Advanced Computer Networks

Stephan Sigg

Georg-August-University Goettingen, Computer Networks

30.04.2015

Outline

Desirable properties of secure communication

Confidentiality

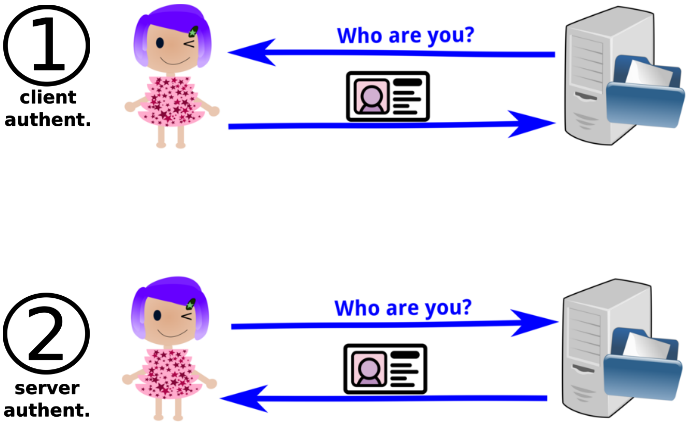
Message integrity

Authentication (in communication systems)

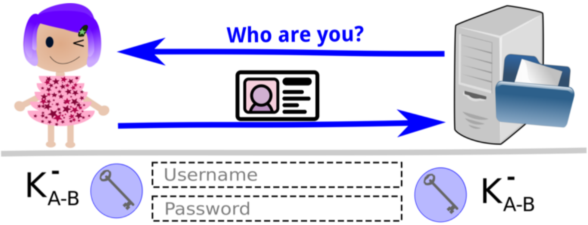
Sender and receiver should be able to confirm the identity of the other party

Operational security

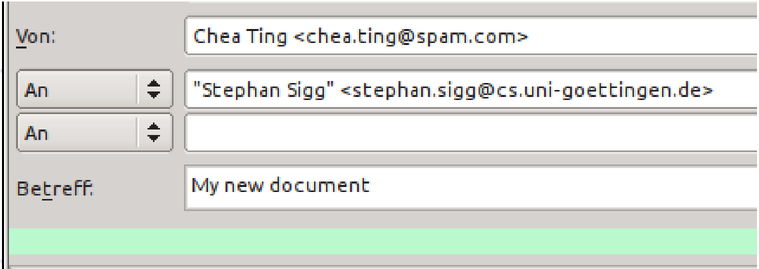
Authentication



Client-authentication



Login Symmetric key known to both sides



Dear Stephan,

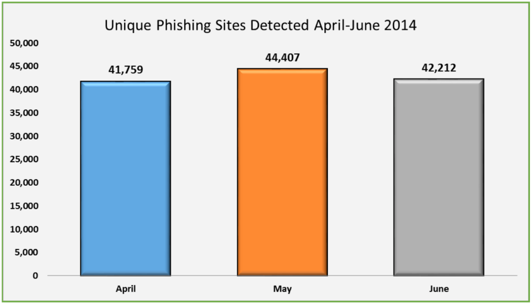
Please check out my modified document on Google docs:

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.[1]



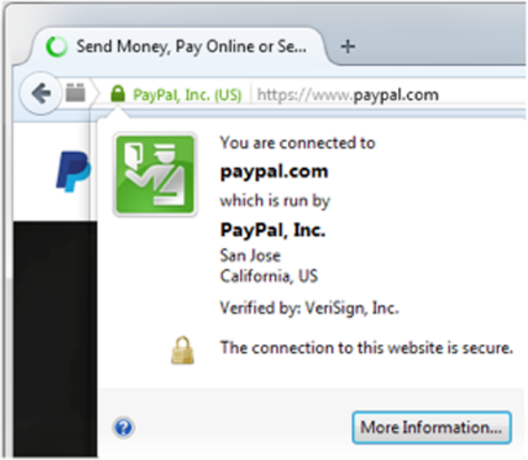
April through June 2014 saw the second-highest number of phishing sites ever observed in a quarter. [p. 4]

2

[1] Gartner Group, http://www.gartner.com/newsroom/id/565125

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

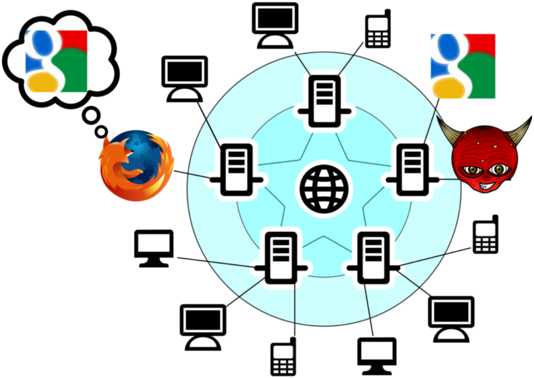
Your browser knows the identity of the website visited



Why is authentication difficult in communication systems?

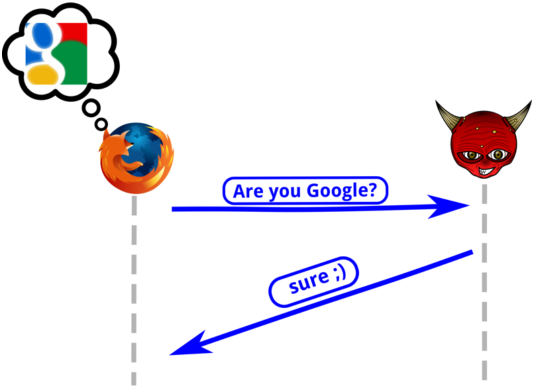
Why is authentication difficult in communication systems?

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



Why is authentication difficult in communication systems?

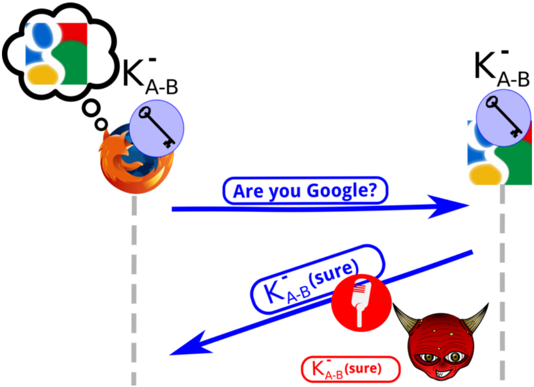
⇒ Unlike face-to-face communication, other party is 'invisible'



Why is authentication difficult in communication systems?

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

⇒ Replay attacks

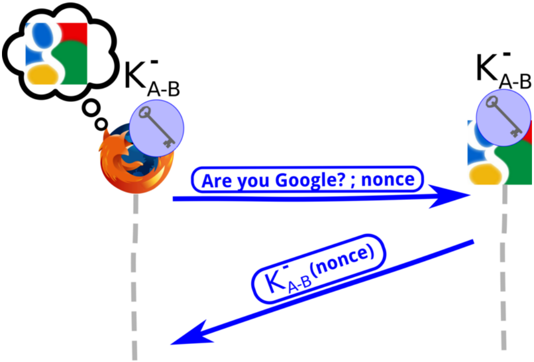


Why is authentication difficult in communication systems?

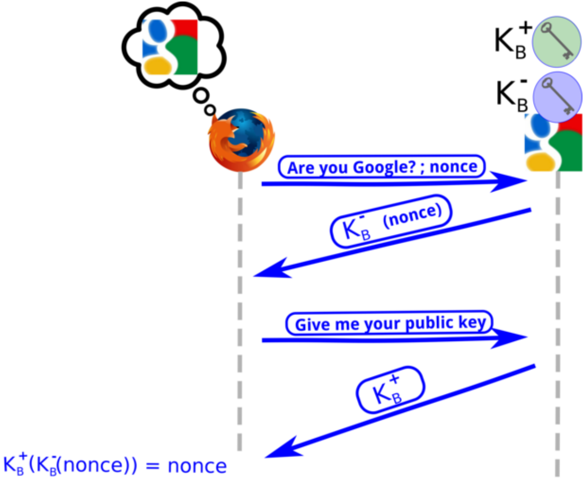
⇒ Unlike face-to-face communication, other party is 'invisible'

⇒ Replay attacks

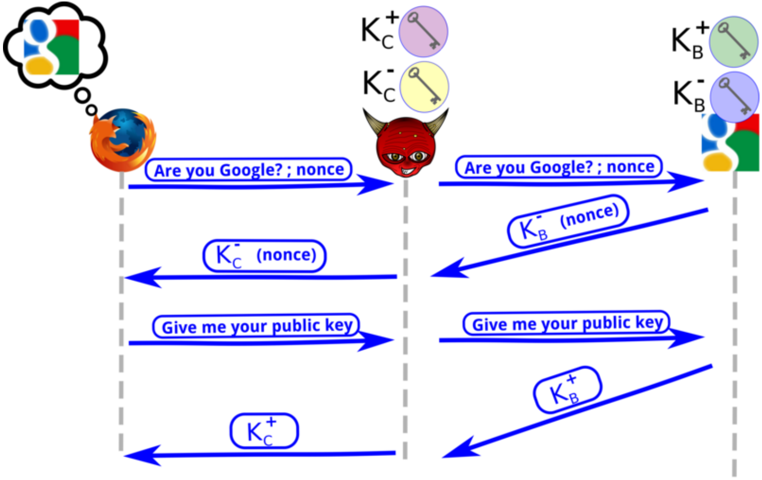
Solution? Using a nonce to ensure *freshness*



Use asymmetric cryptography instead?

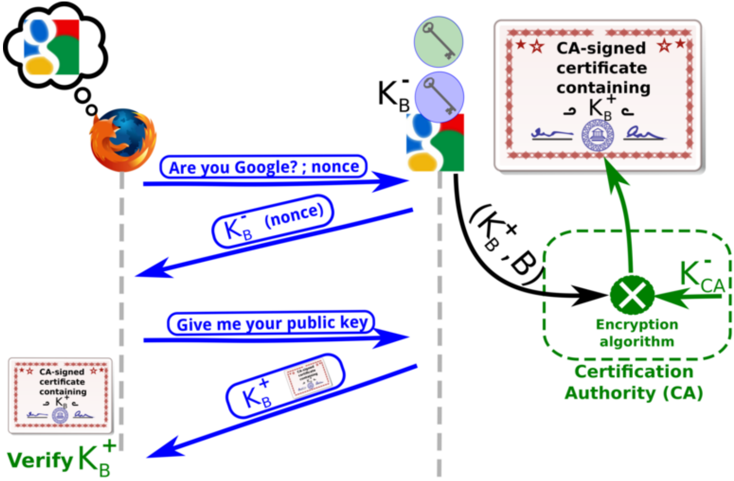


Use asymmetric cryptography instead?



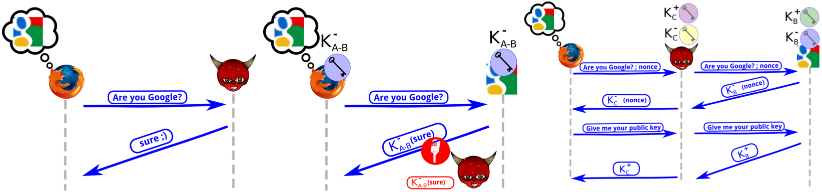
⇒ Vulnerable to Man-in-the-Middle attacks

Solution: Certified Authority



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

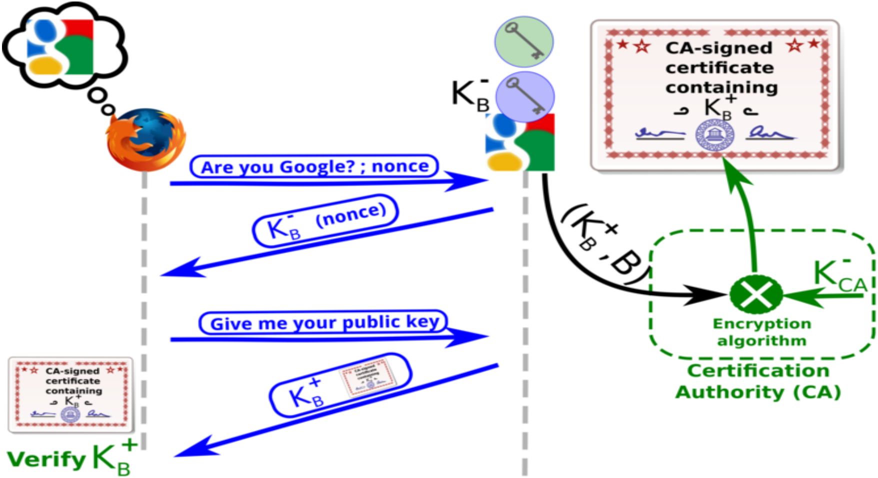
Summary



- 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

Motivation

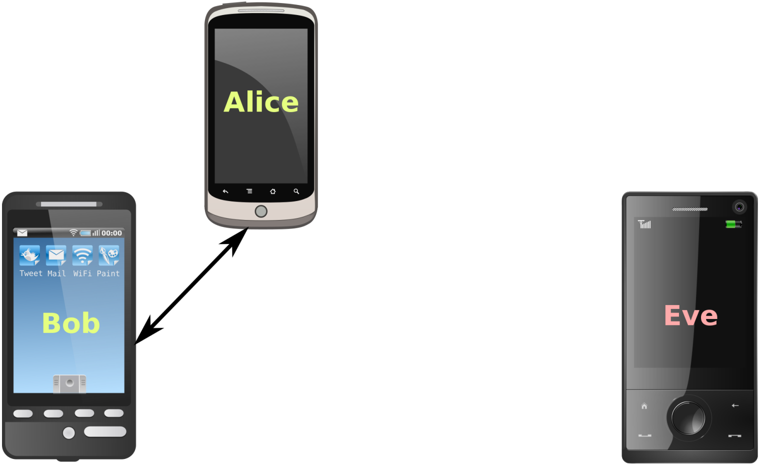
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

Motivation

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

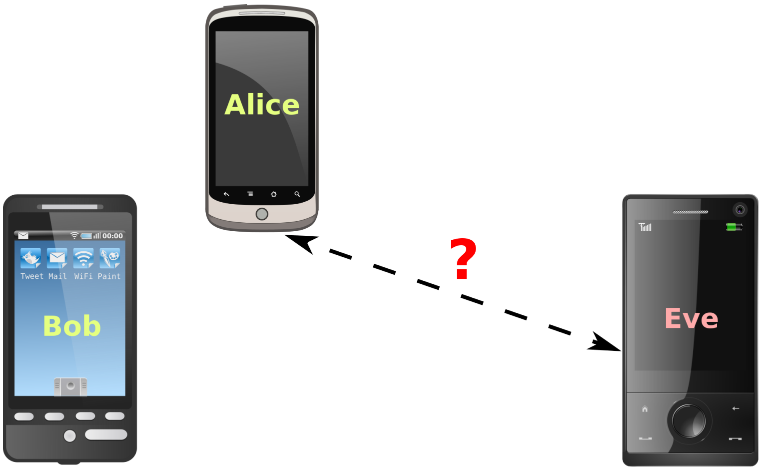
Motivation

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



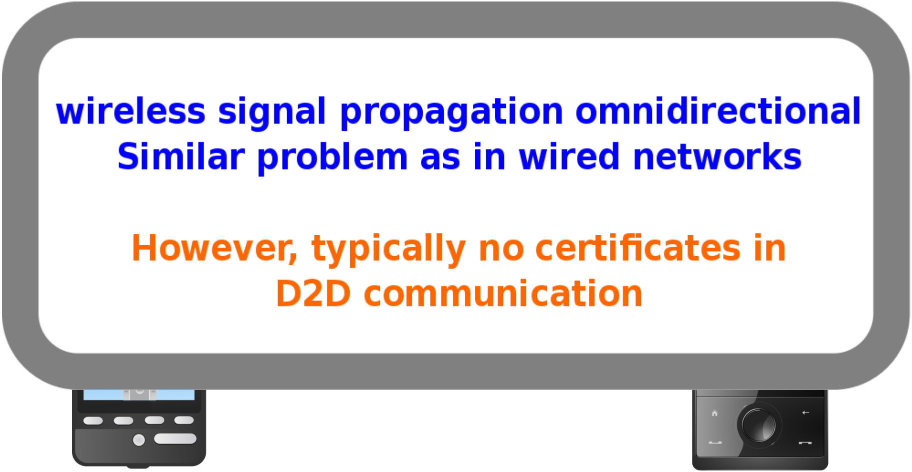
Motivation

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

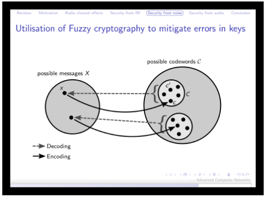


Motivation

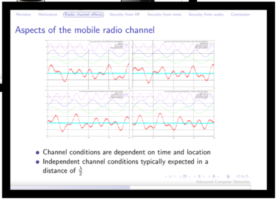
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.



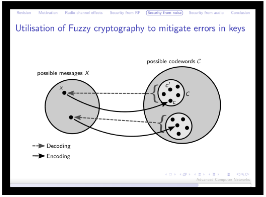

Revision Motivation Radio channel effects Security from RF Security from noise Security from audio Conclusion
Motivation
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.
Alice
Bob
?
Eve
Advanced Computer Networks



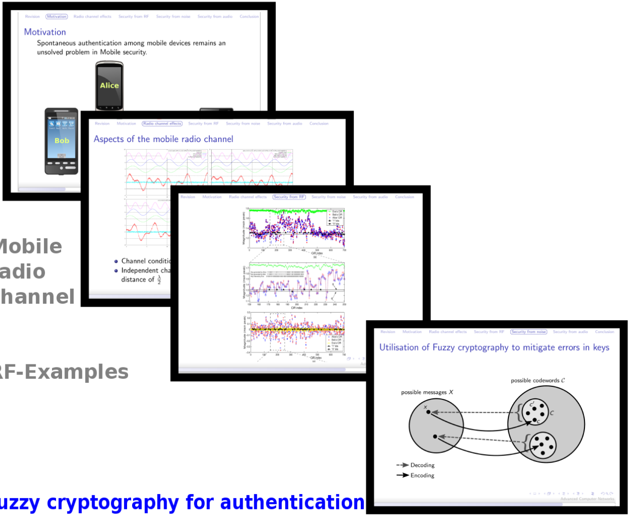
Fuzzy cryptography for authentication



Mobile radio channel



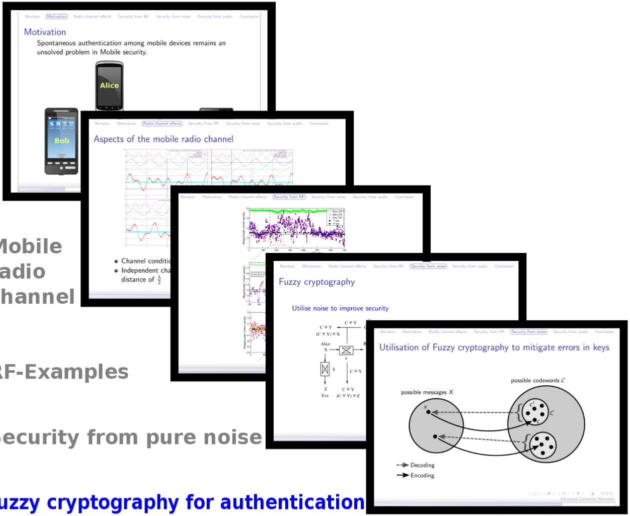
Fuzzy cryptography for authentication



Mobile radio channel

RF-Examples

Fuzzy cryptography for authentication

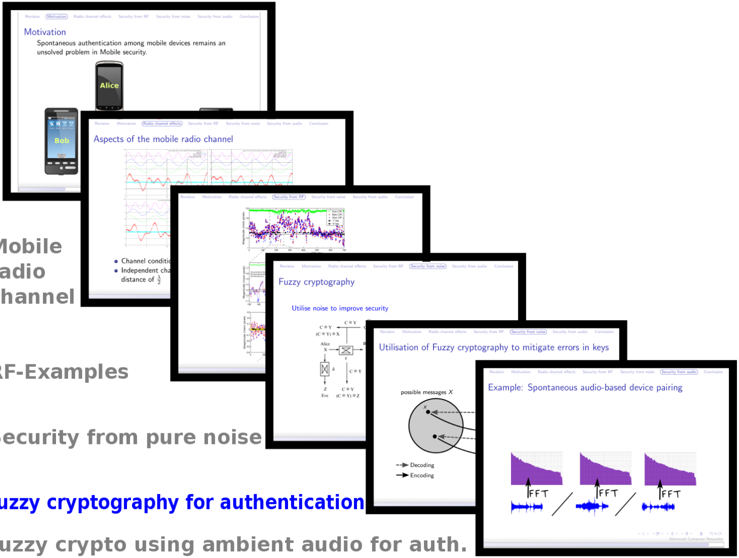


Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication



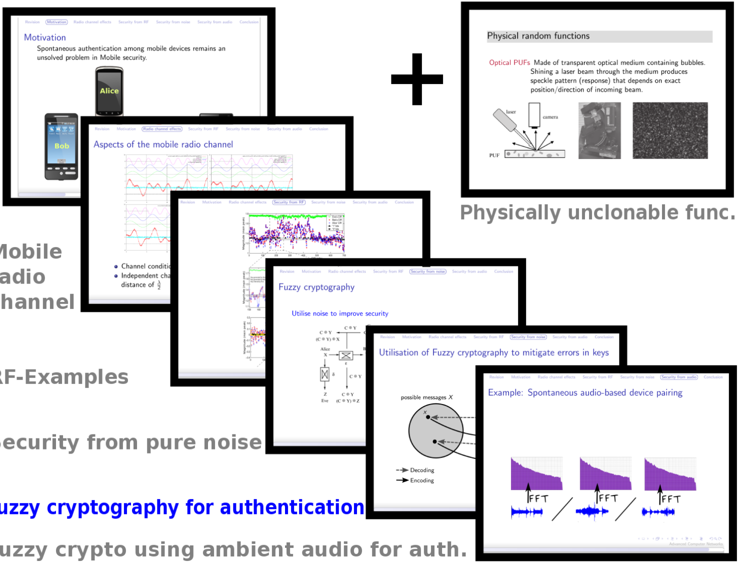
Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

Fuzzy crypto using ambient audio for auth.



Physically unclonable func.

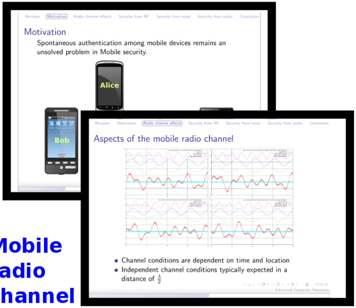
Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

Fuzzy crypto using ambient audio for auth.



Mobile radio channel

Aspects of the mobile radio channel

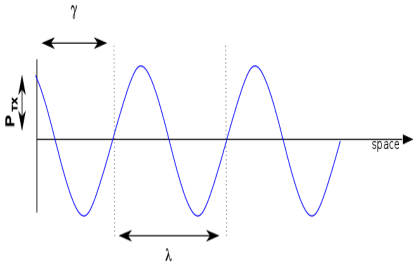
RF transmission

- 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

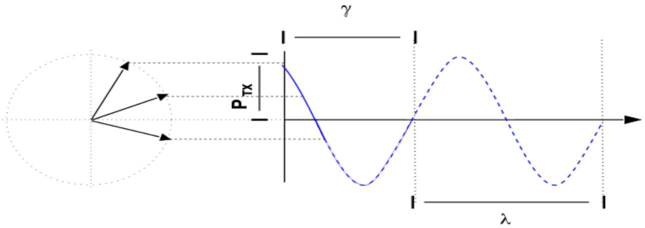
- Transmission power:
  - $P_{TX}[W]$
- Frequency:
  - $f[\frac{1}{sec}]$
- Phase offset:
  - $\gamma[\pi]$
- Wavelength:
  - $\lambda = \frac{c}{f}[m]$



Aspects of the mobile radio channel

RF signal

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

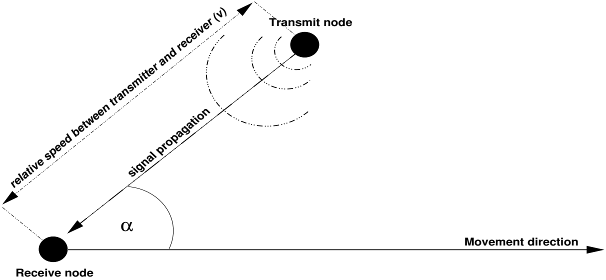


Video: Changes in Audio

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:[3]

$$P_N = -103dBm$$

- Value observed by measurements

[3] 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:

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

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 σ^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

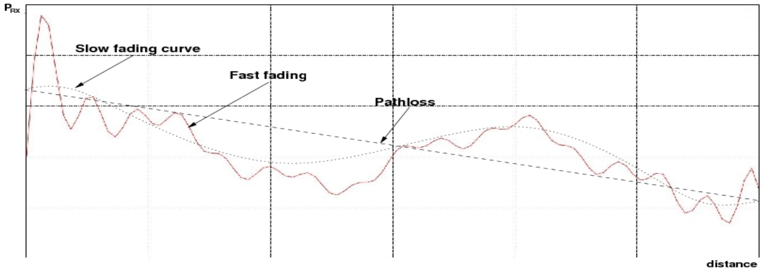
Path-loss

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

- Utilised in outdoor scenarios
  - Direct line of sight
  - No multipath propagation
- d impacts the RSS quadratically
- Other values for the path-loss exponent α 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

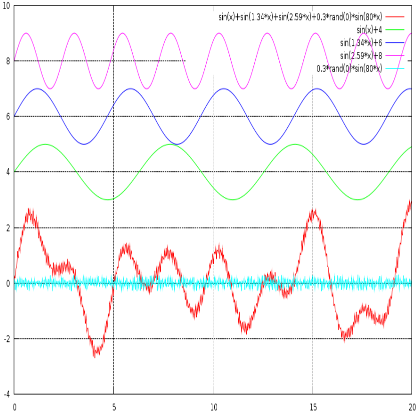
Fast fading

- 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

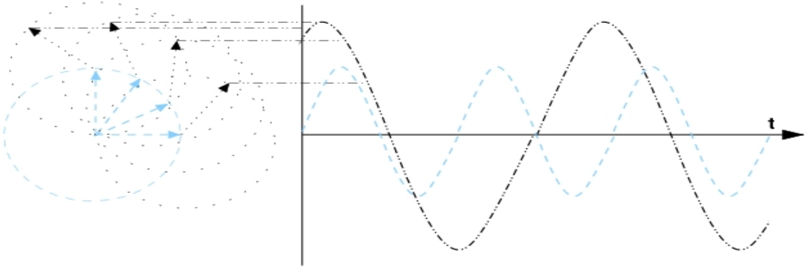
Superimposition of RF signals

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



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

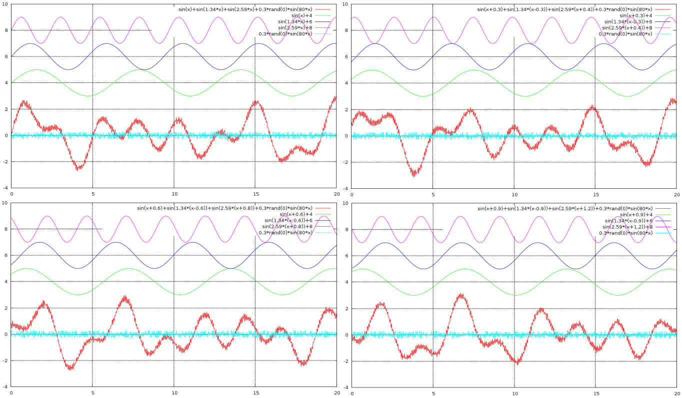
Aspects of the mobile radio channel



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

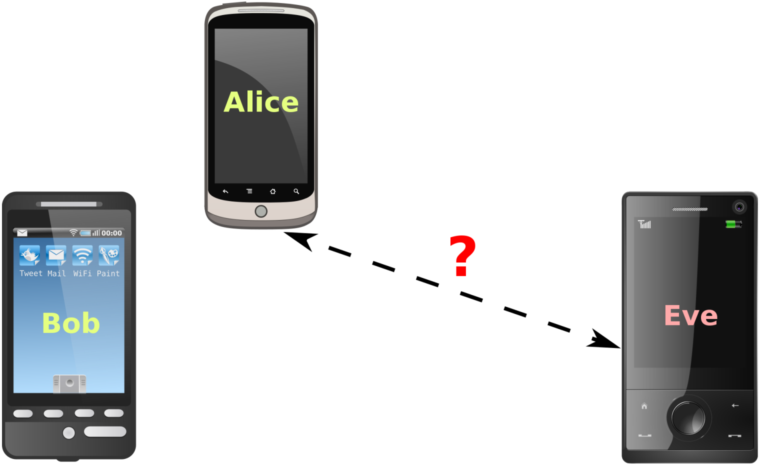
Aspects of the mobile radio channel



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

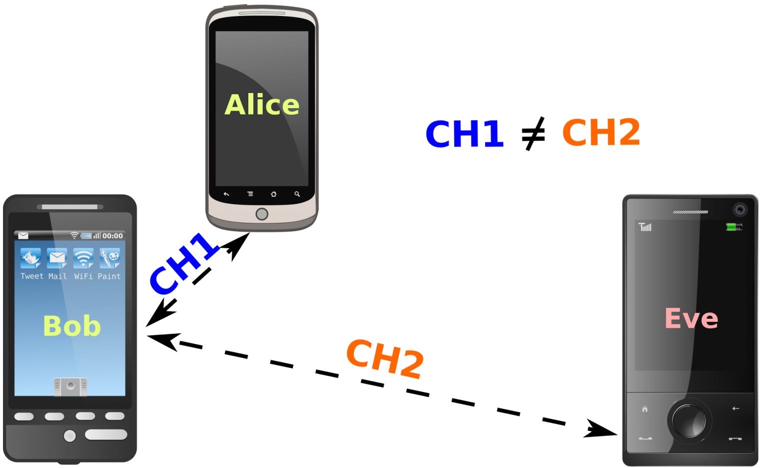
With respect to our Motivation:

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!)

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

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!)

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

General multi-antenna caste:

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

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!)

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

General multi-antenna caste:

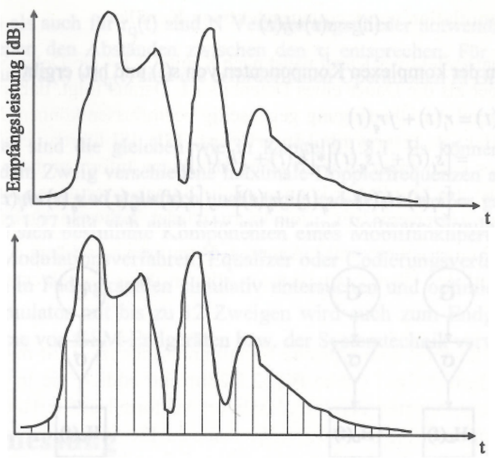
$$\overrightarrow{\zeta^{RX}} = \begin{bmatrix} \zeta_1^{RX} \\ \zeta_2^{RX} \\ \vdots \\ \zeta_M^{RX} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1L} \\ h_{21} & \ddots & & h_{2L} \\ \vdots & & \ddots & \vdots \\ h_{M1} & h_{M2} & \cdots & h_{ML} \end{bmatrix} \begin{bmatrix} \zeta_1^{TX}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

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

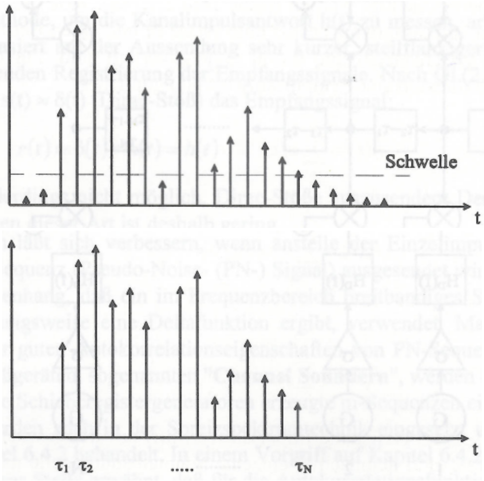
Simulation of frequency selective channels[4]



[4] 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

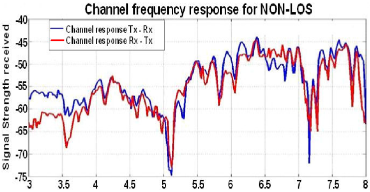
Mobile radio channel

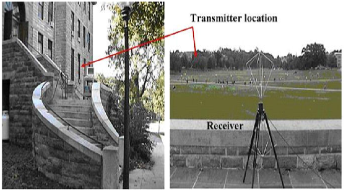
RF-Examples

Security from RF

Secure communication based on deep fades in the SNR[5]

- 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



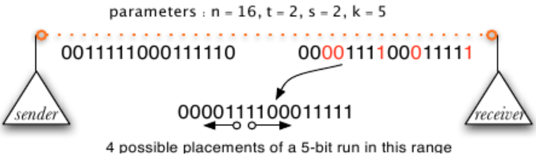


[5] Azimi-Sadjadi, Kiayias, Mercado, Yener, Robust Key Generation from Signal Envelopes in Wireless Networks, CCS, 2007

Security from RF

Secure communication based on deep fades in the SNR

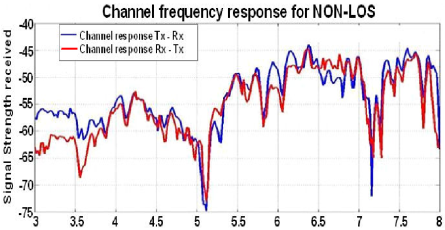
- Key generation
  1. Sender and receiver sample bit sequences
  2. Sender transmits key verification information to receiver
  3. Receiver decides on correct key by scanning through all possible error vectors



Security from RF

Secure communication based on deep fades in the SNR

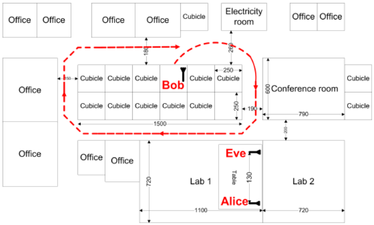
- Discussion
  1. Computationally cheap approach
  2. No special hardware required
  3. Probably uneven distribution of 0 and 1 (Dependent on Channel characteristics and time slot)
  4. Key generation in the presence of noise not optimal

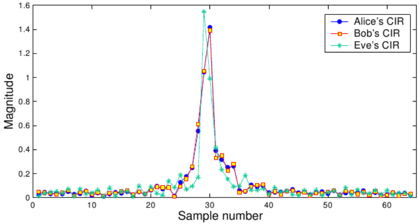


Security from RF

Secure communication based on the CIR[6] [7]

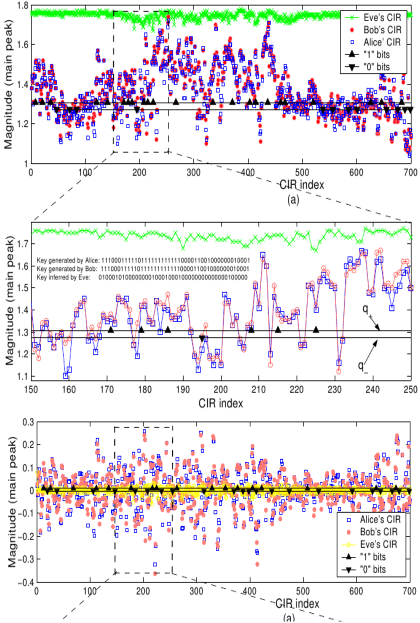
- Utilise Channel impulse response as secure secret
  - Utilise magnitude of CIR pain peak
  - Transformed to binary sequence via Threshold
  - Error correction method required in order to account for noise in the binary sequences

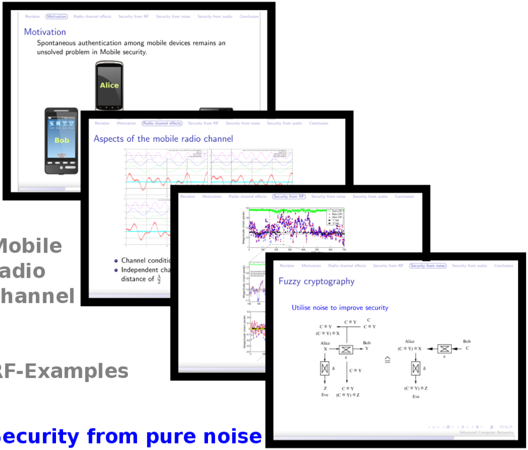




[6] Mathur, Trappe, Mandayam, Ye, Reznik, Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, MobiCom, 2008

[7] Tmar, Hamida, Pierrot, Castelluccia, An adaptive quantisation algorithm for secret key generation using radio channel measurements, NTMS, 2009


Eve's CIR
Bob's CIR
Alice' CIR
"1" bits
"0" bits
Magnitude (main peak)
CIR index
(a)
Key generated by Alice: 1110001111101111111111110000110010000000010001
Key generated by Bob: 1110001111101111111111110000110010000000010001
Key inferred by Eve: 01000101000000000100010001000000000000000100000
q+
q−
Magnitude (main peak)
CIR index
Alice's CIR
Bob's CIR
Eve's CIR
"1" bits
"0" bits
Magnitude (main peak)
CIR index
(a)



Mobile radio channel

RF-Examples

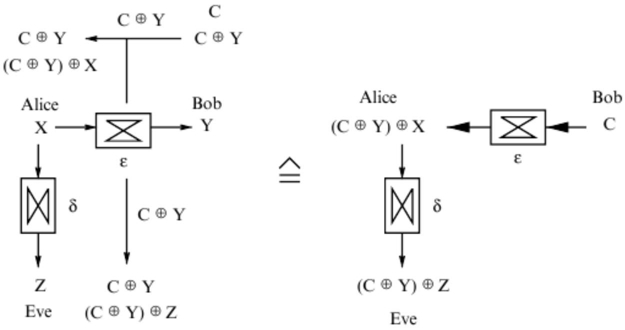
Security from pure noise

Exploit noise for security among devices

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

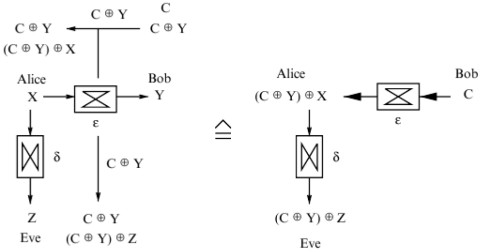
Security from noise

Utilise noise to improve security



Security from noise

Utilise noise to improve security

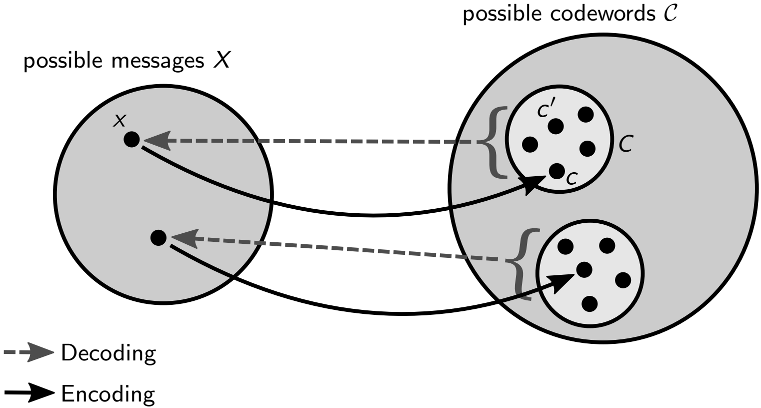


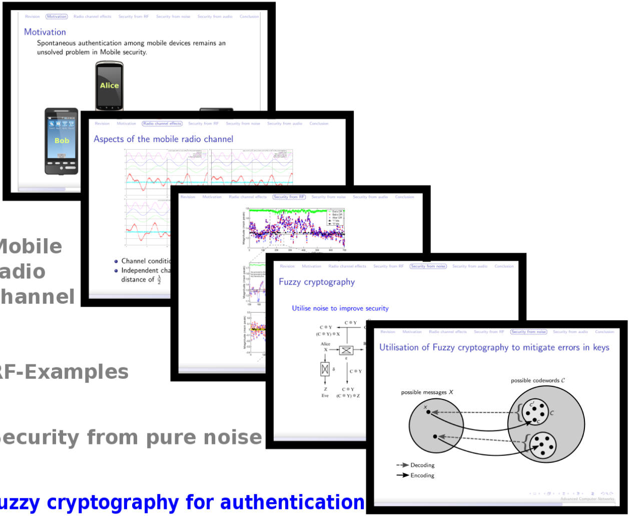
By inverting the direction of communication the noise in Eve's reception is increased above those in Alice's

Establishing of a secure key is possible over binary symmetric channel iff the noise in the reception of Eve's message is higher[8]

[8] Wyner, The wire-tap channel, Bell system Technical Journal, 54:1355-1387,1975

Utilisation of Fuzzy cryptography to mitigate errors in keys





Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

Fuzzy cryptography

Fuzzy Commitment

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

Fuzzy Commitment

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 κ

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

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 (κ', x') such that $\kappa \neq \kappa'$

Hiding Given y alone, it is infeasible to compute κ

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 κ 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

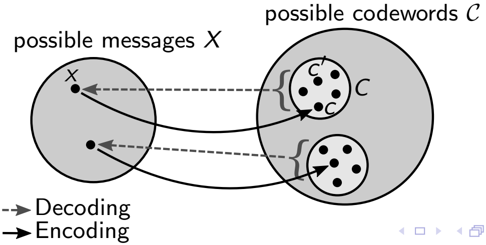
Noise of physical function may be viewed as the difference $c - c'$

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

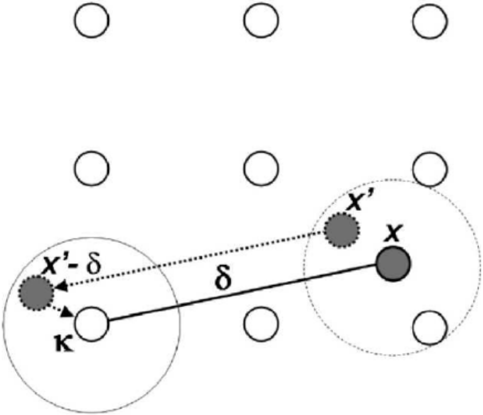
For fuzzy commitment, the secret key κ is chosen uniformly at random from the codeword space C. Then,

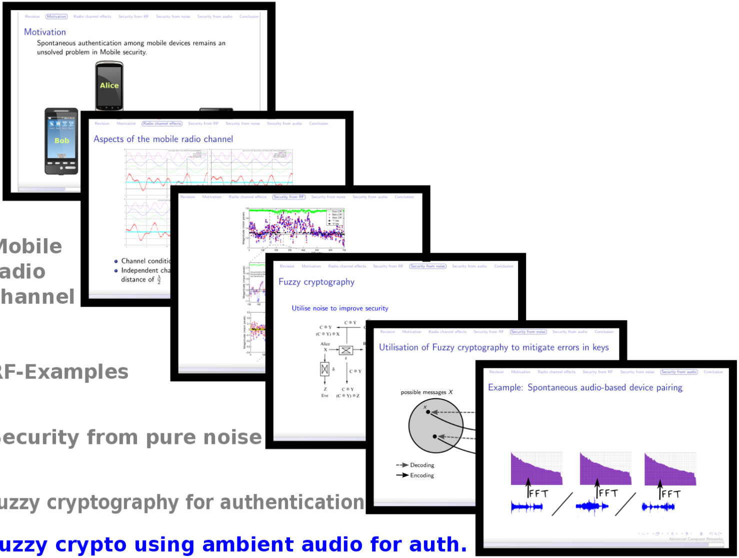
1. An offset $\delta = x - \kappa$ is computed
2. A one-way, collision-resistant hash function is applied to obtain $h(\kappa)$
3. $y = (\delta, h(\kappa))$ is made public
4. $\kappa' = f(x' - \delta)$ is computed
5. It is possible to de-commit y under a witness x' with $Ham(x, x') < \frac{d}{2}$

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

Fuzzy cryptography

Fuzzy Commitment





Mobile radio channel

RF-Examples

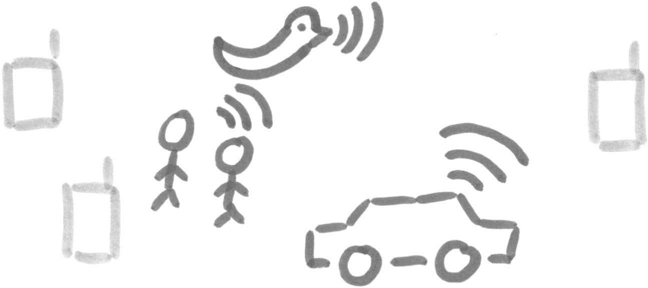
Security from pure noise

Fuzzy cryptography for authentication

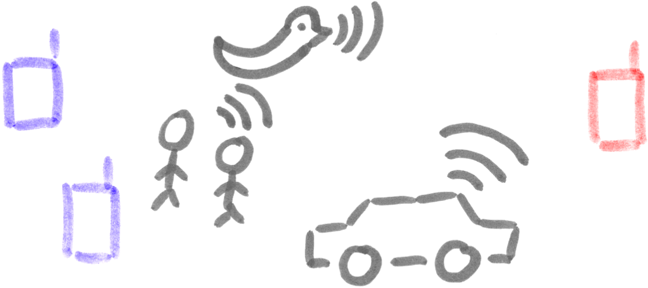
Fuzzy crypto using ambient audio for auth.

Example: Spontaneous audio-based device pairing

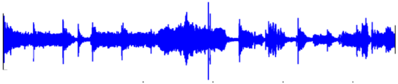
Example: Spontaneous audio-based device pairing



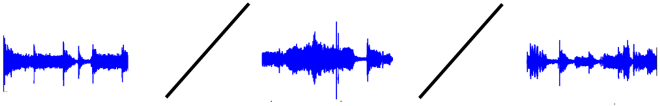
Example: Spontaneous audio-based device pairing



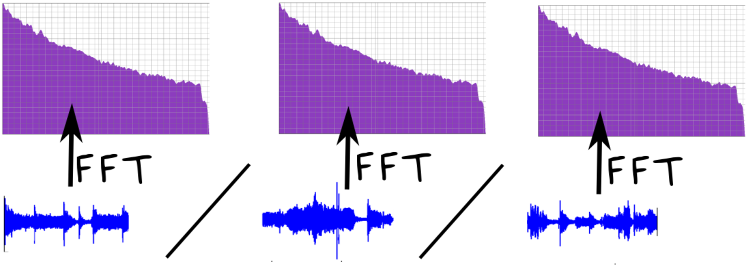
Example: Spontaneous audio-based device pairing



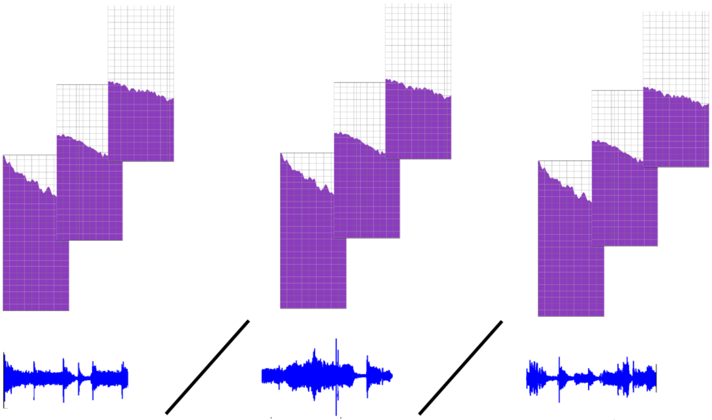
Example: Spontaneous audio-based device pairing



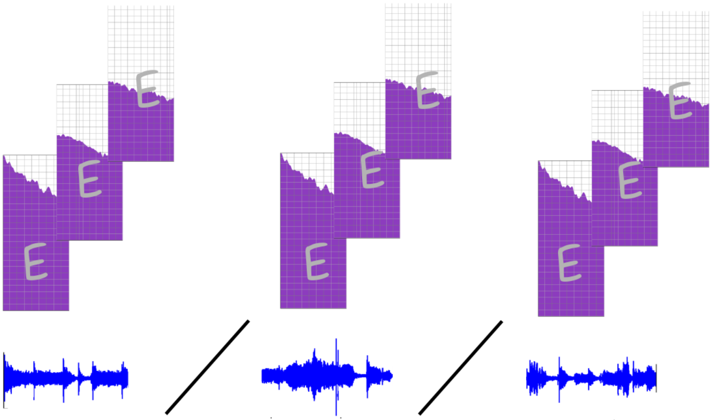
Example: Spontaneous audio-based device pairing



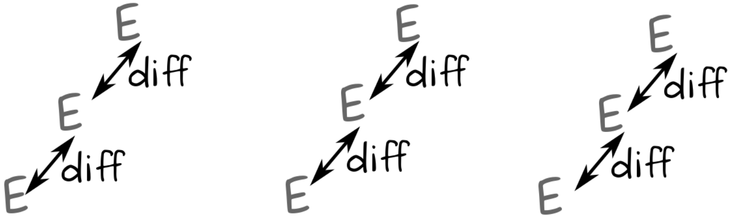
Example: Spontaneous audio-based device pairing



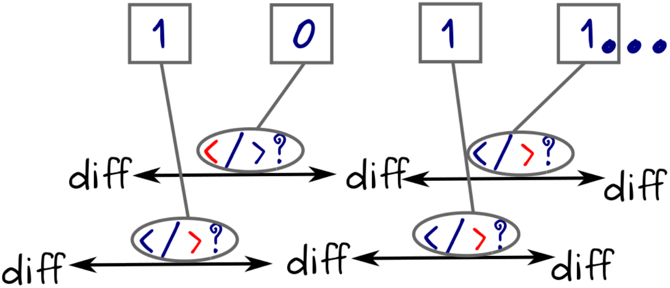
Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



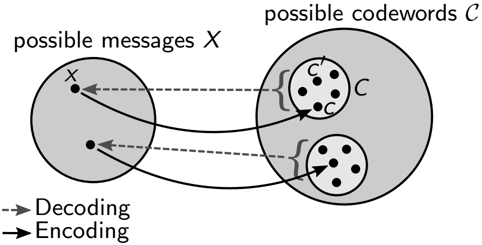
Example: Spontaneous audio-based device pairing



Encryption and decryption in the presence of noise

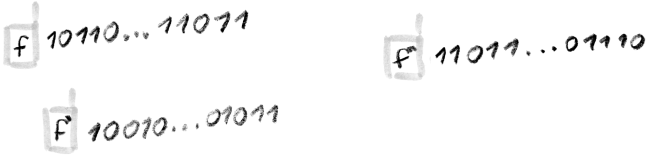
Fuzzy cryptography

- 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

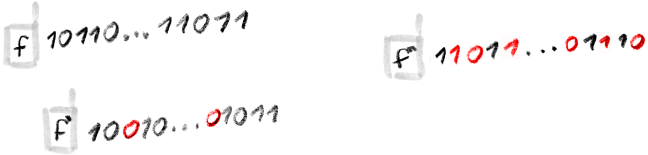


Example: Spontaneous audio-based device pairing

Example: Spontaneous audio-based device pairing

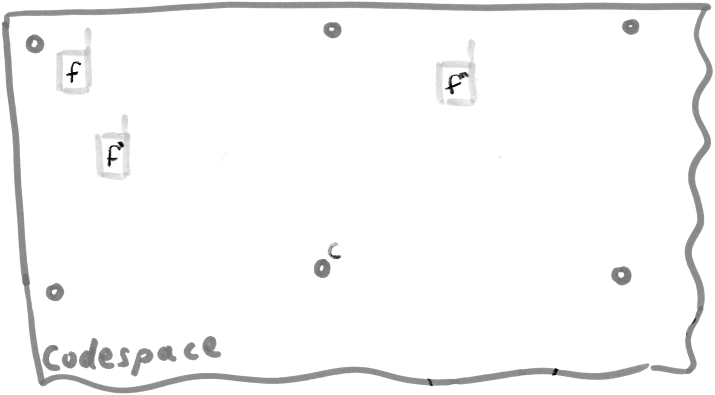


Example: Spontaneous audio-based device pairing

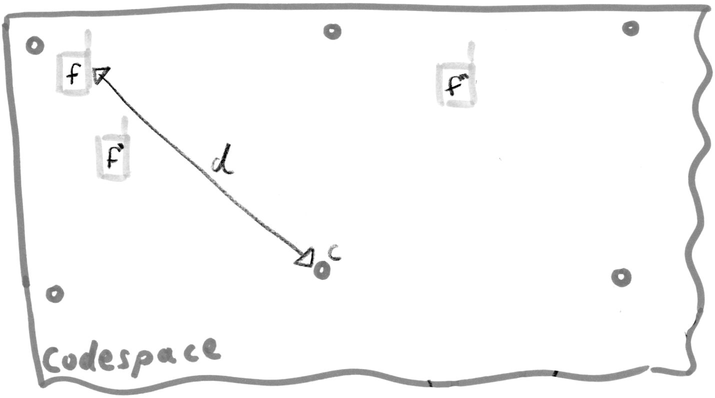


Example: Spontaneous audio-based device pairing

Example: Spontaneous audio-based device pairing

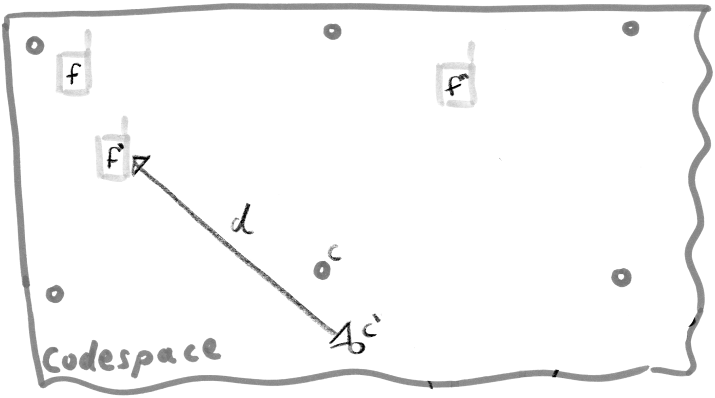


Example: Spontaneous audio-based device pairing

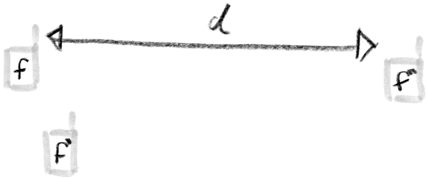


Example: Spontaneous audio-based device pairing

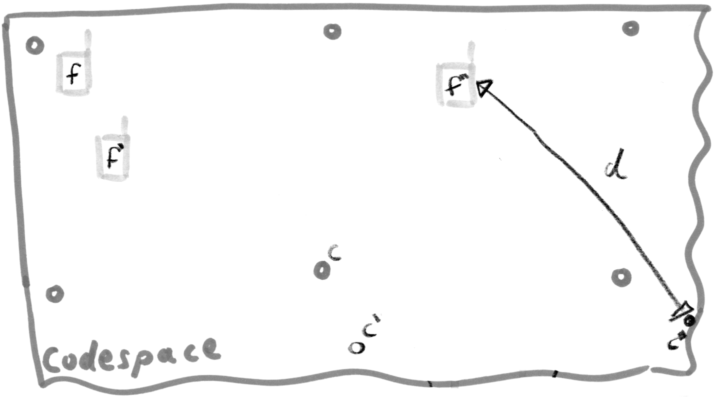
Example: Spontaneous audio-based device pairing



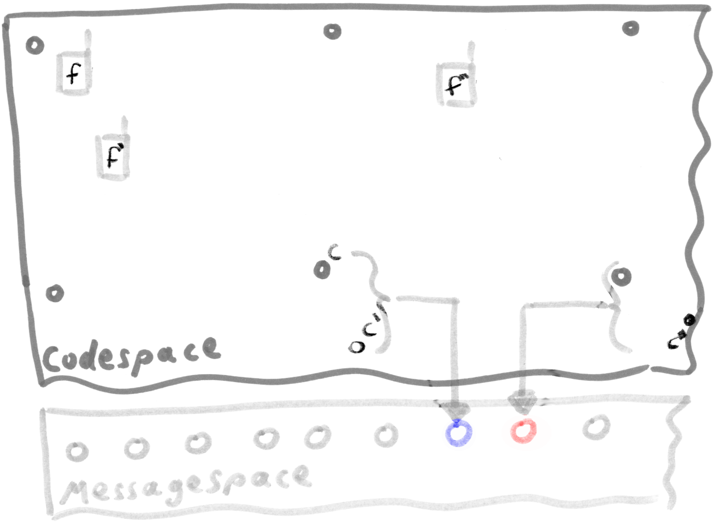
Example: Spontaneous audio-based device pairing



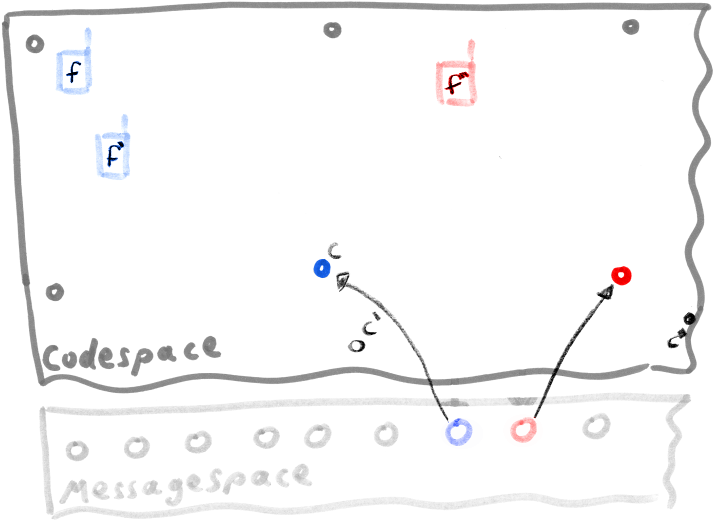
Example: Spontaneous audio-based device pairing

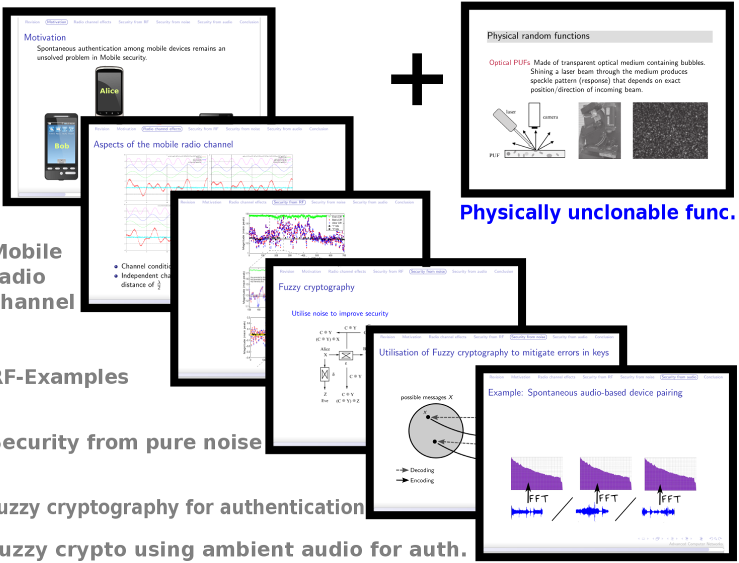


Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing





Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

Fuzzy crypto using ambient audio for auth.

+

Physically unclonable func.

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

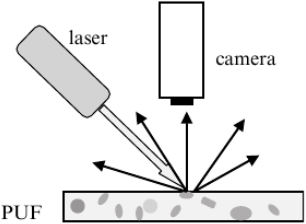
Digital PUFs Simplest kind of PUF. Digital key K is embedded in a tamper-proof package along with some logic that computes

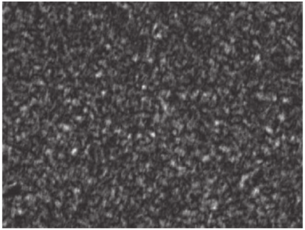
$$Response = RF(K, Challenge)$$

for some random function RF

Physical random functions

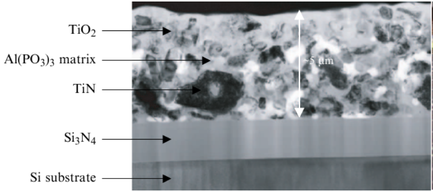
Optical PUFs Made of transparent optical medium containing bubbles. Shining a laser beam through the medium produces speckle pattern (response) that depends on exact position/direction of incoming beam.

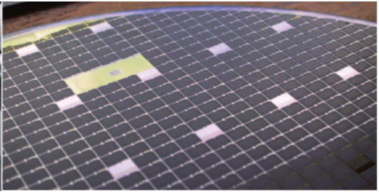




Physical random functions

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

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

This makes PUFs tamper resistant to some extend

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[9]

[9] 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

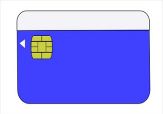
Physical random functions

Standard application: Key-card[10]

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



[10] R. Pappu, Physical One-Way Functions, PhD thesis, MIT, 2001

Outline

Controlled Physical random functions

Definition

Controlled physical random function (CPUF):

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

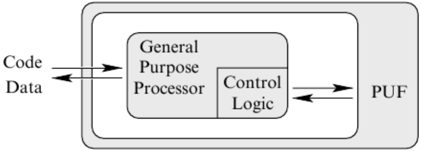
In order to engage in cryptography with a PUF device, a user has to exploit the fact that only he and the device know the response to a specific challenge.

Controlled Physical random functions

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

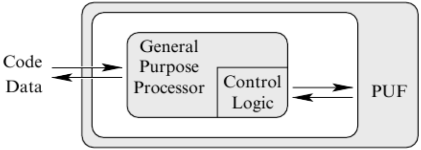
Problem: Adversary can freely query the PUF

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 looses 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:

```
GetAuthenticBroken(Chal){
        my Resp = PUF(Chal);
        // Do some computation, produce result
        return (Result, MAC(Result, Resp));
}
```

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:

```
StealResponse(Chal){
        return (PUF(Chal));
}
```

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

`GetSecret(Chal)=Hash(PHashReg, PUF(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:

```
GetAuthenticBroken(Chal){
        hashblock()({// HB
                // Do some computation, produce result
        });
        my Secret = GetSecret(Chal);
        return (Result, MAC(Result, Secret));
}
```

CPUF API

GetSecret

Alice can now compute `Secret` from `Response` by computing `Hash(PHash(HB),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

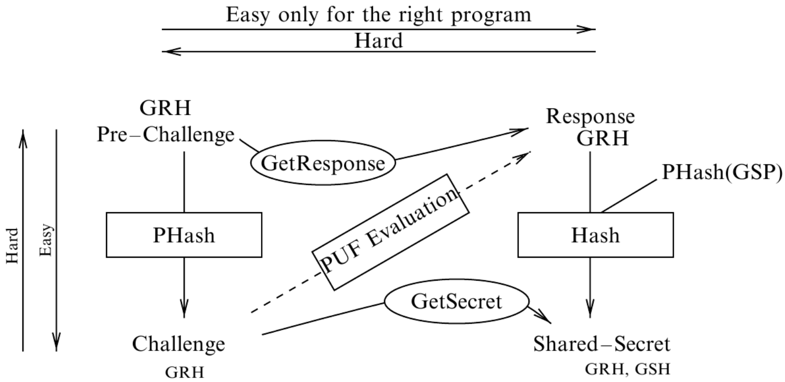
Therefore: Might prefer alternative that not relies on a RNG that much

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

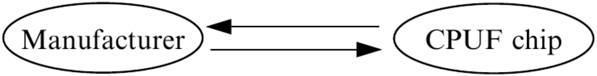
Bootstrapping

1. Pick a pre-challenge `PreChal` at random
2. Execute

```
Bootstrap(PreChal){
        hashblock(PreChal)({
                Return GetResponse();
        });
}
```

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

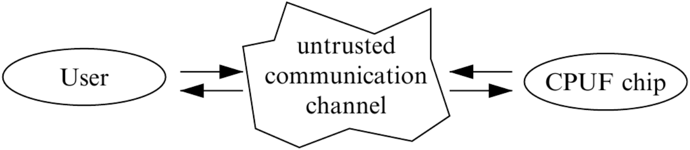
```
Renew(OldChal, PreChal){
        hashblock(OldChal, PreChal)({
                my NewResponse = GetResponse();
                my Secret = GetSecret(OldChal);
                return Encrypt(NewResponse, Secret);//Key:Secret
        });
}
```

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 `OldChal` is only known to the user, the method is secure.



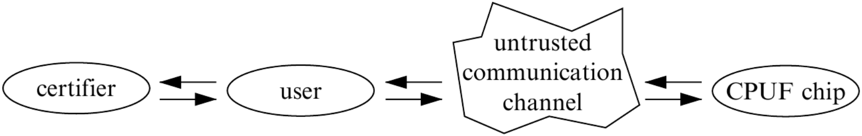
CPUF API

Introduction

Provide user with CRP

Assumption:

Trusted channel between user and certifier



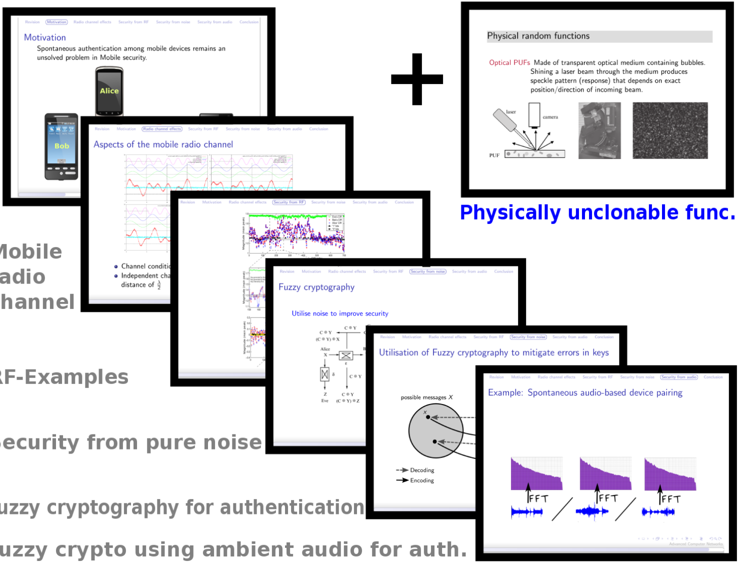
CPUF API

Introduction

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

```
Introduction(OldChal, PubKey, PreChal){
        hashblock(PubKey, PreChal)({
                my NewResponse = GetResponse();
                my Message = PublicEncrypt(NewResponse,
PubKey);
                my Secret' = GetSecret(OldChal);
                Return (Message, MAC(Message, Secret'));
        });
}
```

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



Physically unclonable func.

Mobile radio channel

RF-Examples

Security from pure noise

Fuzzy cryptography for authentication

Fuzzy crypto using ambient audio for auth.

Questions?

Stephan Sigg
stephan.sigg@cs.uni-goettingen.de

Literature

- C.M. Bishop: Pattern recognition and machine learning, Springer, 2007.
- P. Tulys, 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.