Fuzzy cryptography (for audio-based secure device pairing) – brief

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

Version 1.0, September 1, 2016
Secure spontaneous authentication from ambient audio
Motivation

Trust and proximity

We will use audio as a source of common information in proximity.
Motivation

Trust and proximity
We will use audio as a source of common information in proximity
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing

```
10110...11011
```

```
10010...01011
```

```
11010...01110
```
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing

codespace
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Spontaneous audio-based device pairing
Secure pairing from noisy data

possible messages $X$

possible codewords $C$

Decoding

Encoding
Audio-based ad-hoc secure pairing

- Use audio to generate secret key
- high Entropy, fuzzy cryptography, case studies, attack scenarios

Hamming distance in created fingerprints (loud audio source in 1.5m and 3m)

<table>
<thead>
<tr>
<th>Audio sequence class</th>
<th>Median percentage of identical bits in fingerprints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clap</td>
<td>0.5</td>
</tr>
<tr>
<td>Music</td>
<td>0.55</td>
</tr>
<tr>
<td>Snap</td>
<td>0.6</td>
</tr>
<tr>
<td>Speak</td>
<td>0.65</td>
</tr>
<tr>
<td>Whistle</td>
<td>0.7</td>
</tr>
</tbody>
</table>

Percentage of tests in one test run that passed at >5% for Kuiper KS p-values

<table>
<thead>
<tr>
<th>Test run</th>
<th>Percentage of passed tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.91</td>
</tr>
<tr>
<td>2</td>
<td>0.93</td>
</tr>
<tr>
<td>4</td>
<td>0.95</td>
</tr>
<tr>
<td>6</td>
<td>0.97</td>
</tr>
<tr>
<td>8</td>
<td>0.99</td>
</tr>
<tr>
<td>10</td>
<td>1.01 (confidence value at $\alpha = 0.03$)</td>
</tr>
</tbody>
</table>

Fingerprints created for matching audio samples
Fingerprints created for non-matching audio samples

1S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing
Security from environmental stimuli

Audio-based ad-hoc secure pairing²

- Audio as common context source
- Fuzzy cryptography

Security from environmental stimuli

Hamming distance in created fingerprints
(loud audio source in 1.5m and 3m)

Fingerprints created for matching audio samples
Fingerprints created for non-matching audio samples

Audio sequence class

Median percentage of identical bits in fingerprints

Fingerprints created for matching audio samples
Fingerprints created for non-matching audio samples

Clap
Music
Snap
Speak
Whistle

Hamming distance in created fingerprints
(loud audio source in 1.5m and 3m)

0.5
0.55
0.6
0.65
0.7
0.75
0.8

Hamming distance in created fingerprints
(loud audio source in 1.5m and 3m)

0.91
0.93
0.95
0.97
0.99
1.01

Percentage of tests in one test run
that passed at >5% for Kuiper KS p-values

1.01947 (confidence value at $\alpha = 0.03$)
0.92053 (confidence value at $\alpha = 0.03$)

Only music
Only whistle
Only snap
Only speak
Only clap

Security from environmental stimuli

Real-time implementation on android mobile phones

Stephan Sigg, et al., AdhocPairing: Spontaneous audio-based secure device pairing for Android mobile devices, IWSSI 2012

- Hardware noise cancellation on some phones
- Hardware originated synchronisation offset
Security from environmental stimuli

How to synchronise audio without disclosing information?
No data shall be transmitted among devices
Hardware-originated synchronisation offset

- Approximate pattern matching with arbitrary common sequence

Security from environmental stimuli

Hardware-originated synchronisation offset

- Synchronisation in the order of 3ms possible
- No additional data transmitted among devices\(^3\) \(^4\)

---

\(^3\) N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Pattern-based Alignment of Audio Data for Ad-hoc Pairing, ISWC, 2012

\(^4\) N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Using ambient audio in secure mobile phone communication, PerCom, 2012
Security from environmental stimuli
Security from environmental stimuli

No data transmission

Sketch
Security from environmental stimuli
Security from environmental stimuli

sketch
Security from environmental stimuli
Security from environmental stimuli

[Sketch of a diagram with arrows and shapes]