Technische
Universität
Braunschweig

PINtext: A framework for secure communication based on context

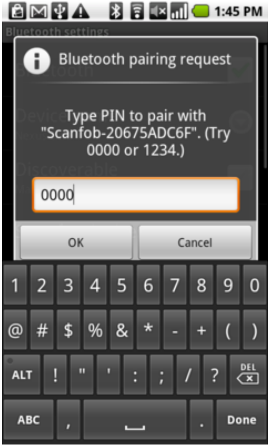
MobiQuitous2011

Stephan Sigg, Dominik Schürmann, Yusheng Ji

December 8, 2011

Motivation

Bluetooth



Motivation

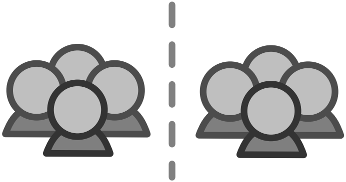
Our solution

- Unobtrusive approach:
  Secure pairing based on context information
- In our study: Context information $\widehat{=}$ audible background noise

Trust in real life

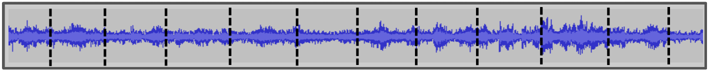
- Frequently we trust people that share our context
- Users decide based on physical context if it is a trustworthy situation
- Trust is often based on “physical limits”

$\Rightarrow$ Use spatially limited context information ($\widehat{=}$ background noise) for unobtrusive security



Audio fingerprinting (J. Haitsma and T. Kalker, 2002)

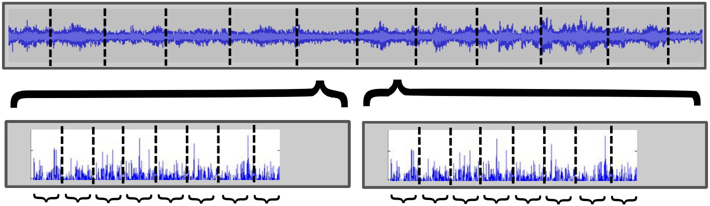
Framing



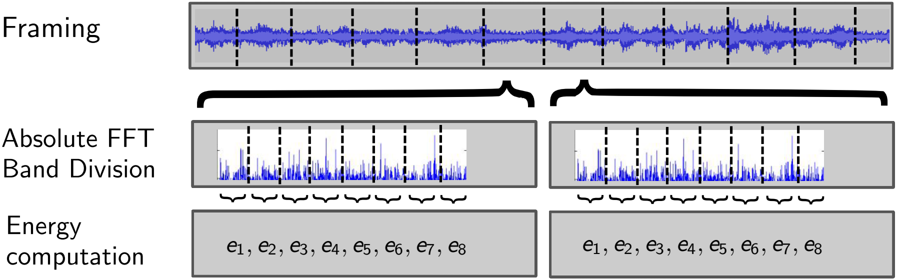
Audio fingerprinting (J. Haitsma and T. Kalker, 2002)

Framing

Absolute FFT
Band Division



Audio fingerprinting (J. Haitsma and T. Kalker, 2002)



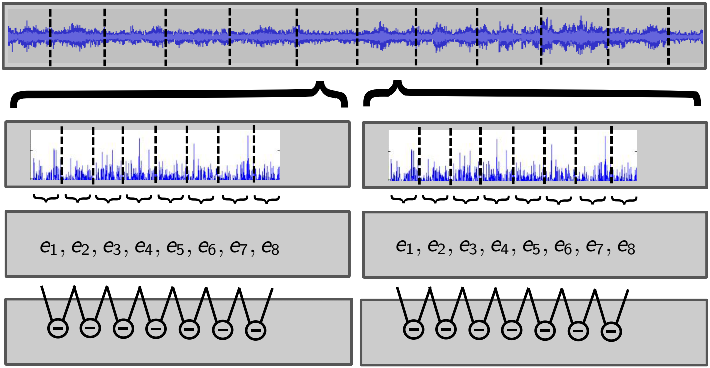
Audio fingerprinting (J. Haitsma and T. Kalker, 2002)

Framing

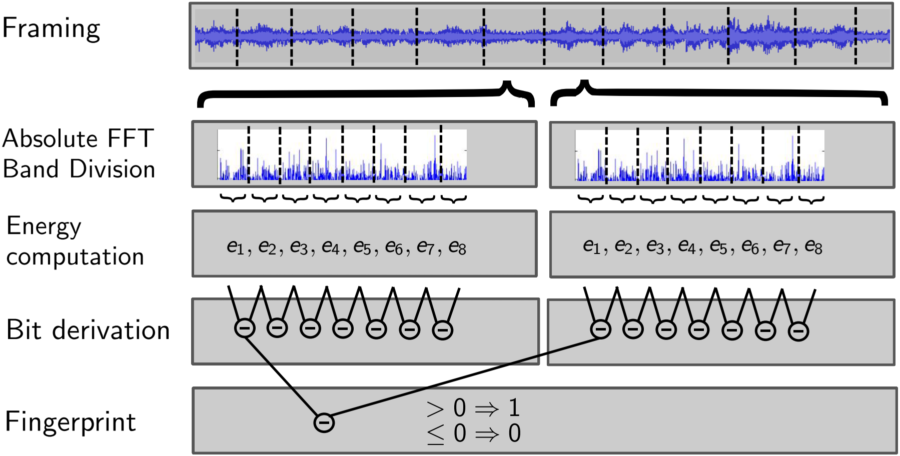
Absolute FFT Band Division

Energy computation

Bit derivation



Audio fingerprinting (J. Haitsma and T. Kalker, 2002)



Audio fingerprints as context information

How to use audio fingerprints for secure pairing?

- Fingerprints are not exactly equal

  ... but similarities are visible!
- Don't compare fingerprints by transmitting themselves
- Threshold of minimum percentage of identical bits for successful pairing is needed

  ⇒ Fuzzy Cryptography

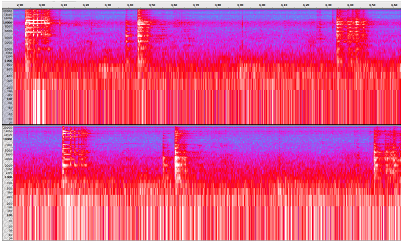


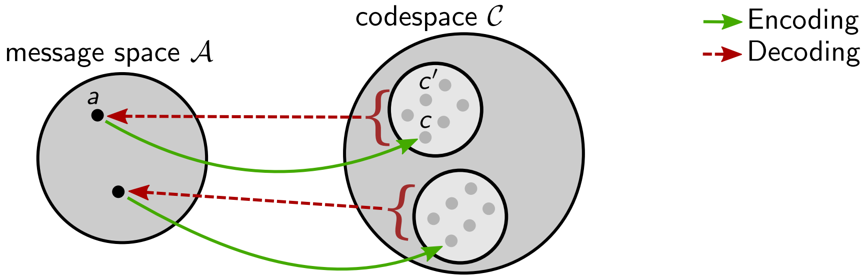
Figure: Spectograms of audio recordings on two devices in physical proximity

Fuzzy Cryptography

Error-correcting codes

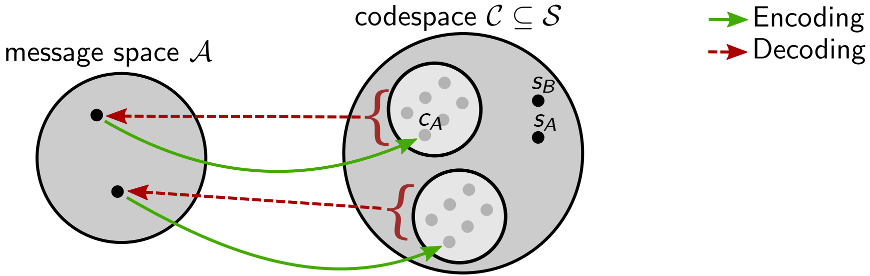
Encoding Adds redundancies to given word to produce codeword

Decoding Many similar codewords are decoded to one definite word



Fuzzy Cryptography[1]

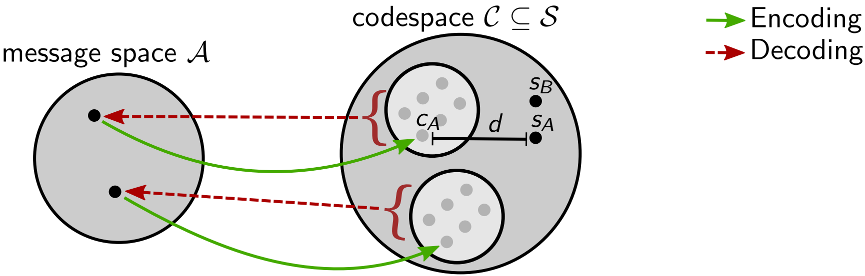
1. Device A and B generate their audio fingerprints $s_A \in \mathcal{S}$ ans $s_B \in \mathcal{S}$
2. Device A chooses a definite codeword $c_A \in \mathcal{C}$ randomly



[1] based on "A Fuzzy Commitment Scheme" (A. Juels and M. Wattenberg, 1999)

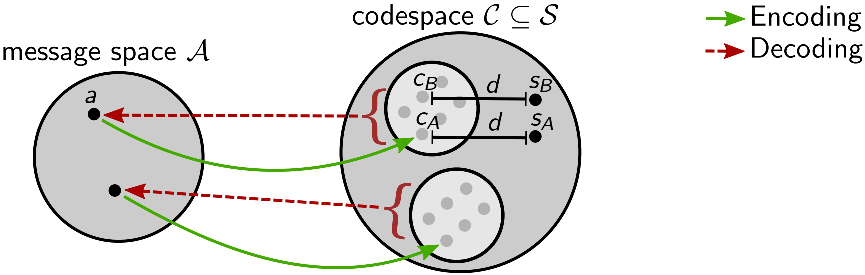
Fuzzy Cryptography

3. Device A calculates $d = m(s_A, c_A)$ using a distance metric $m : \mathcal{S} \times \mathcal{S} \to \mathbb{R}$
4. d is send from A to B over air

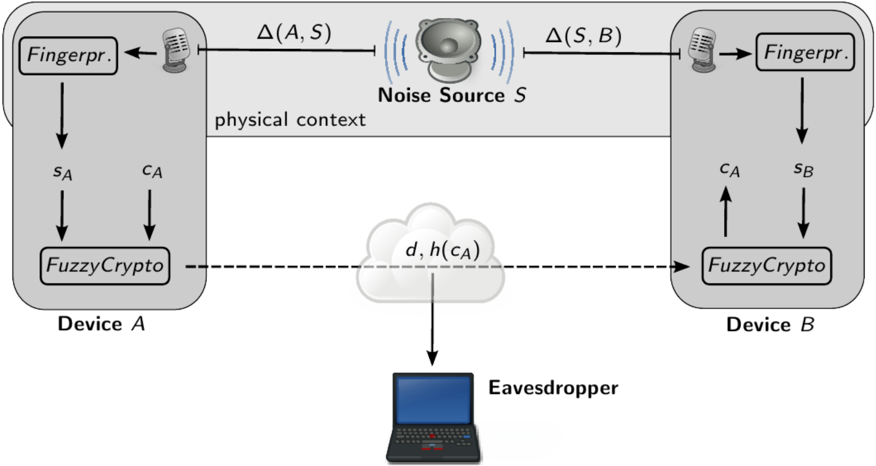


Fuzzy Cryptography

5. Device B calculates c_B by subtracting the received d from its fingerprint s_B.
6. c_B is decoded to $a \in \mathcal{A}$ and encoded back to get $c_A \in \mathcal{C}$, if the fingerprints have enough equal bits



Pairing Model



Framework

Context sources: Temperature, light, audio,. . .

Pairing Protocol

1. Device synchronisation
2. Feature extraction
3. Context processing
4. Key generation
5. Communication

Issues

Recording Hardware

- Existing audio hardware record different frequency spectra
- Different delays until recording starts after initiating it

Time Synchronisation

- Using Network Time Protocol (NTP)
- Derive fingerprints by shifting generated fingerprint in time

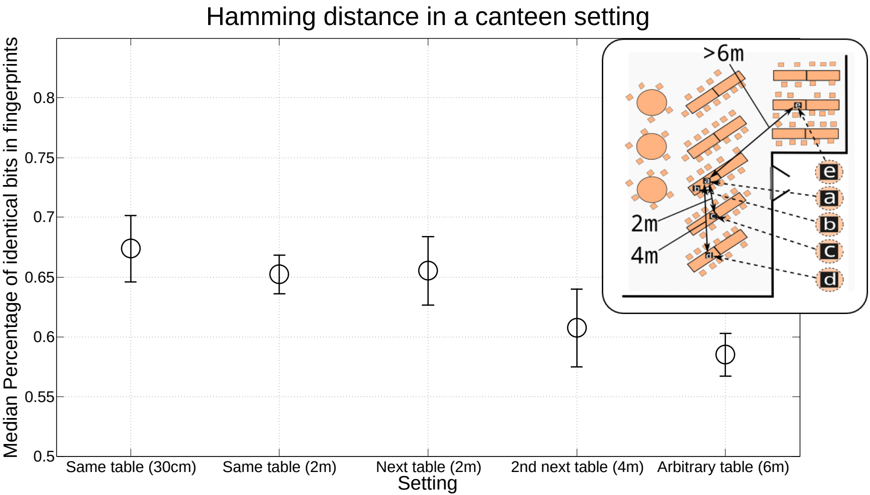


Figure: Median percentage of bit errors in fingerprints generated by two mobile devices in a canteen environment

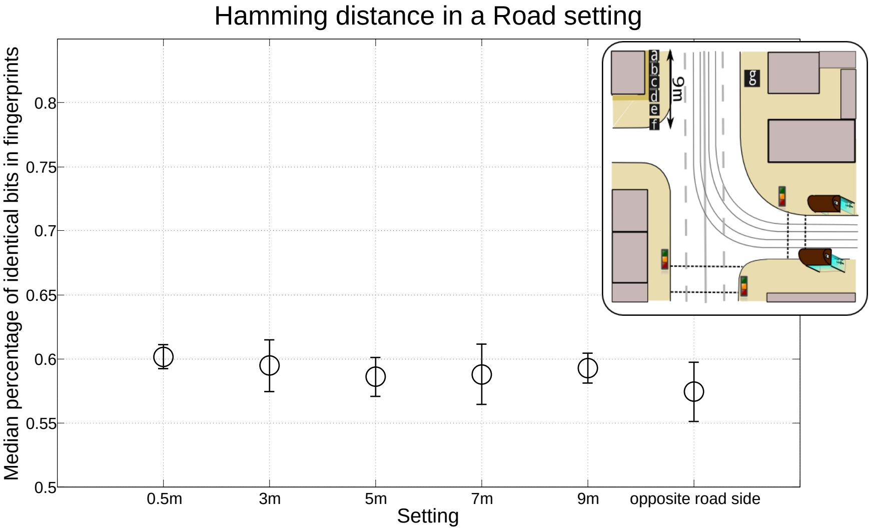


Figure: Median percentage of bit errors in fingerprints from two mobile devices beside a heavily trafficked road.

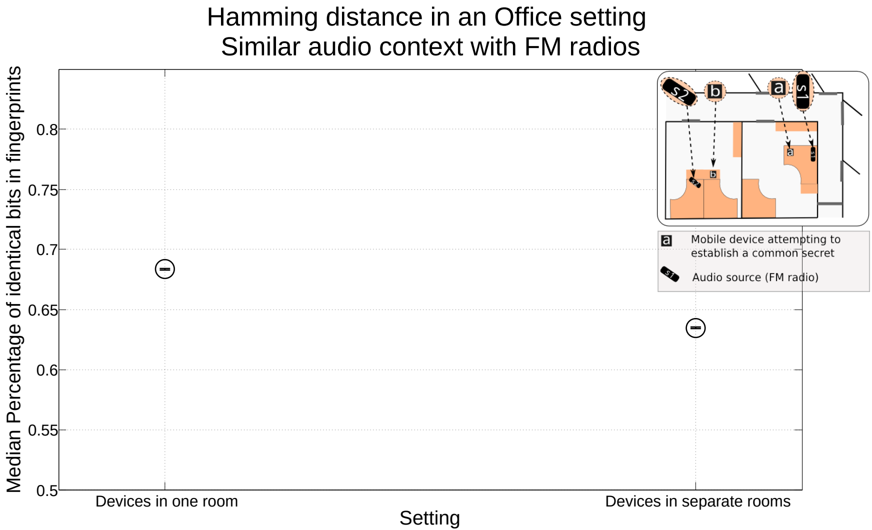


Figure: Fingerprints generated by two mobile devices in an office setting. The audio context was dominated by an FM radio tuned to the same channel.

Conclusion

Results

- Unobtrusive pairing of previously unknown devices
- Real world experiments
- Implementation as a prototype
- Entropy considerations for audio fingerprints

Future use cases

- Pairing headsets without heavy user interaction
- Sharing files in a group of people

See demonstration of prototype at CoSDEO workshop!

Dominik Schürmann
d.schuermann@tu-braunschweig.de

Stephan Sigg, Yusheng Ji
{sigg,kei}@nii.ac.jp

Error correction

- Generally the scheme can correct up to $\left\lfloor \frac{\Delta}{2} \right\rfloor$ errors

1. Decode c_B to $\mathcal{A}$: a_B
2. Encoding a back to $\mathcal{C}$: $\overline{c_B}$
3. $\overline{c_B} = c_B$ iff $m(s_A, s_B) < \left\lfloor \frac{\Delta}{2} \right\rfloor \Leftrightarrow m(c_A, c_B) < \left\lfloor \frac{\Delta}{2} \right\rfloor$

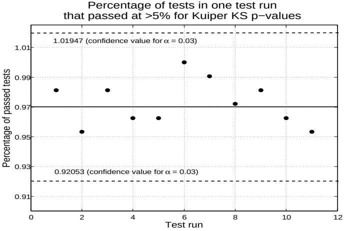
Entropy

Test suite

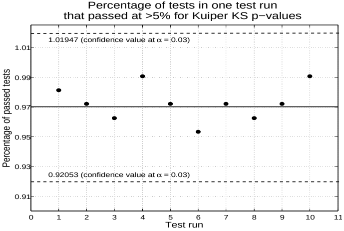
- DieHarder test suite to test entropy
- Tests calculates the p-value of a given random sequence with respect to several statistical tests
- The p-value denotes the probability to obtain an input sequence by a truly random bit generator

Results

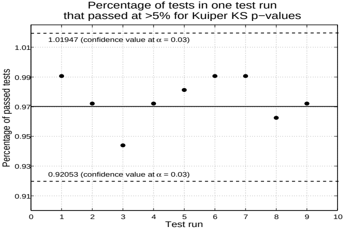
- 7490 statistical-test-batches consisting of 100 repeated applications of one specific test each
- Only 173, or about 2.31% resulted in a p-value of less than 0.05



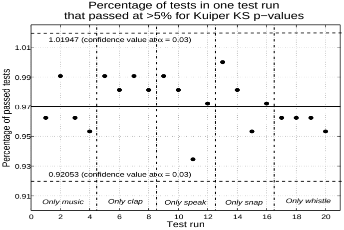
(a) Proportion of sequences from an indoor laboratory environment passing a test



(b) Proportion of sequences from various outdoor environments passing a test



(c) Proportion of sequences from all but music samples passing a test



(d) Proportion of sequences belonging to a specific audio class passing a test