen, Computer Networks

---

30.04.2015

# Outline

Revision: Secure authentication in the Internet

Motivation: spontaneous secure authentication for mobile devices

Radio channel

Security from RF

Security from noise

Security from audio

Physical random functions

Conclusion

# Desirable properties of secure communication

Confidentiality

Message integrity

Authentication (in communication systems)

Sender and receiver should be able to confirm the identity of the other party

Operational security

# Authentication

1  
client  
authent.

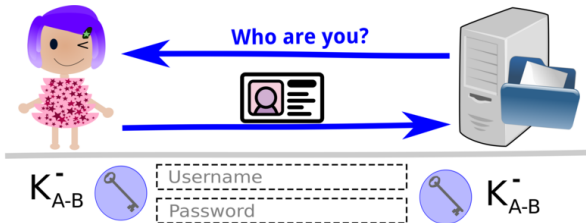


2  
server  
authent.





# Client-authentication



Login Symmetric key known to both sides

Von:

Chea Ting <chea.ting@spam.com>

An



"Stephan Sigg" <stephan.sigg@cs.uni-goettingen.de>

An



Betreff:

My new document

Dear Stephan,

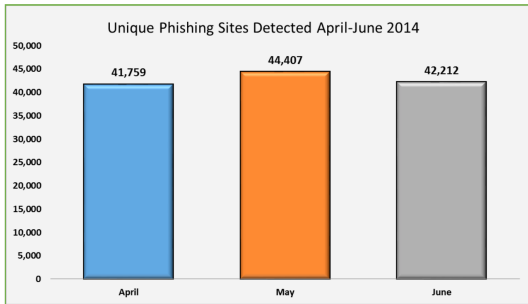
Please check out my modified  
document on Google docs:

<https://www.docs.google.com>

Cheers,

Klaus

Theft through phishing activities costs U.S. banks and credit card issuers an estimated \$2.8 billion annually.<sup>1</sup>



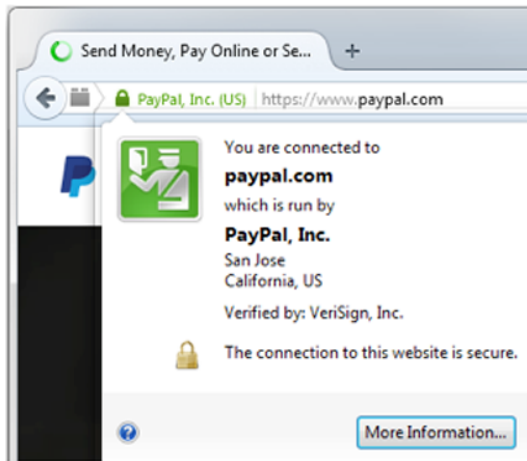
*April through June 2014 saw the second-highest number of phishing sites ever observed in a quarter. [p. 4]*

2

<sup>1</sup> Gartner Group, <http://www.gartner.com/newsroom/id/565125>

<sup>2</sup> from: APWG Phishing Attack Trends Reports (<http://www.antiphishing.org/resources/apwg-reports/>)

# Your browser knows the identity of the website visited

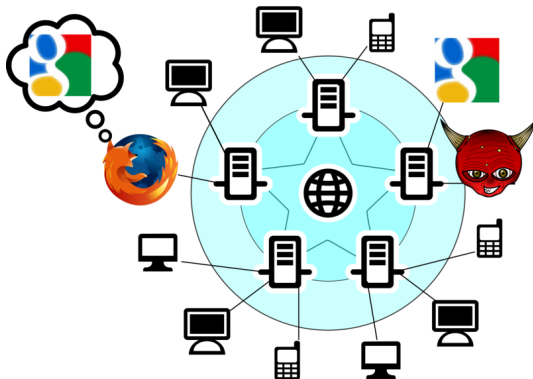


# Why is authentication difficult in communication systems?



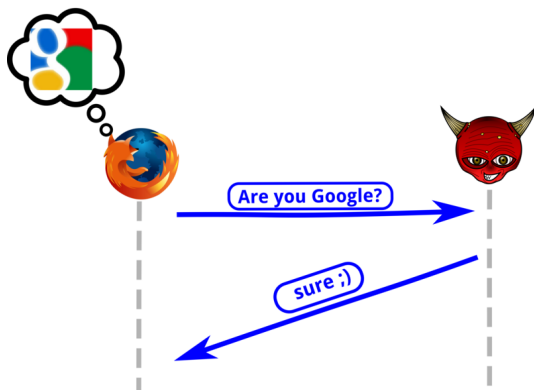
# Why is authentication difficult in communication systems?

⇒ Unlike face-to-face communication, other party is 'invisible'



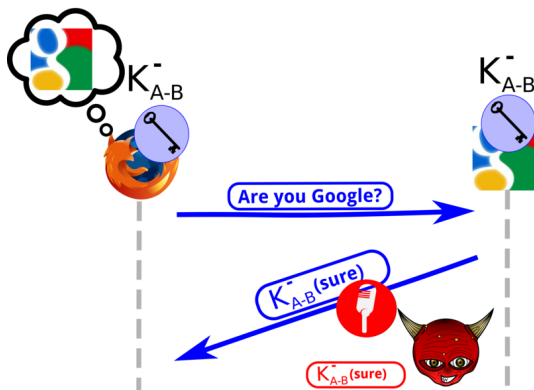
# Why is authentication difficult in communication systems?

⇒ Unlike face-to-face communication, other party is 'invisible'



## Why is authentication difficult in communication systems?

- ⇒ Unlike face-to-face communication, other party is 'invisible'
- ⇒ Replay attacks

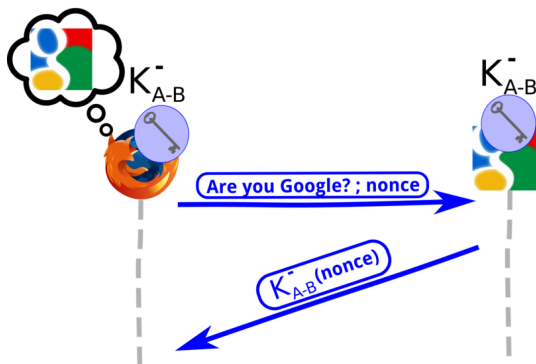




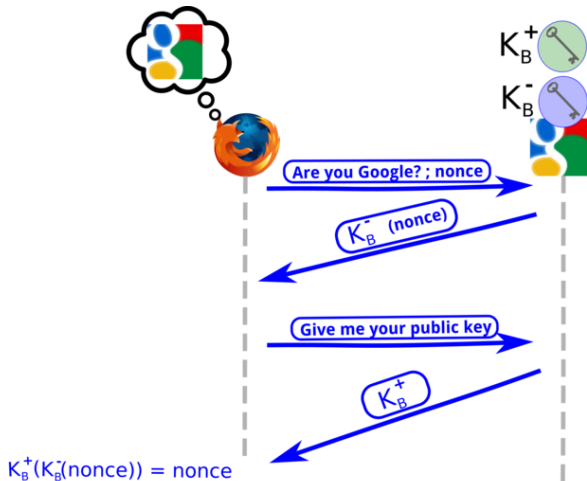
## Why is authentication difficult in communication systems?

- ⇒ Unlike face-to-face communication, other party is 'invisible'
- ⇒ Replay attacks

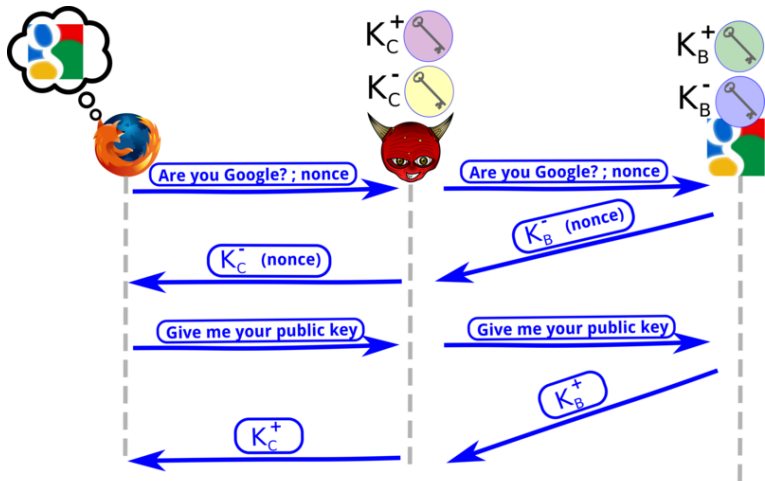
Solution? Using a nonce to ensure *freshness*



# Use asymmetric cryptography instead?

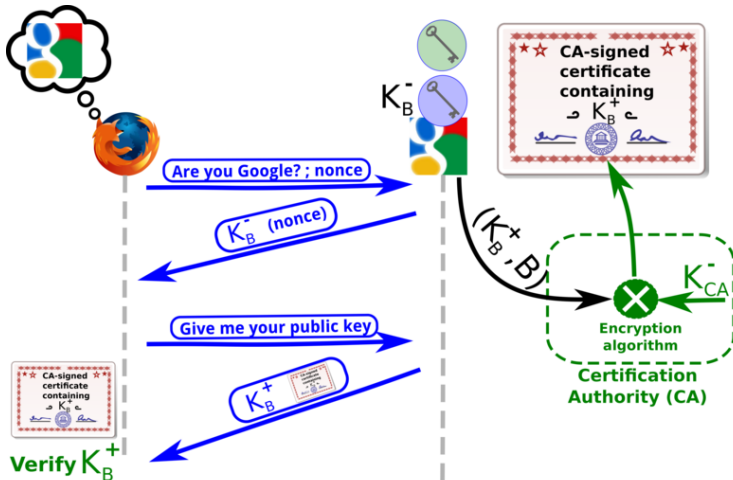


## Use asymmetric cryptography instead?



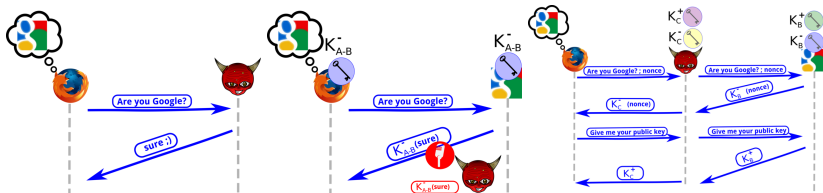
⇒ Vulnerable to Man-in-the-Middle attacks

# Solution: Certified Authority



⇒ CA issued certificate contains  $K_B^+$ ,  $B$ ; digitally signed by  $K_{CA}^-$

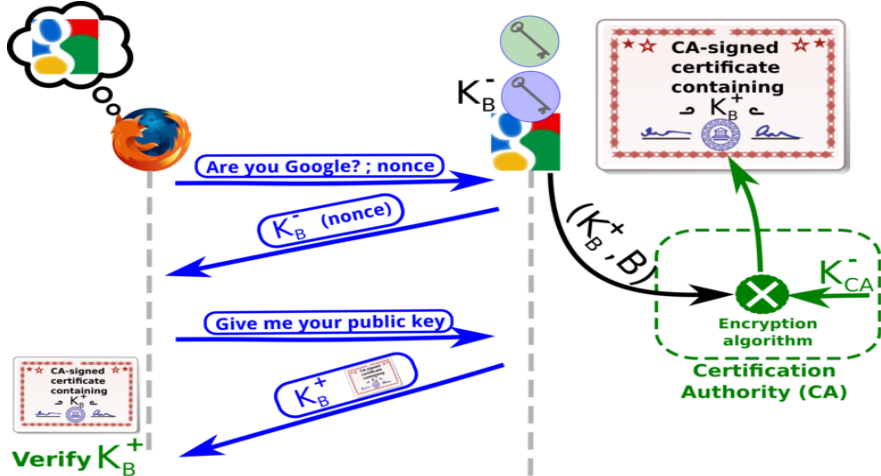
# Summary



- \* Authentication in communication systems is challenging
- \* Freshness/randomness to protect against replay attacks
- \* Asymmetric cryptography vulnerable to MiM attacks

Solution Trusted third party (CA)

# Summary



Solution Trusted third party (CA)

# Outline

Revision: Secure authentication in the Internet

Motivation: spontaneous secure authentication for mobile devices

Radio channel

Security from RF

Security from noise

Security from audio

Physical random functions

Conclusion

## Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.





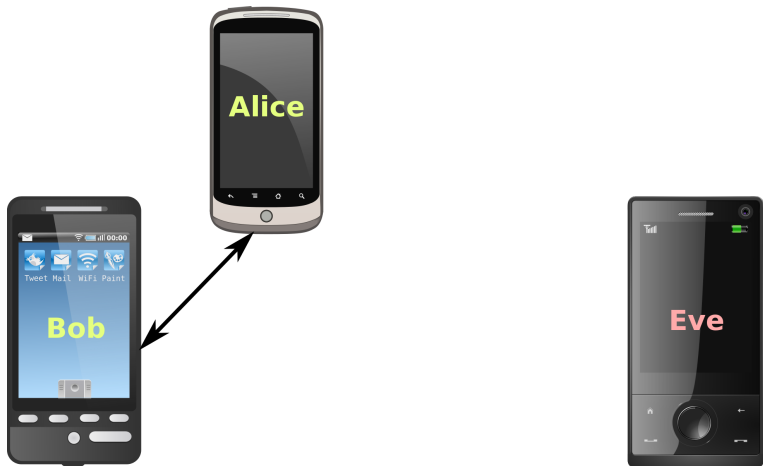
## Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



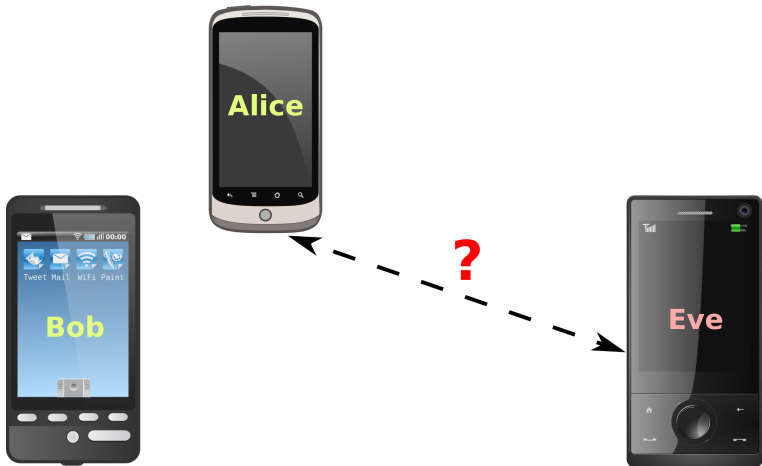
## Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



## Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



## Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**wireless signal propagation omnidirectional**  
**Similar problem as in wired networks**

**However, typically no certificates in**  
**D2D communication**



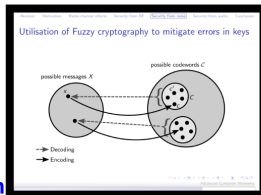
Navigation: Motivation, Radio channel, Security (RF), Security (noise), Security (Audio), Conclusion

### Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



Advanced Computer Networks



## Fuzzy cryptography for authentication

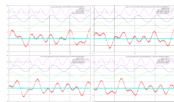
**Motivation**

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



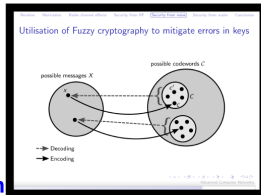
## Mobile radio channel

**Aspects of the mobile radio channel**



- Channel conditions are dependent on time and location
- Independent channel conditions typically expected in a distance of  $\frac{1}{2}$

## Fuzzy cryptography for authentication



**Motivation**

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- Independent channels at distance of  $\frac{1}{2}$

Mobile radio channel

RF-Examples

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

possible messages  $X$

possible codewords  $C$

→ Decoding

→ Encoding

**Fuzzy cryptography for authentication**

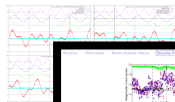


**Motivation**

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.




**Aspects of the mobile radio channel**



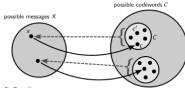
- Channel conditions
- Independent channels over distance of  $\frac{1}{2}$  km

**Fuzzy cryptography**

Utilise noise to improve security



**Utilisation of Fuzzy cryptography to mitigate errors in keys**



possible messages  $X$

possible codewords  $C$

→ Decoding

→ Encoding

Mobile  
radio  
channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

**Motivation**

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent of distance of  $\frac{1}{2}$

**Fuzzy cryptography**

Utilise noise to improve security

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

**Example: Spontaneous audio-based device pairing**

Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

Fuzzy crypto using ambient audio for auth.

**Motivation**  
 Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent of distance of  $\frac{1}{2}$

**Fuzzy cryptography**

Utilise noise to improve security

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

**Example: Spontaneous audio-based device pairing**



**Physical random functions**

**Optical PUF:** Made of transparent optical medium containing bubbles. Shining a laser beam through the medium produces speckle pattern (response) that depends on exact position/direction of incoming beam.

**Physically unclonable func.**

**Mobile radio channel**

**RF-Examples**

**Security from pure noise**

**Fuzzy cryptography for authentication**

**Fuzzy crypto using ambient audio for auth.**

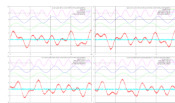
Motivation

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



## Mobile radio channel

Aspects of the mobile radio channel



- Channel conditions are dependent on time and location
- Independent channel conditions typically expected in a distance of  $\frac{1}{2}$

# Aspects of the mobile radio channel

## RF transmission

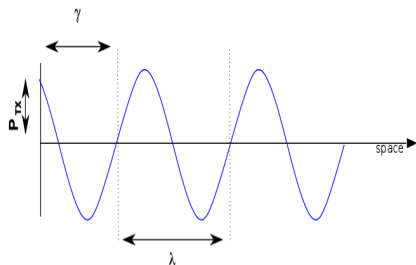
- Electromagnetic signals
- Transmitted in wave-Form
- Omnidirectional transmission
- Speed of light
  - $c = 3 \cdot 10^8 \frac{m}{s}$



# Aspects of the mobile radio channel

## RF signal

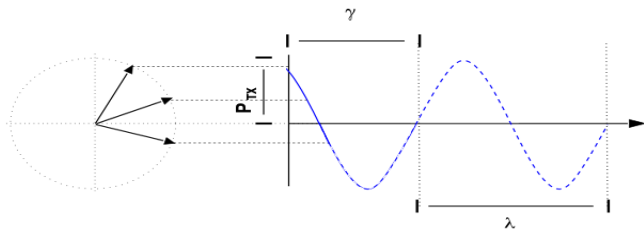
- Transmission power:
  - $P_{TX}[W]$
- Frequency:
  - $f[\frac{1}{sec}]$
- Phase offset:
  - $\gamma[\pi]$
- Wavelength:
  - $\lambda = \frac{c}{f}[m]$



# Aspects of the mobile radio channel

## RF signal

- Real part of rotating vector
  - $\zeta = \Re(e^{j(ft+\gamma)})$
- Instantaneous signal strength:
  - $\cos(\zeta)$
- Rotation Speed: Frequency  $f$



## Video: Changes in Audio

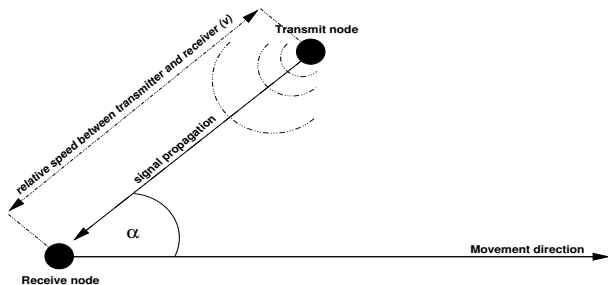
DRK



# Video: Doppler Effect

Doppler

# Aspects of the mobile radio channel



## Doppler Shift

- Frequency of received and transmitted signal may differ
- Dependent on relative speed between transmitter and receiver
- $f_d = \frac{v}{\lambda} \cdot \cos(\alpha)$

# Aspects of the mobile radio channel

## Noise

- In every realistic setting, noise can be observed on the wireless channel
- Typical noise power:<sup>3</sup>

$$P_N = -103dBm$$

- Value observed by measurements

---

<sup>3</sup>3GPP: 3rd generation partnership project; technical specification group radio access networks; 3g home nodeb study item technical report (release 8). Technical Report 3GPP TR 25.820 V8.0.0 (2008-03) (March)

# Aspects of the mobile radio channel

## Noise

- Thermal noise can also be estimated analytically as

$$P_N = \kappa \cdot T \cdot B$$

- $\kappa = 1.3807 \cdot 10^{-23} \frac{J}{K}$ : Boltzmann constant
- $T$ : Temperature in Calvin
- $B$ : Bandwidth of the signal.

# Aspects of the mobile radio channel

## Example

- GSM system with 200kHz bands
- Average temperature: 300K
- Estimated noise power:

$$\begin{aligned}P_N &= \kappa \cdot T \cdot B \\ &= 1.3807 \cdot 10^{-23} \frac{\text{J}}{\text{K}} \cdot 300\text{K} \cdot 200\text{kHz} \\ P_N &= -120.82\text{dBm}\end{aligned}$$

# Aspects of the mobile radio channel

## Path-loss

- Signal strength decreases while propagating over a wireless channel
- Order of decay varies in different environments
- Impact higher for higher frequencies
- Can be reduced by antenna gain (e.g. directed)

Location	Mean Path loss exponent	Shadowing variance $\sigma^2$ (dB)
Apartment Hallway	2.0	8.0
Parking structure	3.0	7.9
One-sided corridor	1.9	8.0
One-sided patio	3.2	3.7
Concrete Canyon	2.7	10.2
Plant fence	4.9	9.4
Small boulders	3.5	12.8
Sandy flat beach	4.2	4.0
Dense bamboo	5.0	11.6
Dry tall underbrush	3.6	8.4

# Aspects of the mobile radio channel

## Path-loss

- For analytic consideration: Path-loss approximated
- Friis free-space equation:

$$P_{TX} \cdot \left( \frac{\lambda}{2\pi d} \right)^2 \cdot G_{TX} \cdot G_{RX}$$

# Aspects of the mobile radio channel

## Path-loss

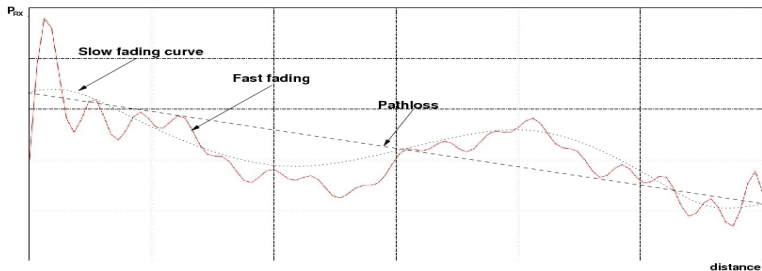
$$P_{RX} = P_{TX} \cdot \left( \frac{\lambda}{2\pi d} \right)^2 \cdot G_{TX} \cdot G_{RX}$$

- Utilised in outdoor scenarios
  - Direct line of sight
  - No multipath propagation
- $d$  impacts the RSS quadratically
- Other values for the path-loss exponent  $\alpha$  possible.
- Path-loss:

$$PL^{FS}(\zeta_i) = \frac{P_{TX}(\zeta_i)}{P_{RX}(\zeta_i)}$$



# Aspects of the mobile radio channel



## Fading

- Signal quality fluctuating with location and time
- Slow fading
- Fast fading

# Aspects of the mobile radio channel

## Slow fading

- Result of environmental changes
- Temporary blocking of signal paths
- Changing reflection angles
- Movement in the environment
  - Trees
  - Cars
  - Opening/closing doors
- Amplitude changes can be modelled by log-normal distribution

# Aspects of the mobile radio channel

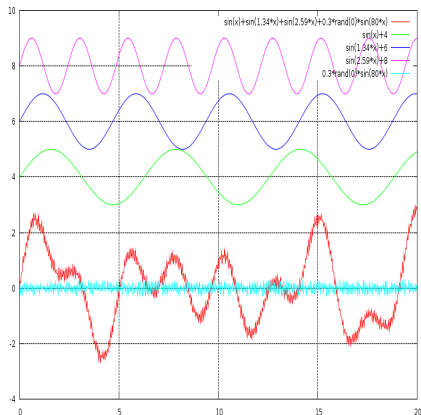
## Fast fading

- Signal components of multiple paths
- Cancellation of signal components
- Fading incursions expected in the distance of  $\frac{\lambda}{2}$
- Channel quality changes drastically over short distances
- Example: Low radio reception of a car standing in front of a headlight is corrected by small movement
- Stochastic models are utilised to model the probability of fading incursions
  - Rice
  - Rayleigh

# Aspects of the mobile radio channel

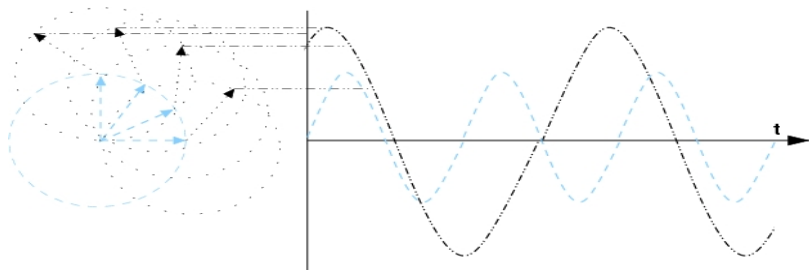
## Superimposition of RF signals

- The wireless medium is a broadcast channel
- Multipath transmission
  - Reflection
  - Diffraction
  - Different path lengths
  - Signal components arrive at different times
- Interference



$$\zeta_{\text{sum}} = \sum_{i=1}^l \Re \left( e^{j(f_i t + \gamma_i)} \right)$$

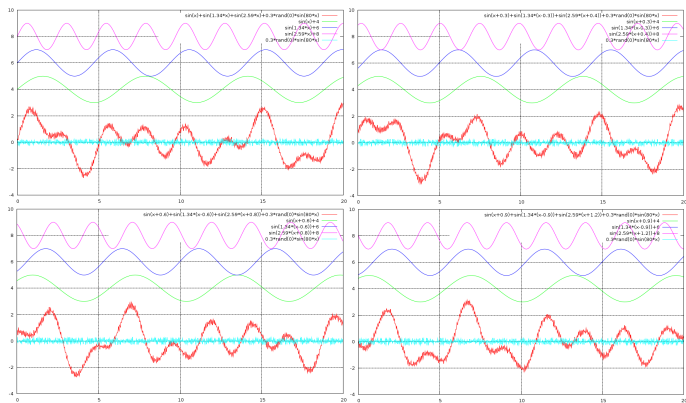
## Aspects of the mobile radio channel



### Superimposition of RF signals

- At a receiver, all incoming signals add up to one superimposed sum signal
- Constructive and destructive interference
- Normally: Heavily distorted sum signal

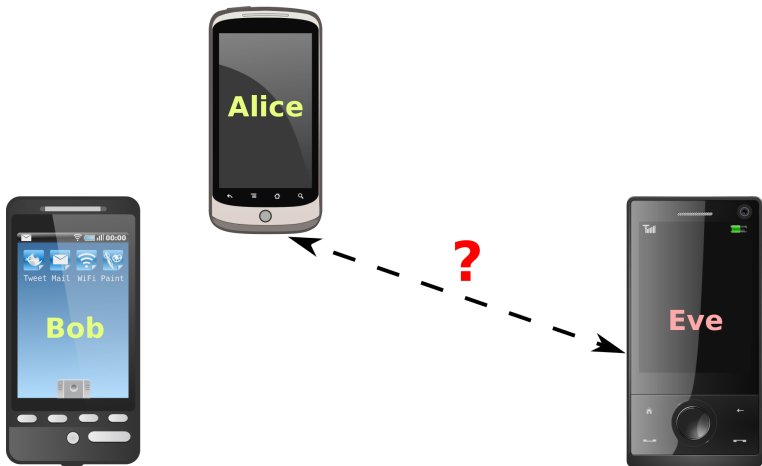
# Aspects of the mobile radio channel



- Channel conditions are dependent on time and location
- Independent channel conditions typically expected in a distance of  $\frac{\lambda}{2}$

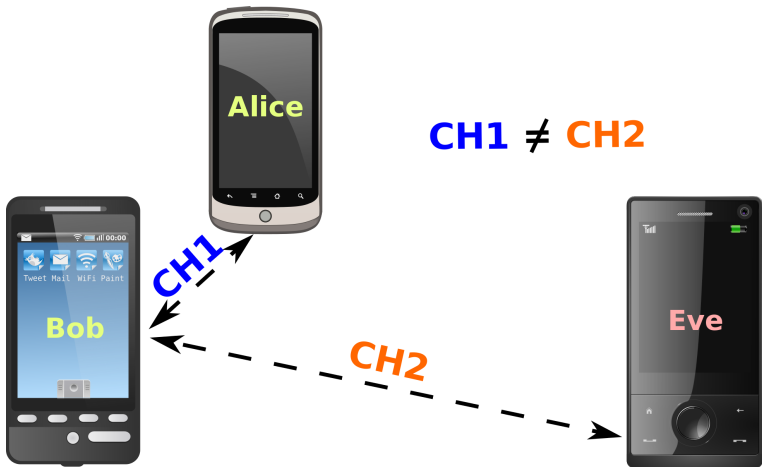
## With respect to our Motivation:

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



## With respect to our Motivation:

Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.





## Aspects of the mobile radio channel

Received signal is defined by the transmitted signal and the applied modifications through the channel (**Unique for each link!**)

$$r(t) = s(t) \cdot h(t)$$

## Aspects of the mobile radio channel

Received signal is defined by the transmitted signal and the applied modifications through the channel (Unique for each link!)

$$r(t) = s(t) \cdot h(t)$$

General multi-antenna case:

$$\vec{\zeta}^{RX} = \begin{bmatrix} \zeta_1^{RX} \\ \zeta_2^{RX} \\ \vdots \\ \zeta_M^{RX} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1L} \\ h_{21} & \ddots & & h_{2L} \\ \vdots & & \ddots & \vdots \\ h_{M1} & h_{M2} & \cdots & h_{ML} \end{bmatrix} \begin{bmatrix} \zeta_1^{TX} \\ \zeta_2^{TX} \\ \vdots \\ \zeta_L^{TX} \end{bmatrix} + \begin{bmatrix} \zeta_1^{\text{noise}} \\ \zeta_2^{\text{noise}} \\ \vdots \\ \zeta_M^{\text{noise}} \end{bmatrix}$$

## Aspects of the mobile radio channel

Received signal is defined by the transmitted signal and the applied modifications through the channel (Unique for each link!)

$$r(t) = s(t) \cdot h(t)$$

General multi-antenna case:

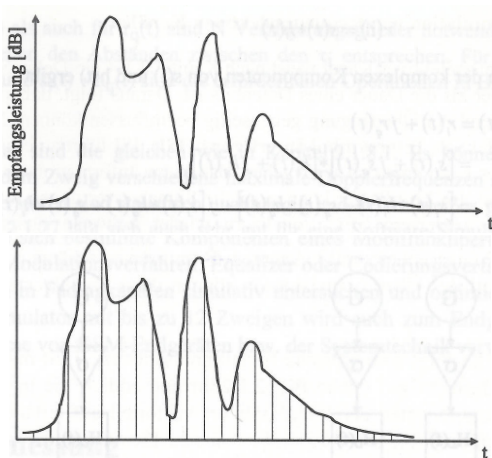
$$\vec{\zeta}^{RX} = \begin{bmatrix} \zeta_1^{RX} \\ \zeta_2^{RX} \\ \vdots \\ \zeta_M^{RX} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1L} \\ h_{21} & \ddots & & h_{2L} \\ \vdots & & \ddots & \vdots \\ h_{M1} & h_{M2} & \cdots & h_{ML} \end{bmatrix} \begin{bmatrix} \zeta_1^{TX} \\ \zeta_2^{TX} \\ \vdots \\ \zeta_L^{TX} \end{bmatrix} + \begin{bmatrix} \zeta_1^{\text{noise}} \\ \zeta_2^{\text{noise}} \\ \vdots \\ \zeta_M^{\text{noise}} \end{bmatrix}$$

### Simulation of frequency selective channels

- Common approach: Estimate channel impulse response (CIR) with training bit-sequence
- Correct signal distortions with CIR

# Aspects of the mobile radio channel

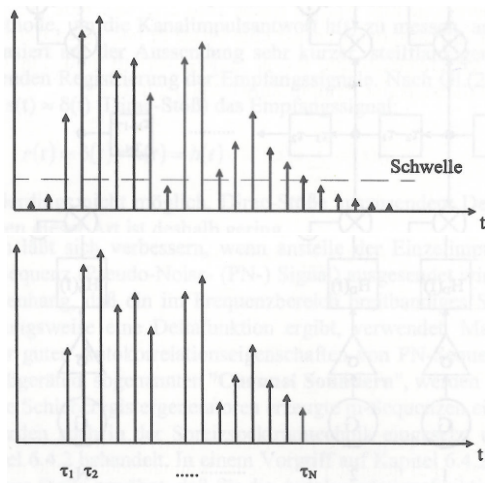
## Simulation of frequency selective channels<sup>4</sup>



<sup>4</sup> David, Benkner, Digitale Mobilfunksysteme, Teubner, 1996

# Aspects of the mobile radio channel

## Simulation of frequency selective channels



# Aspects of the mobile radio channel

## Channel estimation

Approximate  $h(t)$  in the time domain:

- Send very short impulses
  - Can be improved by using pseudo-noise sequence instead of single identical impulses
- Inverse of estimated CIR  $\overline{h(t)^{-1}}$  correlated with received signal:

$$r(t) \cdot \overline{h(t)^{-1}} = s(t) \cdot h(t) \cdot \overline{h(t)^{-1}} \approx s(t)$$

# RF-based activity recognition

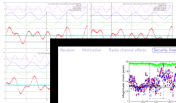
Sensewaves Video

**Motivation**

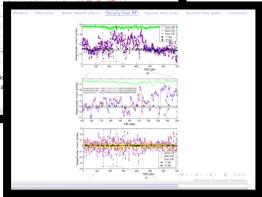
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



**Aspects of the mobile radio channel**



- Channel conditions
- Independent channel conditions at distance of  $\frac{1}{2}$  mile



**Mobile radio channel**

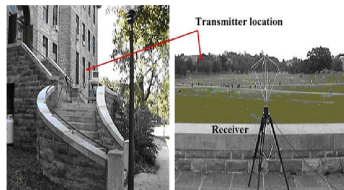
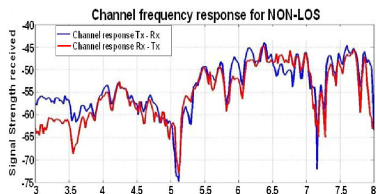
**RF-Examples**



## Security from RF

### Secure communication based on deep fades in the SNR<sup>5</sup>

- Communication partners agree on a threshold value
- Both nodes transmit repeatedly and alternately
- Channel characteristics are transformed to bit sequence
  - Signal envelope below threshold in timeslot: 1, else 0
- No specialised hardware required
  - Only threshold detectors which are already present in transceivers

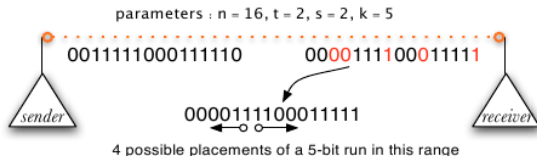


<sup>5</sup> Azimi-Sadjadi, Kiayias, Mercado, Yener, Robust Key Generation from Signal Envelopes in Wireless Networks, CCS, 2007

# Security from RF

## Secure communication based on deep fades in the SNR

- Key generation
  - 1 Sender and receiver sample bit sequences
  - 2 Sender transmits key verification information to receiver
  - 3 Receiver decides on correct key by scanning through all possible error vectors

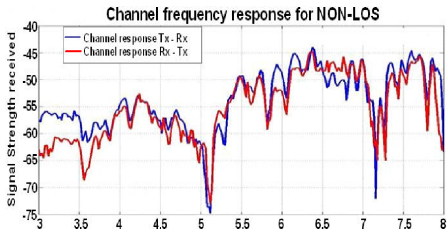


# Security from RF

## Secure communication based on deep fades in the SNR

- Discussion

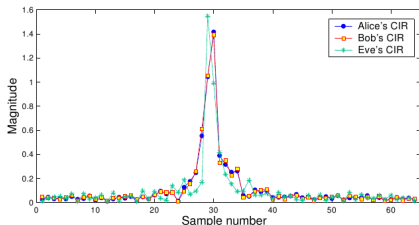
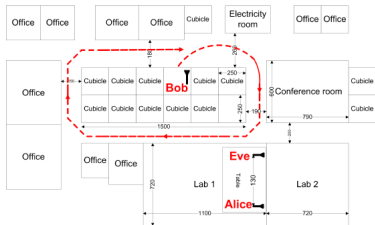
- 1 Computationally cheap approach
- 2 No special hardware required
- 3 Probably uneven distribution of 0 and 1 (Dependent on Channel characteristics and time slot)
- 4 Key generation in the presence of noise not optimal



# Security from RF

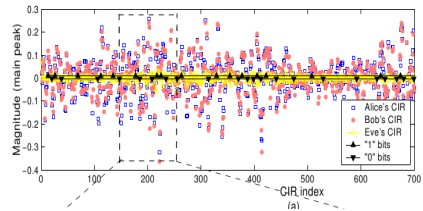
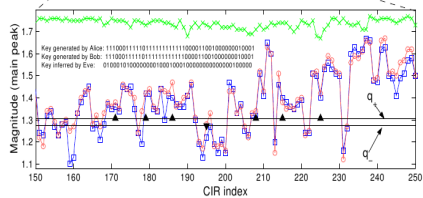
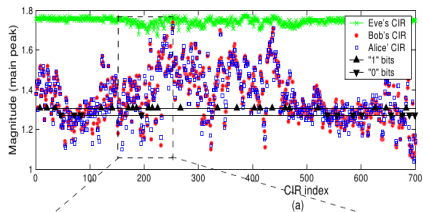
## Secure communication based on the CIR<sup>6 7</sup>

- Utilise Channel impulse response as secure secret
  - Utilise magnitude of CIR main peak
  - Transformed to binary sequence via Threshold
  - Error correction method required in order to account for noise in the binary sequences



<sup>6</sup> Mathur, Trappe, Mandayam, Ye, Reznik, Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, MobiCom, 2008

<sup>7</sup> Tmar, Hamida, Pierrot, Castelluccia, An adaptive quantisation algorithm for secret key generation using radio channel measurements, NTMS, 2009



**Motivation**  
 Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent of distance of  $\frac{1}{2}$

**Fuzzy cryptography**

**Utilise noise to improve security**

Diagram illustrating the use of noise to improve security in a communication system:

$X \oplus N = Y$  (Alice's side)  
 $Y \oplus Z = C$  (Bob's side)  
 $X \oplus Z = Z$  (Alice's side)  
 $C = X \oplus Z$  (Final output)

Mobile radio channel

RF-Examples

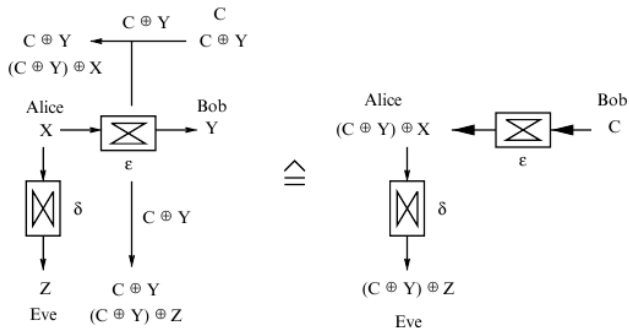
Security from pure noise

# Exploit noise for security among devices

- Utilise noise in a common communication channel
- Employ Fuzzy cryptography to mitigate noise for legitimate communication partners

# Security from noise

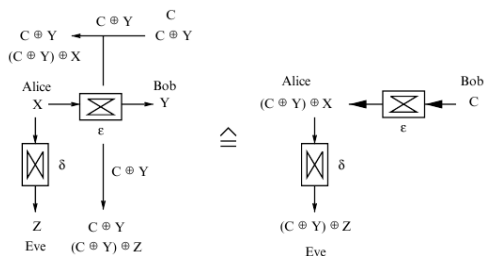
Utilise noise to improve security





# Security from noise

Utilise noise to improve security

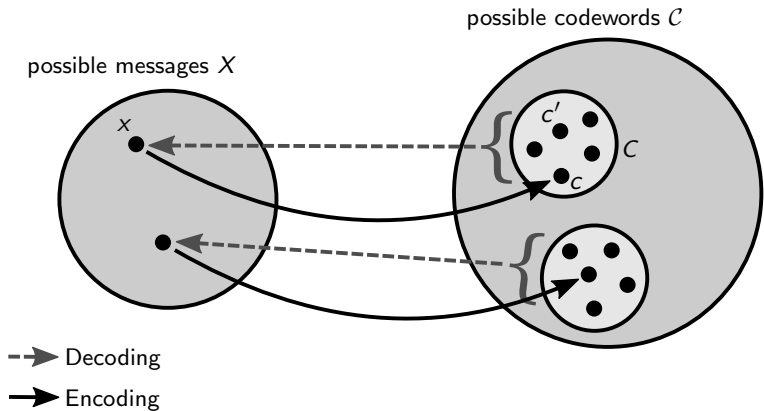


By inverting the direction of communication the noise in Eve's reception is increased above those in Alice's

Establishing of a secure key is possible over binary symmetric channel iff the noise in the reception of Eve's message is higher<sup>8</sup>

<sup>8</sup>Wyner, The wire-tap channel, Bell system Technical Journal, 54:1355-1387,1975

# Utilisation of Fuzzy cryptography to mitigate errors in keys



**Motivation**  
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent of distance of  $\frac{1}{2}$

**Fuzzy cryptography**

Utilise noise to improve security

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

possible messages  $X$

possible codewords  $C$

→ Decoding

→ Encoding

Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

# Fuzzy cryptography

## Commitment schemes

Traditional cryptographic systems rely on secret bit-strings.

When key contains errors (e.g. noise or mistake), decryption fails.

Rigid reliance on perfectly matching secret keys makes classical cryptographic systems less practicable in noisy systems.

**Fuzzy commitment:** cryptographic primitive to handle independent random corruptions of bits in a key.

# Fuzzy cryptography

## Commitment schemes

Traditional cryptographic systems rely on secret bit-strings for secure management of data.

A **cryptographic commitment scheme** is a function

$$G : C \times X \rightarrow Y$$

To commit a value  $\kappa \in C$  a witness  $x \in X$  is chosen uniformly at random and  $y = G(\kappa, x)$  is computed.

A decommitment function takes  $y$  and a witness to obtain the original  $\kappa$

$$G^{-1} : Y \times X \rightarrow C$$

# Fuzzy cryptography

## Traditional Commitment

A well defined commitment scheme shall have two basic properties.

**Binding** It is infeasible to de-commit  $y$  under a pair  $(\kappa', x')$  such that  $\kappa \neq \kappa'$

**Hiding** Given  $y$  alone, it is infeasible to compute  $\kappa$

# Fuzzy cryptography

## Fuzzy Commitment

Fuzzy commitment is an encryption scheme that allows for the use of approximate witnesses

Given a commitment  $y = G(\kappa, x)$ , the system can recover  $\kappa$  from any witness  $x'$  that is close to but not necessarily equal to  $x$ .

Closeness in fuzzy commitment is measured by Hamming distance.

# Fuzzy cryptography

## Fuzzy Commitment

A fuzzy commitment scheme may be based on any (linear) error-correcting code

An error-correcting code consists of

**Message space**  $M \subseteq F^a$  ( $F^i$  denotes all strings of length  $i$  from a finite set of symbols  $F$ )

**Codeword space**  $C \subseteq F^b$  with  $(b > a)$

**Bijection**  $\theta : M \leftrightarrow C$

**Decoding function**  $f : C' \rightarrow C \cup \perp$  (The symbol  $\perp$  denotes the failure of  $f$ )

The function  $f$  maps an element in  $C'$  to its nearest codeword in  $C$ .



# Fuzzy cryptography

## Fuzzy Commitment

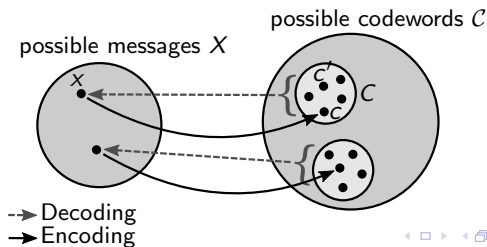
Noise of physical function may be viewed as the difference  $c - c'$

Decoding function  $f$  applied to recover original codeword  $c$

This is successful if  $c'$  is close to  $c$ . In this case:  $c = f(c')$

The minimum distance of the code is the smallest distance  $d = Ham(c - c')$  between any two codewords  $c, c' \in C$

Typically, it is possible to correct at least  $\frac{d}{2}$  errors in a codeword



# Fuzzy cryptography

## Fuzzy Commitment

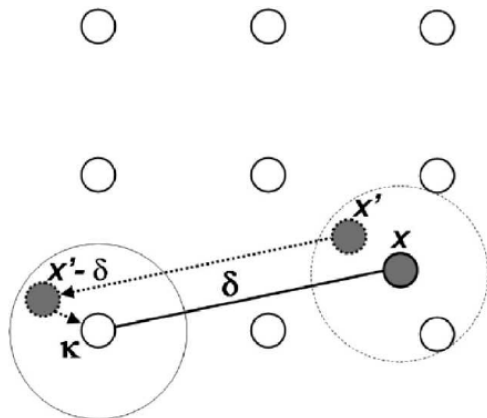
For fuzzy commitment, the secret key  $\kappa$  is chosen uniformly at random from the codeword space  $C$ . Then,

- 1 An offset  $\delta = x - \kappa$  is computed
- 2 A one-way, collision-resistant hash function is applied to obtain  $h(\kappa)$
- 3  $y = (\delta, h(\kappa))$  is made public
- 4  $\kappa' = f(x' - \delta)$  is computed
- 5 It is possible to de-commit  $y$  under a witness  $x'$  with  $\text{Ham}(x, x') < \frac{d}{2}$

Once  $\kappa$  is recovered, its correctness may be verified by computing  $z = h(\kappa)$

# Fuzzy cryptography

## Fuzzy Commitment



**Motivation**  
 Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent of distance of  $\frac{1}{2}$

**Fuzzy cryptography**

Utilise noise to improve security

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

**Example: Spontaneous audio-based device pairing**

**Mobile radio channel**

**RF-Examples**

**Security from pure noise**

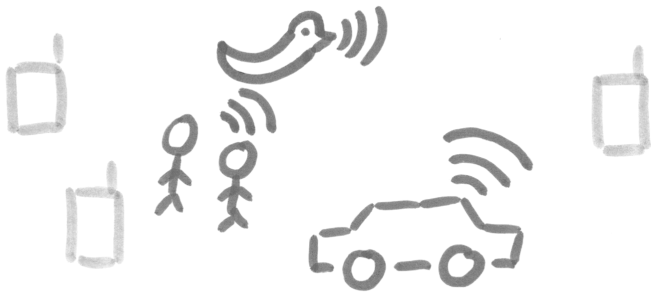
**Fuzzy cryptography for authentication**

**Fuzzy crypto using ambient audio for auth.**

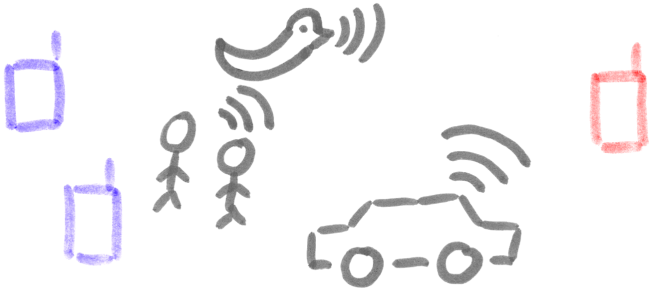
## Example: Spontaneous audio-based device pairing



## Example: Spontaneous audio-based device pairing



# Example: Spontaneous audio-based device pairing



## Example: Spontaneous audio-based device pairing

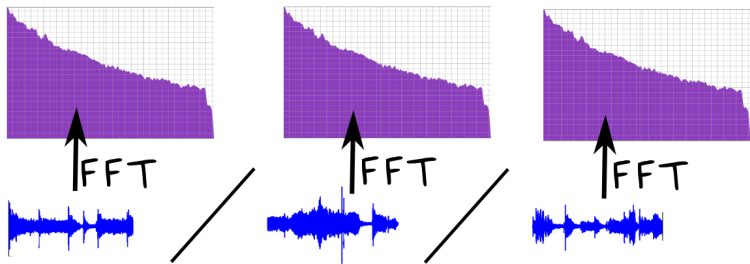




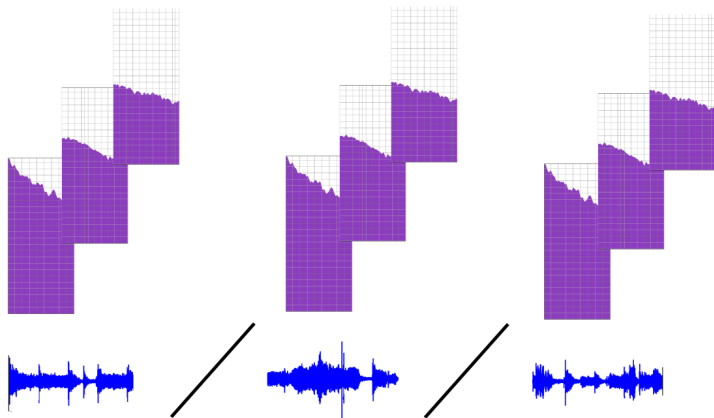
## Example: Spontaneous audio-based device pairing



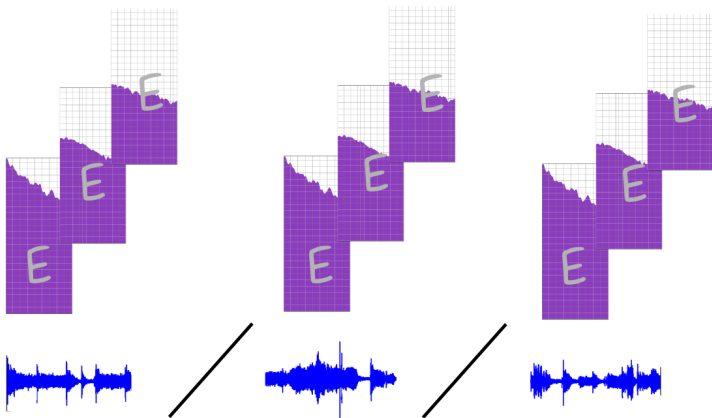
# Example: Spontaneous audio-based device pairing



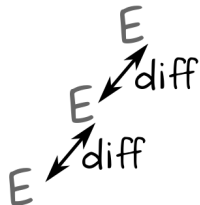
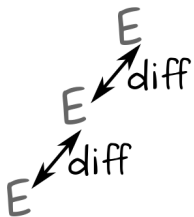
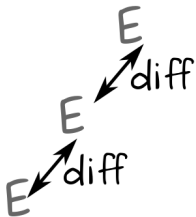
# Example: Spontaneous audio-based device pairing



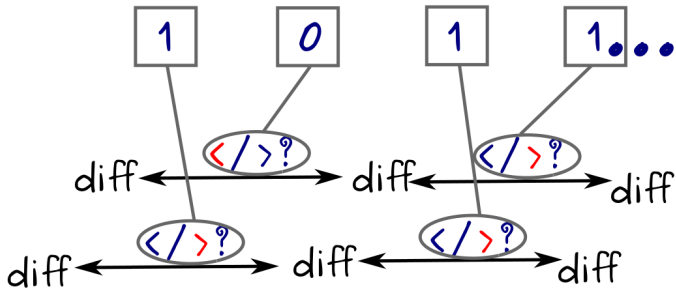
# Example: Spontaneous audio-based device pairing



## Example: Spontaneous audio-based device pairing



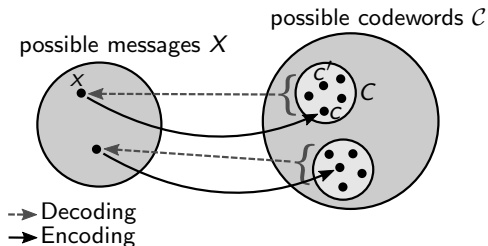
## Example: Spontaneous audio-based device pairing



# Encryption and decryption in the presence of noise

## Fuzzy cryptography

- We can, however, utilise error correcting codes to account for errors in an input sequence
- The general idea is to utilise a function that maps from a feature space to another, key space



## Example: Spontaneous audio-based device pairing





## Example: Spontaneous audio-based device pairing

f 10110...11011

f 11011...01110

F 10010...01011

## Example: Spontaneous audio-based device pairing

f 10110...11011

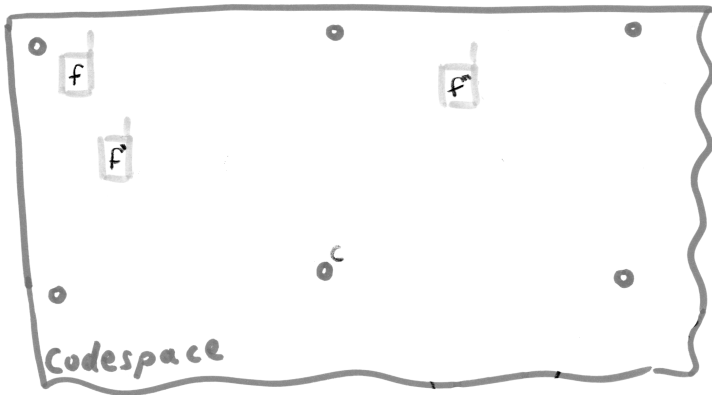
f 11011...01110

F 10010...01011

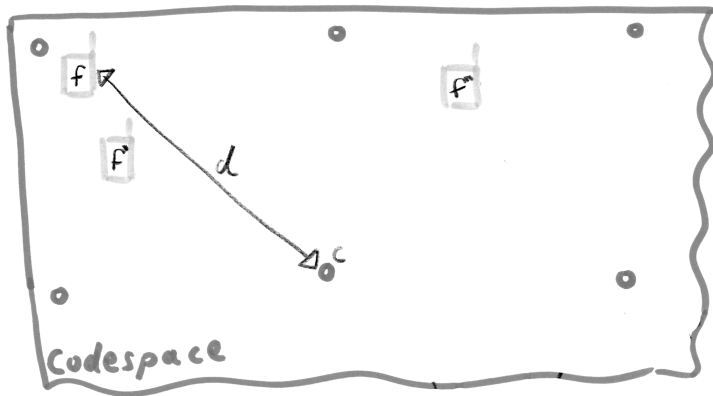
## Example: Spontaneous audio-based device pairing



## Example: Spontaneous audio-based device pairing



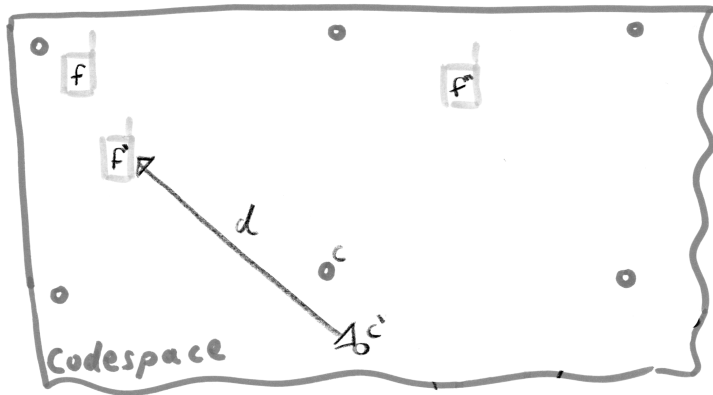
## Example: Spontaneous audio-based device pairing



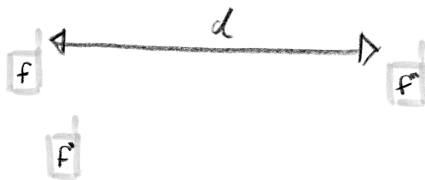
## Example: Spontaneous audio-based device pairing



## Example: Spontaneous audio-based device pairing

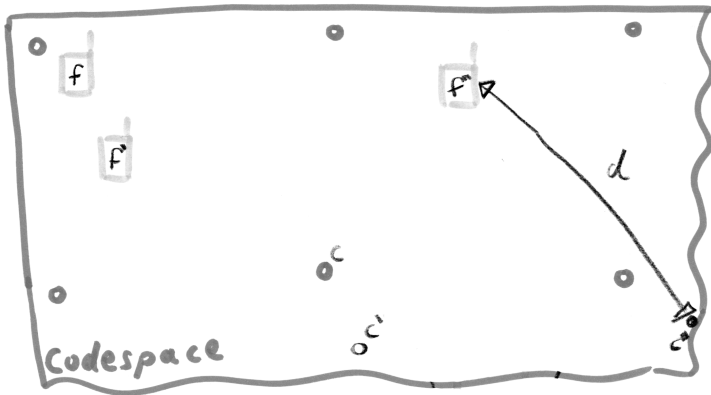


## Example: Spontaneous audio-based device pairing

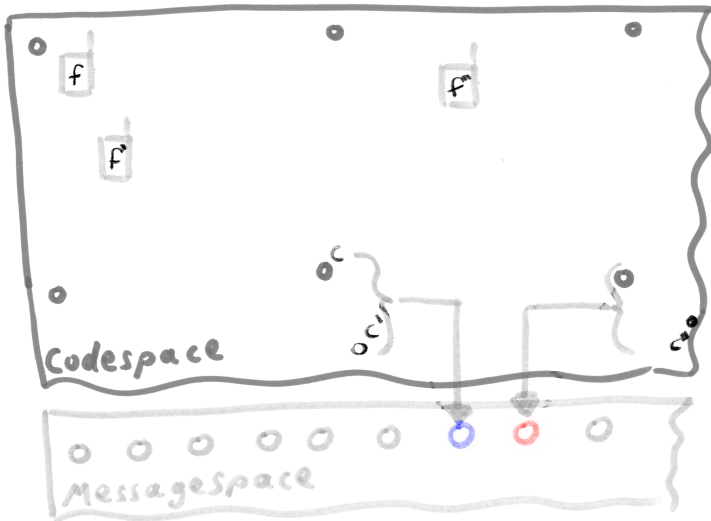




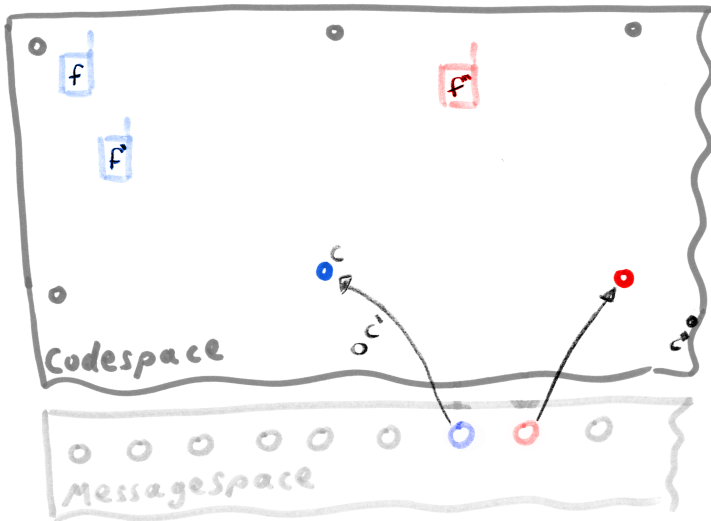
## Example: Spontaneous audio-based device pairing



## Example: Spontaneous audio-based device pairing



# Example: Spontaneous audio-based device pairing



**Motivation**  
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent over distance of  $\frac{1}{2}$

**Fuzzy cryptography**

Utilise noise to improve security

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

possible messages  $X$

→ Decoding  
→ Encoding

**Physical random functions**

**Optical PUF:** Made of transparent optical medium containing bubbles. Shining a laser beam through the medium produces speckle pattern (response) that depends on exact position/direction of incoming beam.



**Physically unclonable func.**

**Mobile radio channel**

**RF-Examples**

**Security from pure noise**

**Fuzzy cryptography for authentication**

**Fuzzy crypto using ambient audio for auth.**

**Example: Spontaneous audio-based device pairing**

# Physical random functions

## Physical random functions / Physically unclonable functions

Random functions that can only be evaluated with the help of a physical system

# Physical random functions

## Physical random functions / Physically unclonable functions

Random functions that can only be evaluated with the help of a physical system

### Definition

A PUF is a random function that can only be evaluated with the help of a specific physical system. The inputs to a physical random function are challenges and the outputs are responses.

# Physical random functions

## Physical random functions / Physically unclonable functions

Random functions that can only be evaluated with the help of a physical system

### Definition

A PUF is a random function that can only be evaluated with the help of a specific physical system. The inputs to a physical random function are challenges and the outputs are responses.

The essential idea of PUFs is to utilise inherent properties of a physical device which are not possible to re-produce given current technological advance.

# Physical random functions

**Digital PUFs** Simplest kind of PUF. Digital key  $K$  is embedded in a tamper-proof package along with some logic that computes

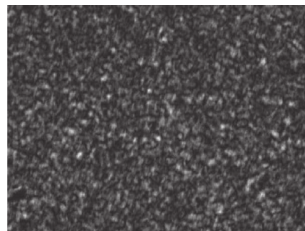
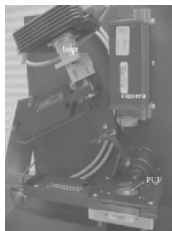
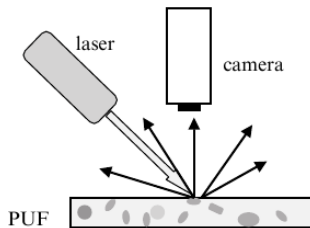
$$\text{Response} = RF(K, \text{Challenge})$$

for some random function  $RF$



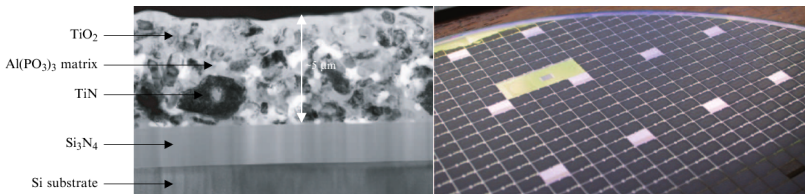
# Physical random functions

**Optical PUFs** Made of transparent optical medium containing bubbles. Shining a laser beam through the medium produces speckle pattern (response) that depends on exact position/direction of incoming beam.



# Physical random functions

**Silicon PUFs** Challenge is an input to a circuit that reconfigures the path that signals follow through the circuit. Response is related to the time it takes for signals to propagate through a complex circuit.



# Physical random functions

Security of PUFs relies on difficulty of extracting all necessary parameters from a complex physical system

## An attacker

trying to extract all physical parameters might modify the PUF in the process

This makes PUFs tamper resistant to some extent

## Physical random functions

PUF implementations build on random manufacturing variations (bubble position or exact wire delays):

Exact behaviour is a mystery even for the manufacturer

Not feasible to create two identical copies of a PUF

A difficulty of optical and silicon PUFs is that their output is noisy

Error correction that does not compromise the security is required<sup>9</sup>

---

<sup>9</sup>G.E. Suh, C.W. O'Donnell, I. Sachdev, S. Devadas, Design and implementation of the AEGIS single-chip secure processor using physical random functions, Proceedings of the 32nd Annual International Symposium of computer Architecture, 2005

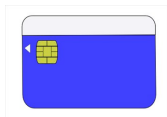
## Physical random functions

Standard application: Key-card<sup>10</sup>

Lock stores a database of challenge response pairs (CRPs) for PUF

When the bearer of the PUF wants to open the lock, it selects a challenges it knows and asks the PUF for the corresponding response

Each CRP can be used only once : Card will eventually run out of PUFs



---

<sup>10</sup>R. Pappu, Physical One-Way Functions, PhD thesis, MIT, 2001

# Outline

Revision: Secure authentication in the Internet

Motivation: spontaneous secure authentication for mobile devices

Radio channel

Security from RF

Security from noise

Security from audio

Physical random functions

Conclusion

# Controlled Physical random functions

## Definition

Controlled physical random function (CPRUF):

PUF that can only be accessed through specific API

Main problem with uncontrolled PUFs: Anybody can query the PUF for the response to any challenge

In order to engage in cryptography with a PUF device, a user has to exploit the fact that only she and the device know the response to a specific challenge.

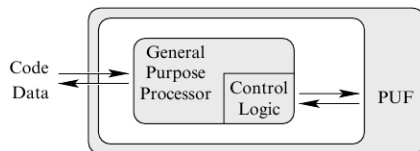
# Controlled Physical random functions

Third party could try to overhear challenge, obtain response from PUF and spoof the device

## Problem: MiM

Adversary can freely query the PUF

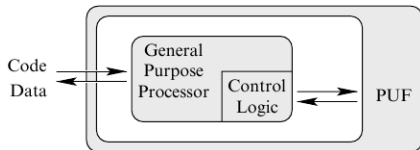
By using CPUFs, Access to PUF restricted by control algorithm that prevents this attack



Embedding control logic for PUF in physical system of PUF makes it difficult to conduct invasive attacks on the control logic



# Controlled Physical random functions



The PUF and its control logic have complementary roles

The PUF protects the control logic from invasive attacks

The control logic protects the PUF from protocol attacks

# Controlled Physical random functions

## Applications for CPUFs

Applications for CPUFs include applications that require single symmetric key on a chip

- **Smartcards that implement authentication:**

Current smart-cards: Hidden digital keys can be extracted using various attacks

PUF on the smartcard: Can authenticate chip – Digital key not required (Smartcard hardware itself is the secret key)

Key can not be duplicated: Person that temporary loses control of card need not fear that an adversary might have cloned the card or that the security became somehow impaired.

# Outline

Revision: Secure authentication in the Internet

Motivation: spontaneous secure authentication for mobile devices

Radio channel

Security from RF

Security from noise

Security from audio

Physical random functions

Conclusion

# CPUF API

CPUF typically modelled as general-purpose processing element with access to a PUF

## Man-in-the-Middle Attack:

Adversary intercepts communication to device wants Alice to accept incorrect result as coming from device

Alice would execute the following protocol

# CPUF API

Alice would execute the following protocol

- 1 Pick one CRP (Char, Response) at random
- 2 Execute the following function on the PUF:

```
1: GetAuthenticBroken(Chal){
2:     my Resp = PUF(Chal);
3:     // Do some computation, produce result
4:     return (Result, MAC(Result, Resp));
5: }
```
- 3 Use the MAC and Response to check that the data is authentic

# CPUF API

Protocol is not secure against Man-in-the-Middle attacks

Attacker could

- 1 Intercept message send to `GetAuthenticBroken` and extract `Chal`
- 2 Execute on the PUF:
  - 1: `StealResponse(Chal){`
  - 2: `return (PUF(Chal));`
  - 3: `}`
- 3 Forward Alice the message `MAC(FakeResult, Response)`
- 4 Since the MAC was computed with the correct response, Alice accepts `FakeResult`

# CPUF API

Problem: When Alice releases her challenge, Adversary can ask PUF for corresponding response and impersonate PUF

Problem persists as long as the PUF freely provides responses

# CPUF API

## GetSecret

To solve this problem:

PUF shall only be accessed via call

$\text{GetSecret}(\text{Chal}) = \text{Hash}(\text{PHashReg}, \text{PUF}(\text{Chal}))$

PUF reveals combination of response and executed program instead of response

Since the Hash is a one-way function: Response not recovered easily



# CPUF API

## GetSecret

We alter the call of Alice accordingly:

```
1: GetAuthenticBroken(Chal){
2:     hashblock()({// HB
3:         // Do some computation, produce result
4:     });
5:     my Secret = GetSecret(Chal);
6:     return (Result, MAC(Result, Secret));
7: }
```

# CPUF API

## GetSecret

Alice can now compute Secret from Response by computing  $\text{Hash}(\text{PHash}(\text{HB}), \text{Response})$  to check the MAC

An adversary has no way of obtaining Secret

# CPUF API

## GetCRP

However, the solution presented may be too restrictive for Alice also

With no CRP:

No way for Alice to obtain one in the first place:  
Device never reveals response

Possible solution: Primitive called GetCRP that

- 1 Picks a random challenge
- 2 Computes the response
- 3 Returns the response to the caller

When space of challenges large enough:

Unlikely that attacker can compute CRPs identical to Alice's

# CPUF API

## GetResponse

Problem: Random number generators often vulnerable to attacks

Therefore: Might prefer alternative that not relies on a RNG that much

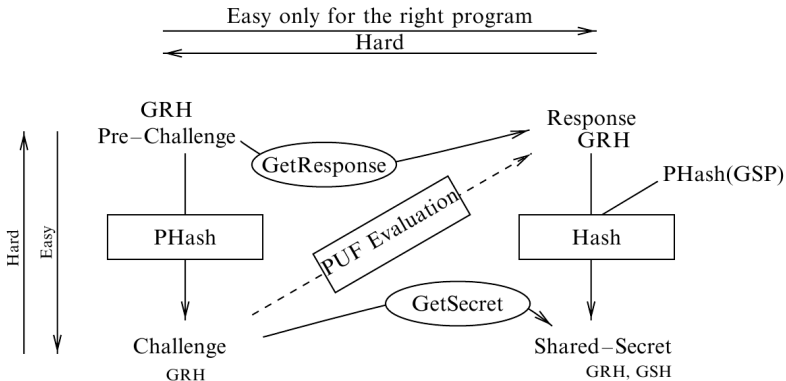
Replace `GetCRP` by `GetResponse()`=`PUF(PHashReg)`

Now: Anybody can generate CRP (`PHashReg,GetResponse()`)

But: Due to hash function, nobody can generate specific CRP

# CPUF API

## GetResponse



# CPUF API

## GetResponse

Man-in-the-Middle attack is prevented since each user has his own CRPs

Challenges can be public, but responses are required to be private

When not told the secret and GSH not leaks information, adversary can only obtain secret by hashing appropriate response

No way for adversary to obtain this response

Therefore:

Man-in-the-Middle attacks are prevented since PUF accessed only through GetSecret and GetResponse.

# CPUF API

## Challenge response pair management

How to get the response to the legitimate user?

The following sequence is proposed for CRP management

- After manufacturing manufacturer gets device-CRP with Bootstrap
- Manufacturer uses Introduction to provide CRPs to certification authorities
- Certification authorities provide CRPs to end users
- Anybody in possession of a CRP can create new CRPs by Renew

# CPUF API

## Bootstrapping

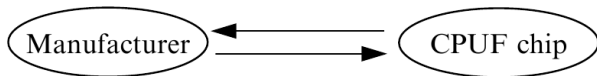
① Pick a pre-challenge `PreChal` at random

② Execute

```
1: Bootstrap(PreChal){
2:     hashblock(PreChal){
3:         Return GetResponse();
4:     };
5: }
```

③ The challenge for the CRP is obtained by calculating `PHash(HB)`

If `PreChal` is not known, the security relies on the hash function





# CPUF API

## Renewal

- 1 Pick a pre-challenge `PreChal` at random
- 2 By using an old challenge `OldChal`, execute

```
1: Renew(OldChal, PreChal){
2:     hashblock(OldChal, PreChal){
3:         my NewResponse = GetResponse();
4:         my Secret = GetSecret(OldChal);
5:         return Encrypt(NewResponse,
6:             Secret); //Key:Secret
7:     }
8: }
```

- 3 Compute `Hash(PHash(HB), OldResponse)` to calculate `Secret`, check the MAC with it and retrieve `NewResponse`

# CPUF API

## Renewal

When the response corresponding to `OldCha1` is only known to the user, the method is secure.



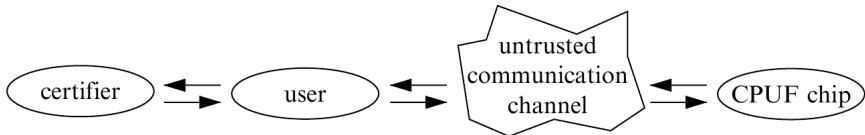
# CPUF API

## Introduction

Provide user with CRP

Assumption:

Trusted channel between user and certifier



# CPUF API

## Introduction

- 1 Cert. authority picks (OldChal, OldResponse), computes  $\text{Secret} = \text{Hash}(\text{PHash}(\text{HB}), \text{OldResponse})$  and returns (OldChal, Secret)
- 2 User picks pre-challenge PreChal at random and executes

```

1: Introduction(OldChal, PubKey, PreChal){
2:     hashblock(PubKey, PreChal){{
3:         my NewResponse = GetResponse();
4:         my Message = PublicEncrypt(NewResponse,
      PubKey);
5:         my Secret' = GetSecret(OldChal);
6:         Return (Message, MAC(Message, Secret'));
7:     }};
8: }
```

- 3 User checks MAC with Secret. ( $\text{Secret} = \text{Secret}'$  since both are computed as  $\text{Hash}(\text{PHash}(\text{HB}), \text{OldResponse})$ ). User Decrypts Message and computes PHash(HB) to obtain Response and Challenge

**Motivation**  
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

**Aspects of the mobile radio channel**

- Channel conditions
- independent of distance of  $\frac{1}{2}$

**Fuzzy cryptography**

Utilise noise to improve security

**Utilisation of Fuzzy cryptography to mitigate errors in keys**

**Physical random functions**

**Optical PUF:** Made of transparent optical medium containing bubbles. Shining a laser beam through the medium produces speckle pattern (response) that depends on exact position/direction of incoming beam.



**Physically unclonable func.**

**Mobile radio channel**

**RF-Examples**

**Security from pure noise**

**Fuzzy cryptography for authentication**

**Fuzzy crypto using ambient audio for auth.**

**Example: Spontaneous audio-based device pairing**

# Questions?

Stephan Sigg

`stephan.sigg@cs.uni-goettingen.de`

# Literature

- C.M. Bishop: Pattern recognition and machine learning, Springer, 2007.
- P. Tuly, B. Skoric, T. Kevenaar: Security with Noisy Data – On private biometrics, secure key storage and anti-counterfeiting, Springer, 2007.
- R.O. Duda, P.E. Hart, D.G. Stork: Pattern Classification, Wiley, 2001.

