Advanced Computer Networks

Stephan Sigg

Georg-August-University Goettingen, Computer Networks

26.06.2014

Outline

Motivation

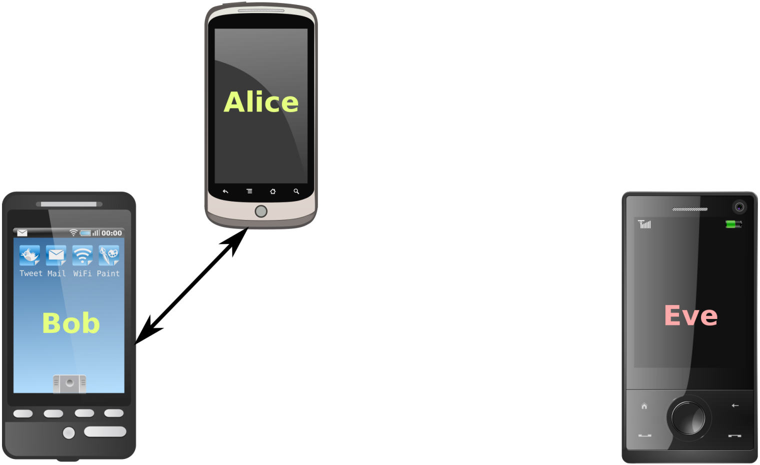
Spontaneous authentication among mobile devices remains an unsolved problem in Mobile security.

Motivation

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

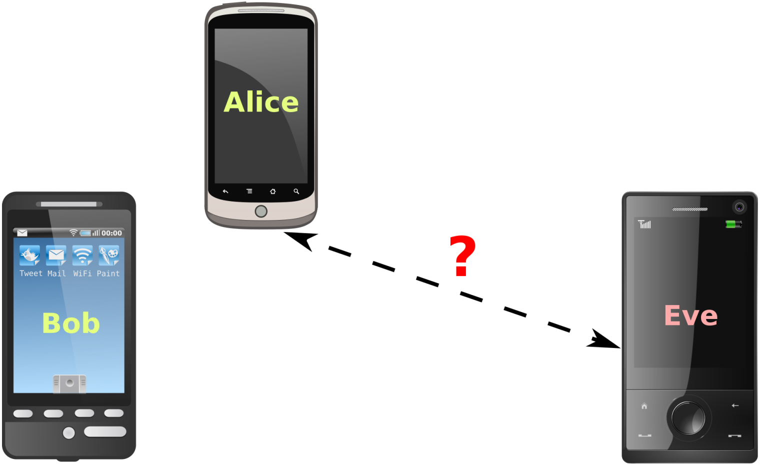
Motivation

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.



This lecture

- Effects of the radio channel
- Utilising RF information for authentication and security
- Fuzzy cryptography

Outline

Aspects of the mobile radio channel

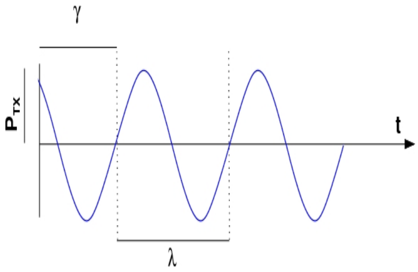
RF transmission

- 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

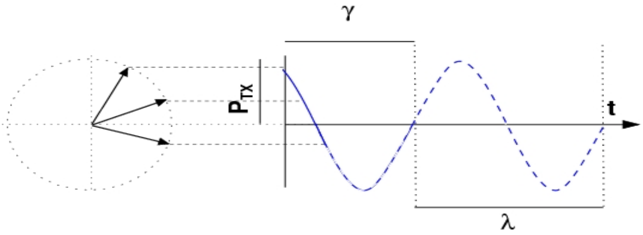
- Transmission power:
  - $P_{TX}[W]$
- Frequency:
  - $f[\frac{1}{sec}]$
- Phase offset:
  - $\gamma[\pi]$
- Wavelength:
  - $\lambda = \frac{c}{f}[m]$



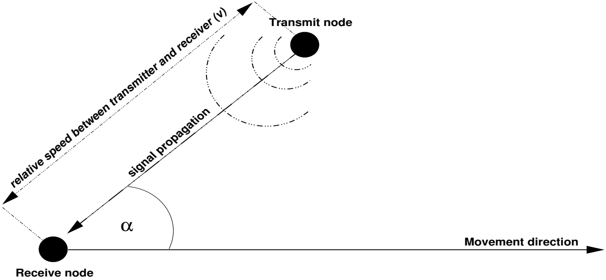
Aspects of the mobile radio channel

RF signal

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



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:[1]

$$P_N = -103dBm$$

- Value observed by measurements

[1] 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

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

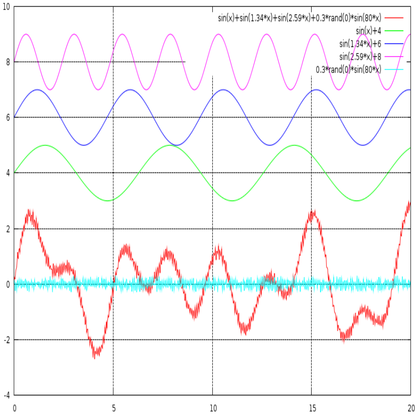
- Utilised in outdoor scenarios
  - Direct line of sight
  - No multipath propagation
- d impacts the RSS quadratically
- Other values for the path-loss exponent α possible.
- Path-loss:

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

Aspects of the mobile radio channel

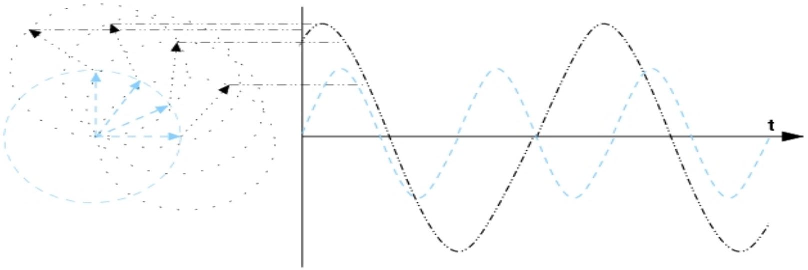
Superimposition of RF signals

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



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

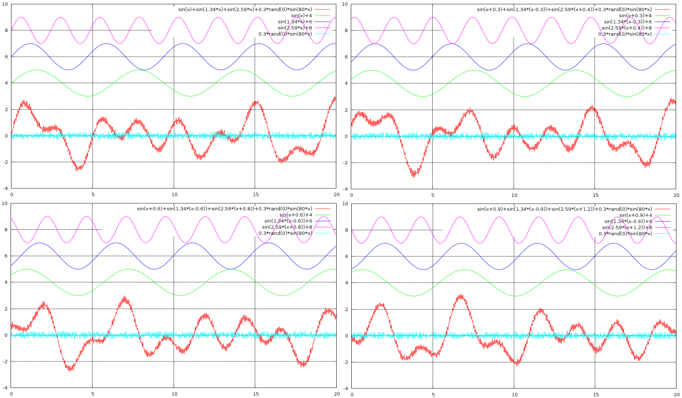
Aspects of the mobile radio channel



Superimposition of RF signals

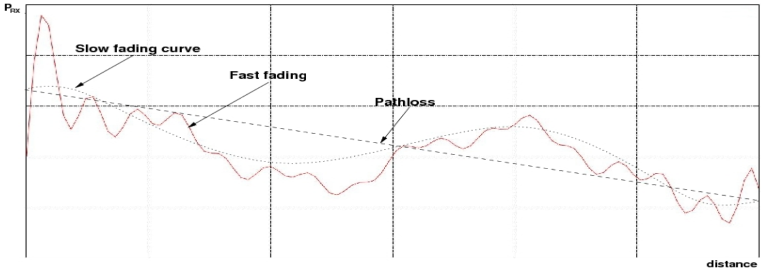
- At a receiver, all incoming signals add up to one superimposed sum signal
- Constructive and destructive interference
- Normally: Heavily distorted sum signal

Aspects of the mobile radio channel



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

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

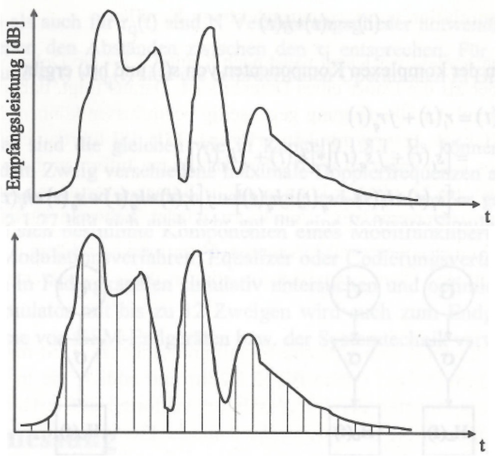
Aspects of the mobile radio channel

Simulation of frequency selective channels

- A common approach is to estimate the channel impulse response during a known training bit-sequence
- When the channel impulse response is known, signal distortions can be corrected
  - When the time axis is divided in discrete parts
  - We can derive discrete impulses for the energy in each of these parts

Aspects of the mobile radio channel

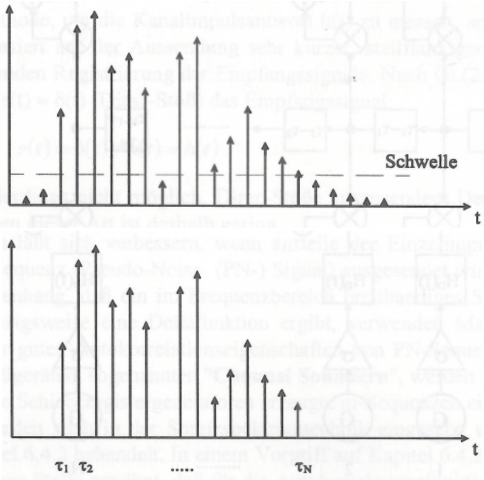
Simulation of frequency selective channels[2]



[2] 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

- The easiest approach to estimate $h(t)$ works in the time domain
- Based on sending very short impulses
- And registering the received signals
- The approach can be improved by utilising a pseudo-noise sequence instead of single identical impulses
- The inverse of the estimated impulse response is correlated $\overline{h(t)^{-1}}$ with the received signal:

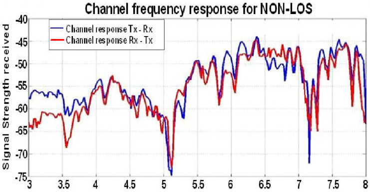
$$r(t) \cdot \overline{h(t)^{-1}} = s(t) \cdot h(t) \cdot \overline{h(t)^{-1}} \approx s(t)$$

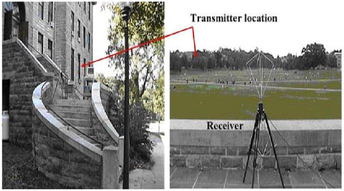
Outline

Features of the RF channel

Secure communication based on deep fades in the SNR[3]

- 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



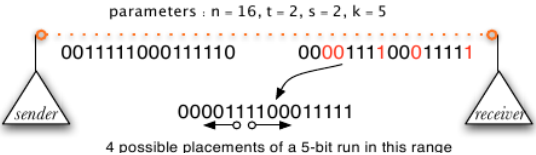


[3] Azimi-Sadjadi, Kiayias, Mercado, Yener, Robust Key Generation from Signal Envelopes in Wireless Networks, CCS, 2007

Features of the RF channel

Secure communication based on deep fades in the SNR

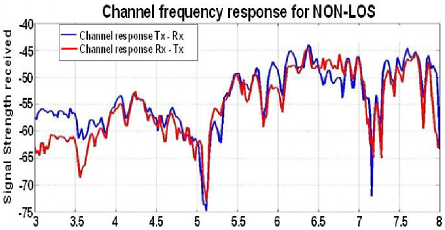
- Key generation
  1. Sender and receiver sample bit sequences
  2. Sender transmits key verification information to receiver
  3. Receiver decides on correct key by scanning through all possible error vectors



Features of the RF channel

Secure communication based on deep fades in the SNR

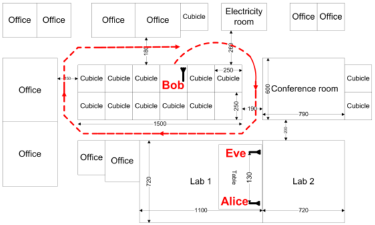
- Discussion
  1. Computationally cheap approach
  2. No special hardware required
  3. Probably uneven distribution of 0 and 1 (Dependent on Channel characteristics and time slot)
  4. Key generation in the presence of noise not optimal

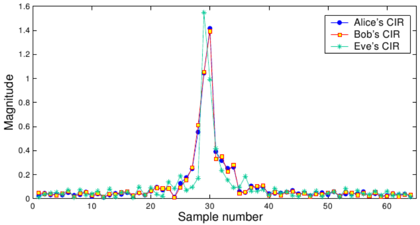


Features of the RF channel

Secure communication based on the CIR[4] [5]

- 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



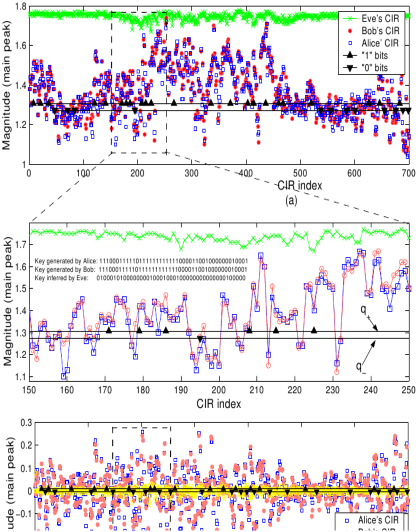


[4] Mathur, Trappe, Mandayam, Ye, Reznik, Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, MobiCom, 2008

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

Features of the RF channel

Secure communication based on the CIR



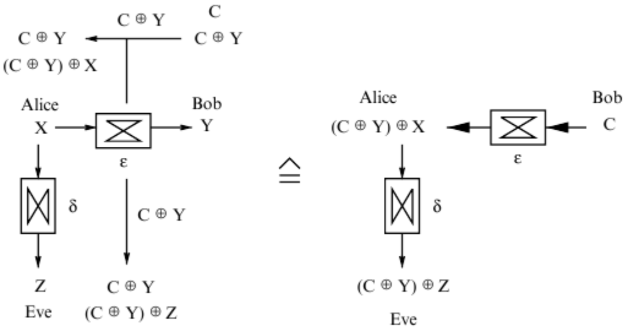
Outline

Exploit noise for security among devices

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

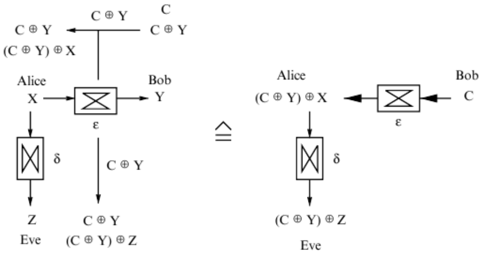
Fuzzy cryptography

Utilise noise to improve security



Fuzzy cryptography

Utilise noise to improve security

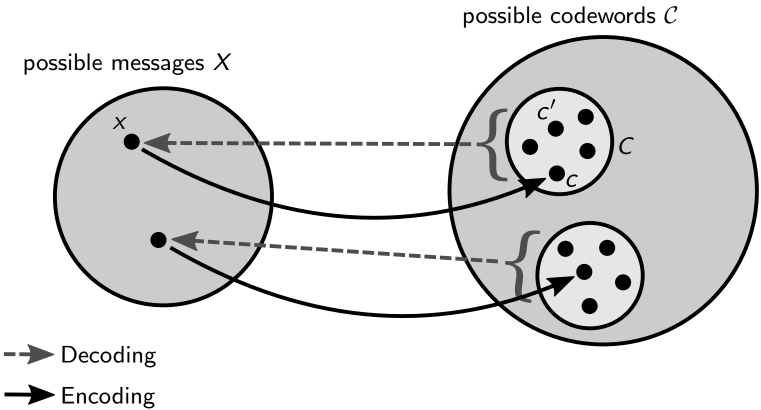


By inverting the direction of communication the noise in Eve's reception is increased above those in Alice's

Establishing of a secure key is possible over binary symmetric channel iff the noise in the reception of Eve's message is higher[6]

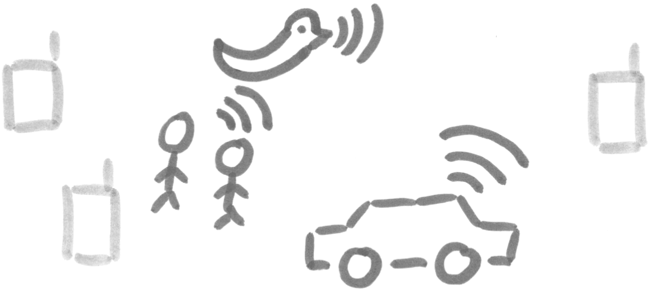
[6] Wyner, The wire-tap channel, Bell system Technical Journal, 54:1355-1387,1975

Utilisation of Fuzzy cryptography to mitigate errors in keys

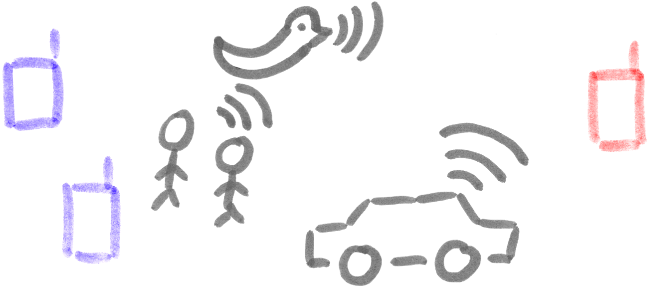


Example: Spontaneous audio-based device pairing

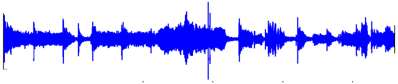
Example: Spontaneous audio-based device pairing



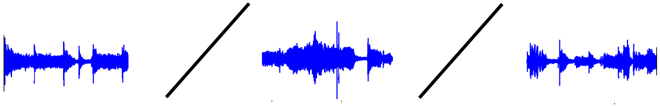
Example: Spontaneous audio-based device pairing



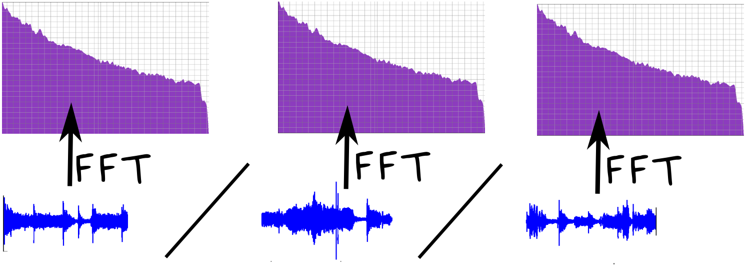
Example: Spontaneous audio-based device pairing



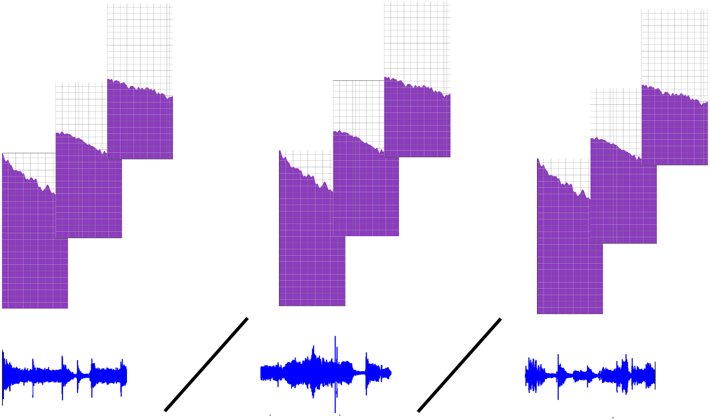
Example: Spontaneous audio-based device pairing



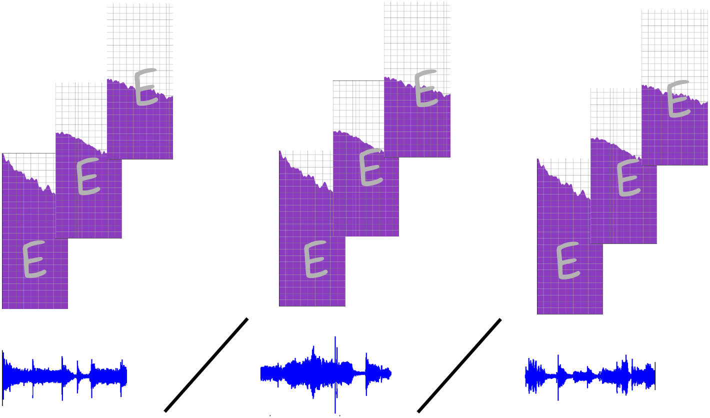
Example: Spontaneous audio-based device pairing



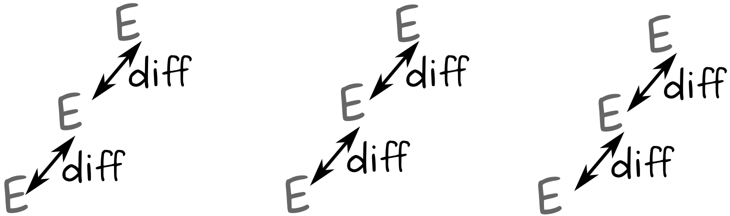
Example: Spontaneous audio-based device pairing



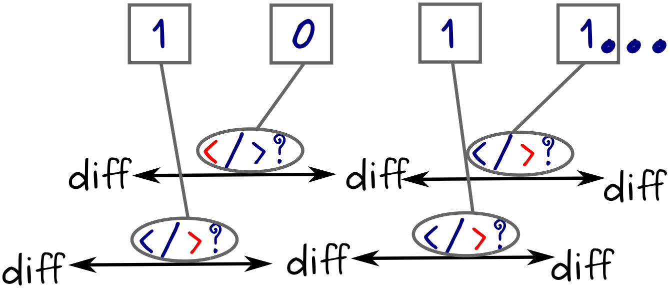
Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



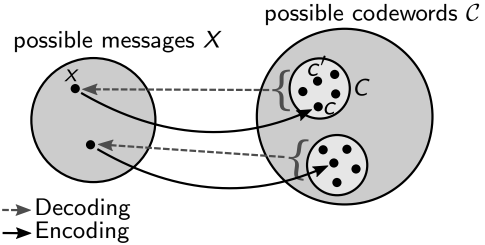
Example: Spontaneous audio-based device pairing



Encryption and decryption in the presence of noise

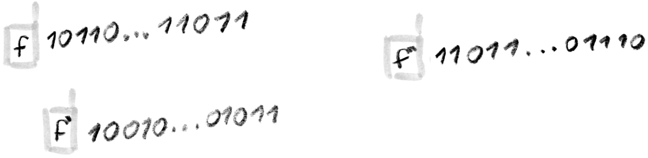
Fuzzy cryptography

- 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

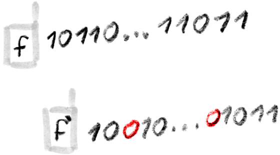


Example: Spontaneous audio-based device pairing

Example: Spontaneous audio-based device pairing

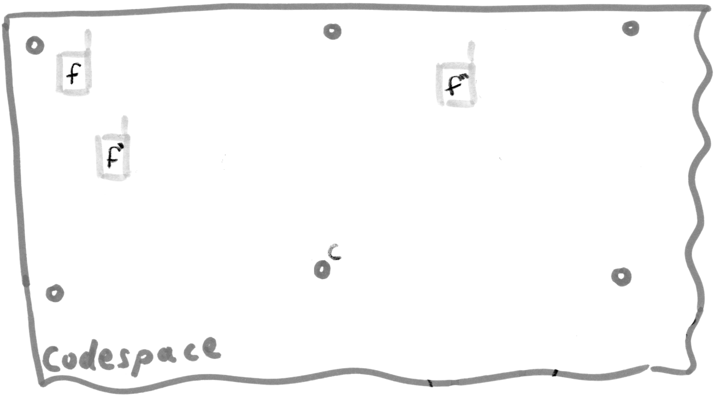


Example: Spontaneous audio-based device pairing

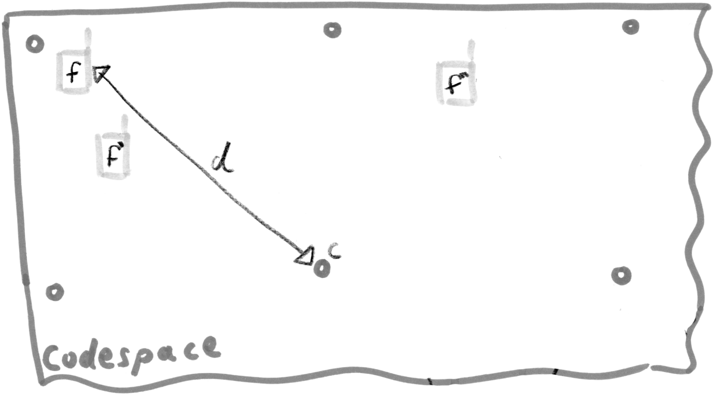


Example: Spontaneous audio-based device pairing

Example: Spontaneous audio-based device pairing

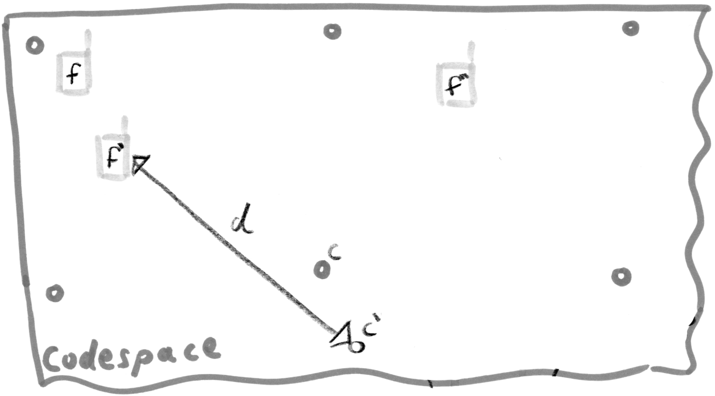


Example: Spontaneous audio-based device pairing

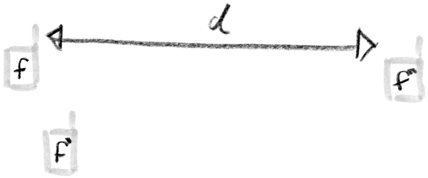


Example: Spontaneous audio-based device pairing

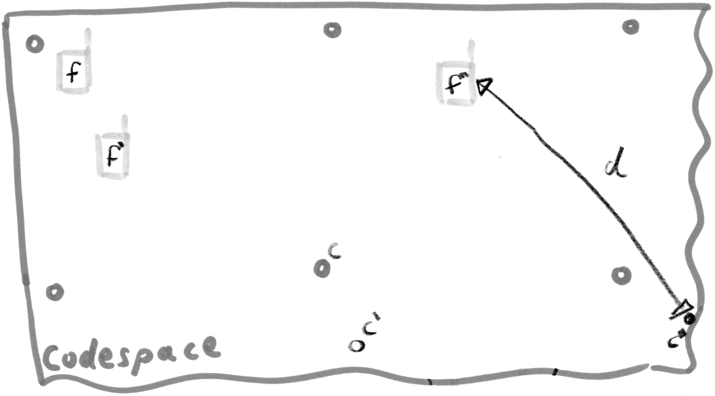
Example: Spontaneous audio-based device pairing



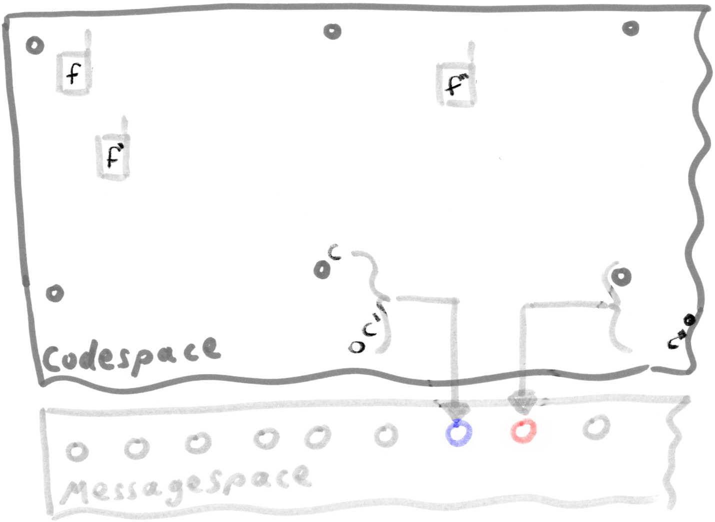
Example: Spontaneous audio-based device pairing



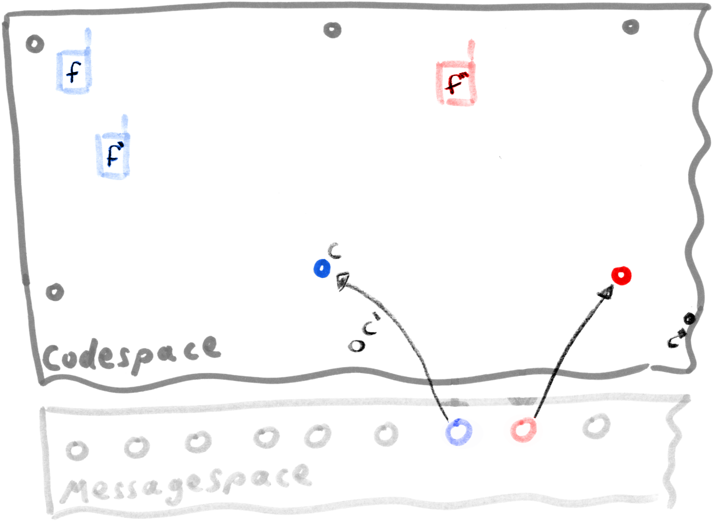
Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



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

Fuzzy 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

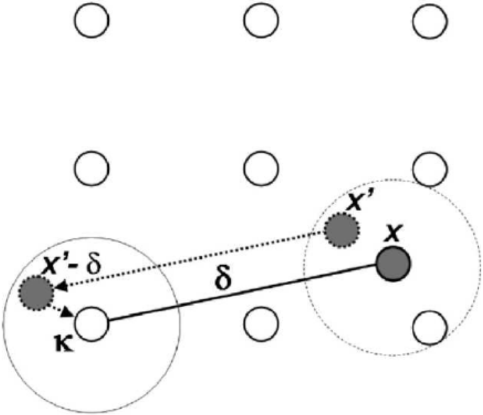
For fuzzy commitment, the secret key κ is chosen uniformly at random from the codeword space C. Then,

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



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.