Technische
Universität
Braunschweig

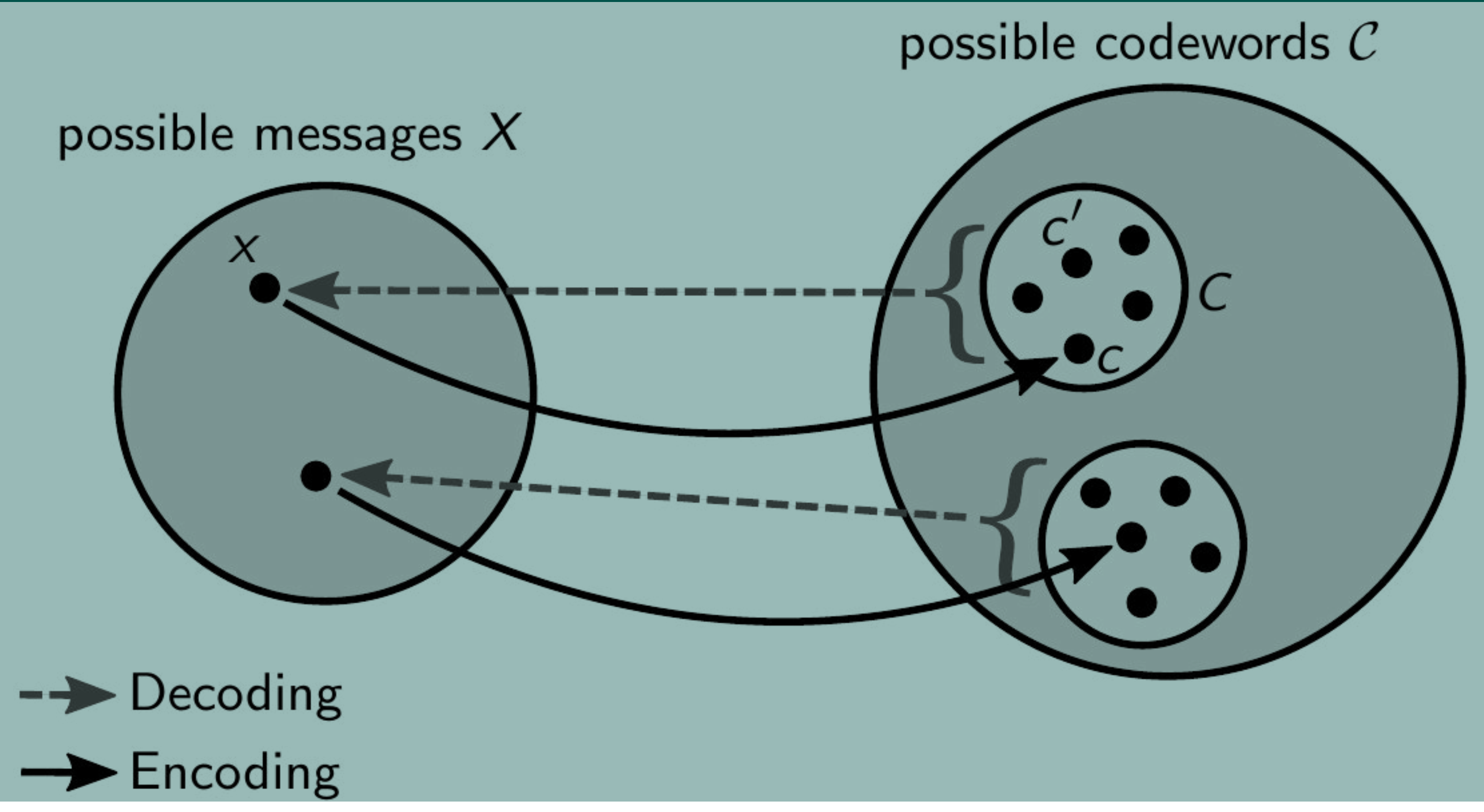
**Institut für Betriebssysteme
und Rechnerverbund**

Secure communication based on ambient audio

Dominik Schuermann and Stephan Sigg
Technische Universität Braunschweig | Institut für Betriebssysteme und Rechnerverbund
< schuerm | sigg >@ibr.cs.tu-bs.de | Telefon +49 531 391-3249

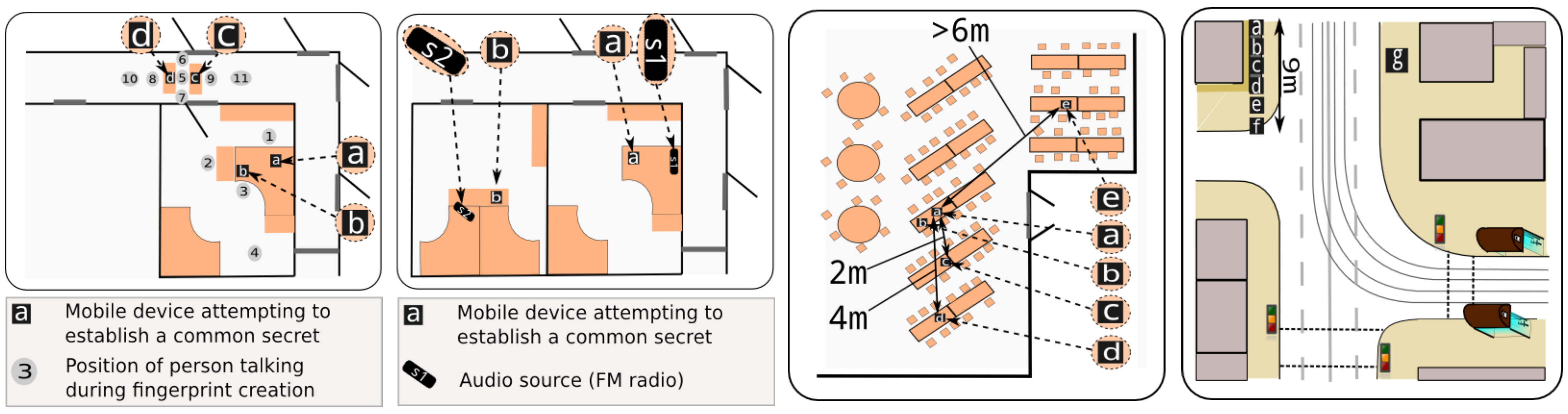
Published in: IEEE Transactions on Mobile Computing (TMC), Feb. 2013, vol. 12 no. 2

We propose to establish a secure communication channel among devices based on similar audio patterns.
Features from ambient audio are used to generate a shared cryptographic key between devices without exchanging information about the ambient audio itself or the features utilised for the key generation process.
We explore a common audio-fingerprinting approach and account for the noise in the derived fingerprints by employing error correcting codes.
This fuzzy-cryptography scheme enables the adaptation of a specific value for the tolerated noise among fingerprints based on environmental conditions by altering the parameters of the error correction and the length of the audio samples utilised.



Fuzzy cryptography on audio fingerprints

We utilise Reed-Solomon $RS(q,m,n)$ error-correcting codes with $q = 2^k, k \in \mathbb{N}$ and $n < 2^k$ in order to generate a common secret among devices from similar ambient audio. Fingerprints are linked to codewords and sufficiently similar fingerprints decode to an identical message x.

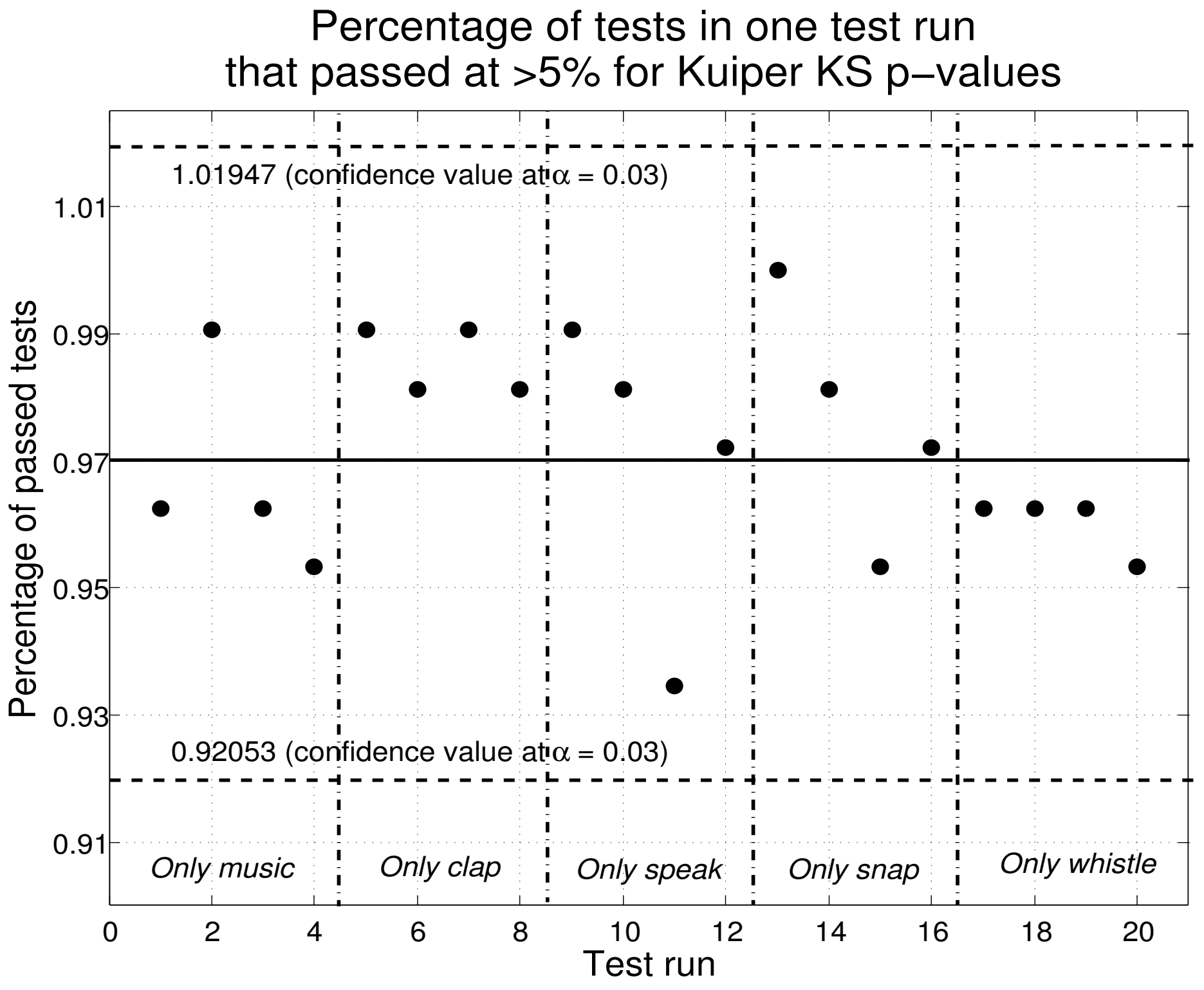

d
c
10
8
d
5
c
9
11
6
7
1
2
a
b
3
4
a
b
a Mobile device attempting to establish a common secret
3 Position of person talking during fingerprint creation
s2
b
a
s1
a Mobile device attempting to establish a common secret
s1 Audio source (FM radio)
>6m
2m
4m
e
a
b
c
d
9m
a
b
c
d
e
f
g

Experimental case studies

Our experiments in four situations feature differing loudness levels and background noise. In scenario 1, we consider ad-hoc secure communication from ongoing discussions in an office environment. In scenario 2 we demonstrate that even for an adversary able to establish a similar dominant audio context in a different room by listening to the same FM-radio-channel, the gap in the created fingerprints is significant. Scenario 3 places devices at distinct locations in a canteen to study the success probability based on their distance. In scenario 4 we study the feasibility of establishing a secure communication channel with road-traffic as background noise.

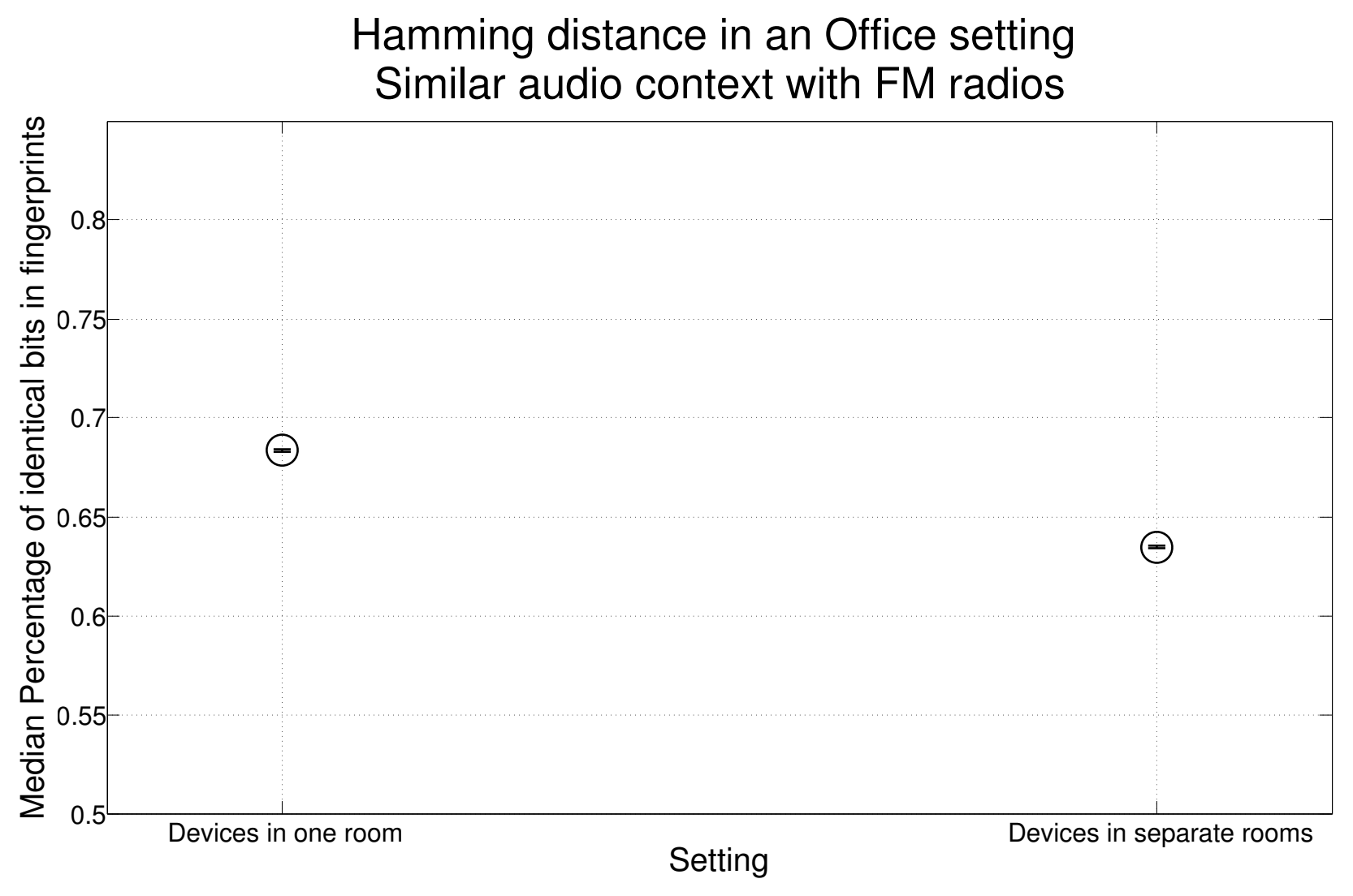
Entropy

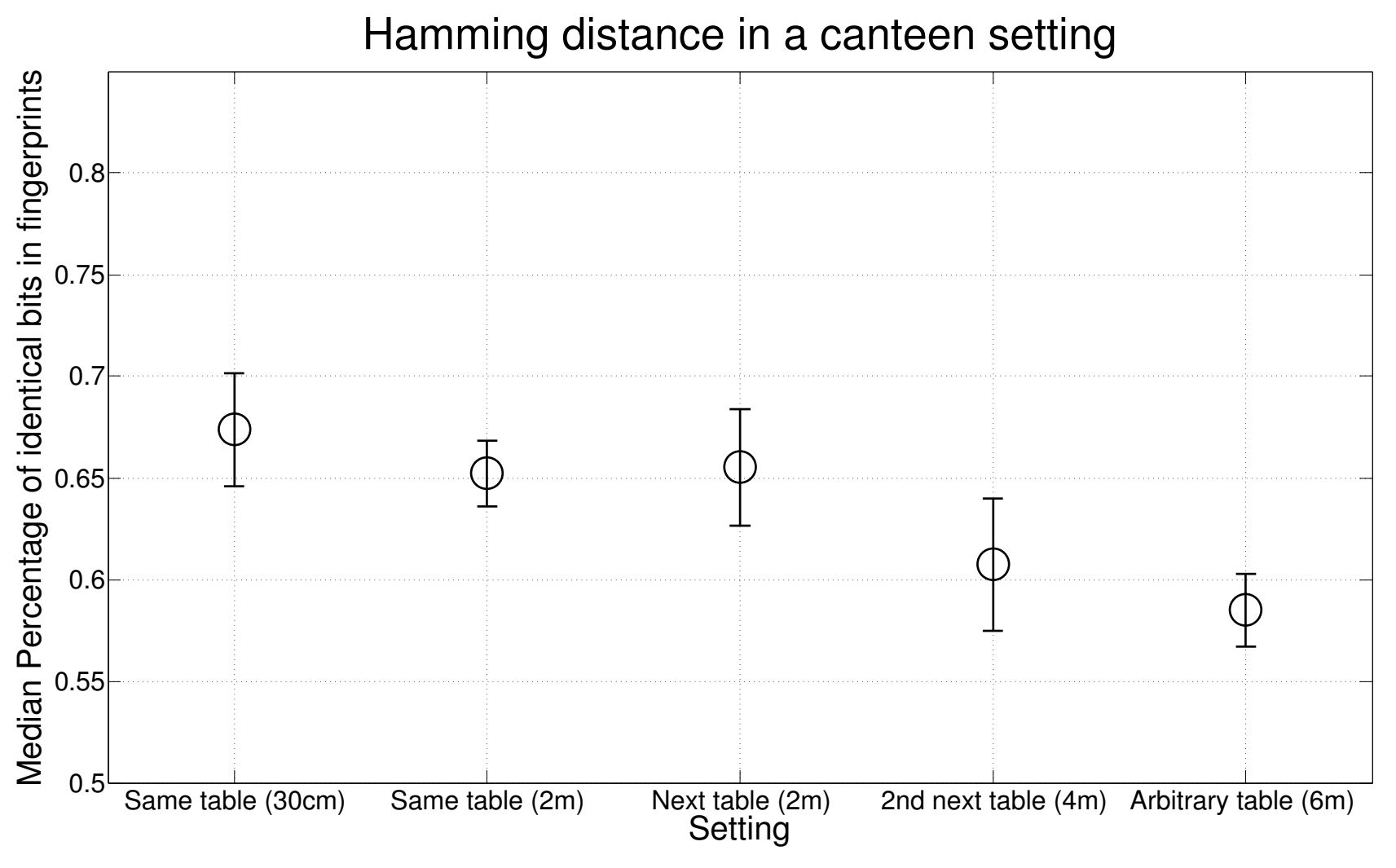
480 bit fingerprints;
7490 statistical-test-batches;
100 repetitions of one specific test.
Only 173, or about 2.31% resulted in a p-value of less than 0.051.

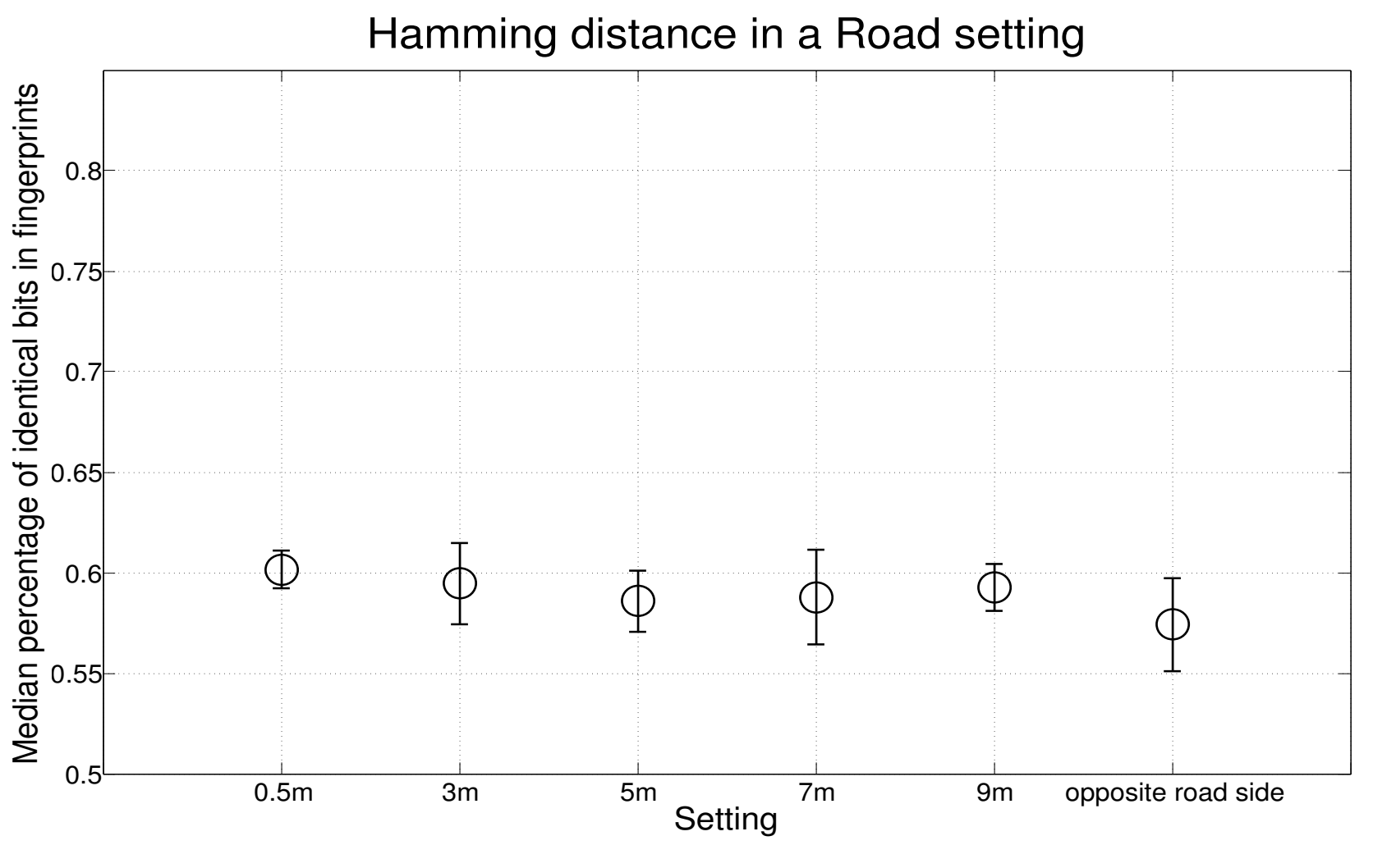


Results

The fingerprint-similarity reached differs with the scenario and its noise characteristics. However, in all cases, the hamming distance reached for devices in proximity can be clearly separated from a device in a remote context which reaches about 50% identical bits with high probabiliity.







Conclusion

We leverage fuzzy-cryptography to exploit ambient audio to establish a secure channel among unacquainted devices. The scheme is unobtrusive and unattended and enables automatically secure communication of autonomous nodes. No information on the secure key is disclosed on the wireless channel. It is adaptable in its noise tolerance through parameters of the error correcting code and audio sample length. In 7500 experiments we derived the expected Hamming distance among audio-fingerprints. The fraction of identical bits is above 0.75 for fingerprints from the same audio context and below 0.55 otherwise. This gap is exploited to generate a common secret.
Statistical tests show that the entropy of audio-fingerprints is high and sufficient for a cryptographic scheme. In 4 case-studies, we tested the protocol under realistic conditions. The largest separation between fingerprints from identical and non-identical audio-contexts was observed indoor with low background noise and a single dominant audio source. Worst results have been obtained in a setting conducted beside a heavily trafficked road.