PINtext: A Framework for Secure Communication Based on Context

Stephan Sigg[1], Dominik Schuermann[2], and Yusheng Ji[1]

[1] National Institute of Informatics, Tokyo, Japan
{sigg,kei}@nii.ac.jp
[2] TU Braunschweig, Braunschweig, Germany
d.schuermann@tu-braunschweig.de

Abstract. We propose a framework for secure device-pairing based on contextual information. In contrast to related work, we utilise fuzzy cryptography schemes to establish a common secret among devices and to account for noise in the contextual features. The framework is implemented for ambient audio and its feasibility is demonstrated in a case study. Additionally, we discuss properties of fingerprints from ambient audio and estimate the entropy of fingerprints in statistical tests.

1 Introduction

With the increased penetration by mobile devices in recent years, security threats and security requirements similarly have multiplied. This orchestration of distinct threats, however, is vague to mobile users. In addition to this, security mechanisms are often perceived as a hassle since they are not unobtrusive and might distract from high-level tasks. Pin, smartcard and password-based schemes are perceived as annoying so that users may even consider to switch off security mechanisms on their device [23]. The requirement that passwords shall be frequently changed, increases the perceived complexity of these systems further. Contemporary mobile communication technologies such as Bluetooth [5] or Near Field Communication (NFC) [17] address this problem differently. While Bluetooth increases the effort of the user, requiring a PIN for device pairing, NFC omits security precautions and rely on the restricted communication range solely.

Is it feasible to provide security that is less obtrusive or even unobtrusive?

In this paper we propose a device-pairing paradigm that is capable of providing unobtrusive security means based on environmental contexts. In particular, mobile devices are equipped with a multitude of sensors that provide them with environmental stimuli such as audio, light, RF temperature or proximity. this data can be exploited in order to derive a classification of a given contextual configuration.

Contextual data is in some respect similar to biometric data. However, in contrast to contextual data, for the use in cryptographic applications, biometric data has some unfavourable properties as detailed in [29].

A. Puiatti et al. (Eds.): MobiQuitous 2011, LNICST 104, pp. 314–325, 2012.

The amount of biometric information is limited: Only a restricted amount of different biometric samples is available.

Biometric data can be stolen: It is generally desired, that biometric information is easily retrieved and verified. On the contrary, biometric information shall be hard to obtain by third parties. This contradiction is frequently solved in favour of the former requirement. Consequently, as pictures from a face are easily taken, fingerprints are spread unnoticed and high-quality photographs of an Iris are feasible from greater distance, the security means provided by biometric data can be broken by a determined adversary.

Biometric data does not change significantly: In order to increase the burden for an adversary to break a security system, it is beneficial to periodically change the secret utilised. Since Biometric data never changes significantly, the seed for cryptographic methods is of limited variability.

We propose to use context as an implicit mechanism to establish a basic level of security that adapts to current situations. In particular, context information can be utilised as common secret among devices in the same situation. Observe that this concept of security is similar to our natural perception of trust. Frequently, we have an increased level of trust with people that share our context [6]. Classical security mechanism then need only be inferred when activities with higher security demands are issued.

Despite these benefits, there are also some challenges and concerns that have to be addressed when contextual information is utilised as the basis of security means. Similar to biometric information, context data can be considered as noisy source. This is a hurdle that has to be overcome but it is no principal problem since it can be addressed by appropriate error correction methods similar to those utilised for noisy biometric information [29]. Another challenge is to establish a sufficiently diverse description of context so that the chance of an adversary to obtain information on this description is low. In particular, the representation utilised must have a high entropy.

In this work we present a framework for non-interactive, ad-hoc secure communication based on contextual data. The framework will be exemplified for ambient audio. In a case study, we demonstrate the general feasibility of the approach and discuss the entropy of secure keys generated from ambient audio.

Unobtrusive security mechanisms enable the implementation of a constant security aura surrounding mobile device. This will increase the burden an attacker has to overcome.

In section 2, the related work on context-based authentication and security mechanisms is detailed. Afterwards, in section 3, we propose a framework to establish security means based on contextual information on a set of devices. The framework is then exemplary applied for ambient audio. Section 4.1 describes the generation of audio-fingerprints and discusses their suitability as a seed for a common secret. In section 4.2, we study the entropy of audio-fingerprints and show that it is sufficiently high. Section 4.3 details a case study we conducted to show the feasibility in realistic settings. In Section 5 we draw our conclusion.

2 Related Work

In recent years, increasing interest is expressed in security of mobile devices [24]. The National Institute for Standards and Technology (NIST) summarises many of these considerations regarding device classes, threats and countermeasures in [12]. According to this discussion, generally the threats for mobile devices are comparable to those for stationary computers with additional issues related to the smaller size, the wireless interface and the mobile services provided. The authors also hint that mobile users seldom employ security mechanisms or apply them in a convenient but insecure way as, for instance, by using passwords that are easy to guess. The reason for this behaviour pattern is a general laziness of the mobile user as derived by Nehmadi et al. [23].

Basic requirements of data privacy on mobile phones have been derived by Karlson et al. [13]. Building on these results, De Luca et al. [24] discuss the establishing of context-specific proximity-related security-spheres. In this work, users define which data is accessible in which sphere. The traversal between spheres is established by locations and actions. A work on a context-adaptive mobile device was presented in [25]. The authors present a mechanism for mobile phones to adapt the ringtone volume, vibration and alerts to the current context.

Recently, several authors utilised context as a seed for authentication or the creation of secure keys [22]. Holmquist et al. are probably the first to mention context to establish security [11]. They propose to use context proximity for selective artefact communication. This was later picked up by Gellersen et al. for using identical hand gestures to unlock a credit card [7]. Mayrhofer et al. propose two protocols for secure authentication that utilise accelerometer data in devices which are shaken together [20,21]. In the ShaVe protocol, this information is utilised to verify a Diffie-Hellman key agreement [4]. The ShaCK protocol utilises the extracted feature vectors directly to generate a cryptographic key without further communication between the devices. For sufficient entropy in the generated feature vectors that are utilised as a basis to the key generation, the devices have to be shaken together for a sufficiently long time [19]. This Candidate Key Protocol generates feature sets with identical hash values at both devices and concatenates them to a shared secret key. A similar protocol that utilises rudimentary error correction of binary keys created by shaking processes is introduced by Bichler et al. [1]. They report a false negative rate of more than 11 percent for this approach and for features extracted from accelerometer data [2].

Another popular sensor utilised for authentication is the RF-transceiver. In particular, since the communication channel between two devices is sharply concentrated in time and space but at one time instant unambiguous between two communicating devices [28], authors have utilised the channel impulse response for secret device-pairing [10,16,9]. Although the channel impulse response utilised in these approaches can be considered as a strong cryptographic seed, the approach does not solve the problem of authentication and Man-In-the-Middle attacks. However, some authors have also demonstrated that it is possible to utilise channel information for proximity-restricted protocols [30]. Recently, it

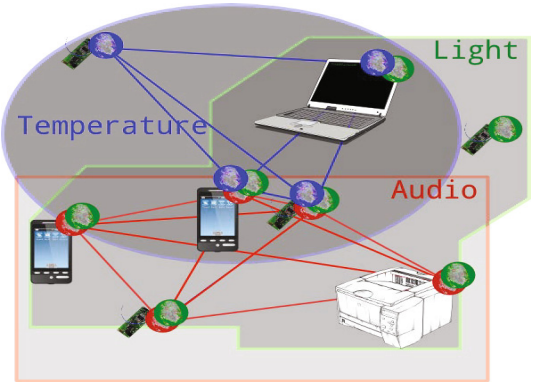


Fig. 1. Illustration of the context-based secure communication scheme with three context classes

was shown that proximity information can accurately be extracted based on recordings of ambient audio. Kunze et al., for instance, demonstrate that the location of a mobile device can be derived by sampling the audio response of its vibration sensor [15]. A discussion on research challenges and opportunities originating from utilising context information for device pairing is found in [26].

Our present work is most related to the work on spontaneous device interaction presented by Mayrhofer et al. in [22,20,21] since we also also propose to utilise context for the creation of a common secret. However, the protocol we describe for our framework is less obtrusive and can even be unobtrusive. The general idea is similar to the approach presented by Bichler et al. but we rely on error correcting codes instead [1]. Very recently, Mathur et al. utilised a similar approach on amplitude and phase data extracted from an RF-channel [18]. Regarding the discussion of the entropy of ambient audio, we recently discussed in [27] the estimation of entropy for contextual information. Similar discussions can be found in [1,22].

3 A Framework for Unobtrusive and Less Obtrusive Secure Device Communication

In this section we propose a framework to establish a secure communication channel based on common but arbitrary contextual information. As depicted in figure 1, we assume that two or more devices which share the same context utilise this information to unobtrusively establish a common secret.

Based on this secret, devices can be paired or a secure communication channel can be established. A device that is not in the same context, however, shall be unlikely able to share the secret. The figure shows devices in three context classes temperature, light and audio. Devices in the same context regarding one or more of these classes are able to utilise contextual information to establish a common secret. For instance, the two mobile phones are in the same audio context and

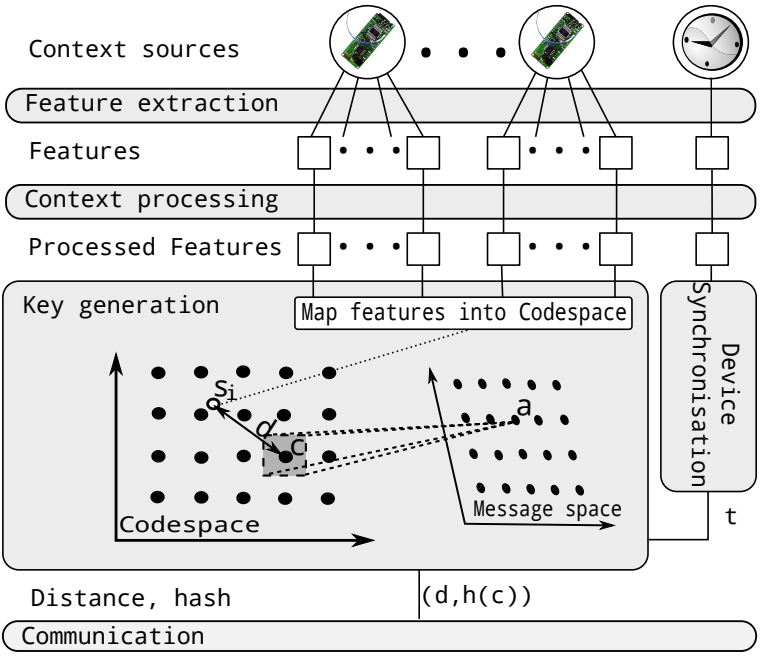


Fig. 2. Modules in our framework for device-pairing based on arbitrary contextual information

are therefore able to establish a secure communication based on this information. The laptop computer is in another audio context and not able to overhear the encrypted communication. It could, however, establish a common secret based on ambient light with the mobile phones. However, in this case, most other devices in the proximity would share the context and therefore the secret.

Establishing of the secure channel can be unobtrusive and non-interactive since it is purely based on the context observed. In order to enable such a communication scheme, features from the context source must be extracted and transformed into a sequence that is sufficiently similar on all devices in the same context but at the same time significantly different for all devices in a different context. This sequence is then utilised as a seed to generate a common secret. For this last step, since features will likely differ slightly also for identical contexts, error correction mechanisms have to be applied.

In the following, we detail general modules that constitute a framework for context-based device authentication. The models are illustrated in figure 2.

`Device synchronisation.` Due to the frequent fluctuation of context, feature values taken at distinct time will likely not be sufficiently similar to establish a common secret among devices. A synchronisation among devices is required. This module establishes sufficient synchronisation among devices dependent on the accuracy required by the features utilised.

`Feature extraction.` Any common feature extraction method can be applied. It is important, that the representation of the features is significantly diverse so that it is infeasible for an adversary to test all possible cases in sufficient time.

`Context processing.` Processing modules such as noise removal, smoothing of features or aggregation can be applied after feature extraction.

`Key generation.` We expect that the feature vector generated is noisy so that the vectors differ for distinct devices. Therefore, error correction has to be applied in order to achieve a common secret. For this error correction we propose a fuzzy cryptography scheme as described in the following (cf. the corresponding module in figure 2).

For devices i, j and feature representations s_i, s_j from a space $\mathcal{S}$, we utilise error correcting codes to disregard the bias between s_i and s_j. We assume that features are acquired by device i and device j in a sufficiently synchronised manner. We distinguish between a code space $\mathcal{C}$ and a message space $\mathcal{A}$. The message space contains clearly separated messages $a \in \mathcal{A}$. The codespace contains codewords $c \in \mathcal{C}$ that are unambiguously mapped onto the messages $\mathcal{A}$ but additionally contain redundancy. Due to this redundancy, the codespace is sparsely populated with codewords and Δ defines the minimum distance (e.g. Hamming distance) between any two codewords $c, c' \in \mathcal{C}$. In the case that a codeword becomes biased, it is generally possible to correct up to $\lfloor \frac{\Delta}{2} \rfloor$ errors so that the mapping between $\mathcal{A}$ and $\mathcal{C}$ is surjective. The procedure to obtain a common secret is the following.

After extracting feature vectors, these vectors are mapped onto representations in $\mathcal{S}$. The sequences are not necessarily identical to any code word $c \in \mathcal{C}$. We require, however, that $\mathcal{C} \subseteq \mathcal{S}$ and define a distance metric $m : \mathcal{S} \times \mathcal{S} \rightarrow \mathbb{R}$. For device i we choose a $c_i \in \mathcal{C}$ randomly and calculate the distance $d = m(s_i, c_i)$ between codeword and context representation on device i. Additionally, the hash of the codeword ($h(c_i)$) can be calculated to allow for verification. When device j now receives $m(s_i, c_i) = d$ and possibly also $h(c_i)$, it will compute c_j so that $m(s_j, c_j) = d = m(s_i, c_i)$ holds. Due to fluctuations in context and in the feature generation process, c_j is not necessarily a valid code word and might differ from c_i so that $d(c_i, c_j) > 0$ holds. By first decoding c_j onto a_j and then encoding a_j back to the message space $\mathcal{C}$, the obtained value $\overline{c_j}$ will equal c_i iff $d(s_i, s_j) < \lfloor \frac{\Delta}{2} \rfloor \Leftrightarrow d(c_i, c_j) < \lfloor \frac{\Delta}{2} \rfloor$. When also $h(c_i)$ is transmitted, device j will assume that a common secret is found when $h(c_i) = h(c_j)$ holds.

`Communication.` An arbitrary transceiver module is sufficient to provide communication during secret key generation and also for the encrypted communication. Unlike other protocols presented in [22], we do not require a separate trusted communication channel for device-pairing. Since the secret is not transmitted on the channel, a single insecure and noisy communication channel is sufficient.

4 Audio-Based Secure Communication

We implemented this framework with ambient audio as context source [26]. Audio recordings are represented by binary audio-fingerprints based on energy fluctuations [8] in 33 frequency bands over 17 non-overlapping sub-sequences of the recording. For codewords $c \in \mathcal{C}$ with length $|c| = 512$ bits and words $a \in \mathcal{A}$ with length $|a| = 204$ bits we utilised Reed-Solomon codes with $\Delta = \lfloor |c| - |a| \rfloor$. To estimate the entropy of fingerprints, we first discuss properties of the fingerprints in section 4.1 and their entropy in section 4.2. In section 4.3 we briefly demonstrate the performance of this implementation in a realistic environment.

4.1 Properties of Audio-Fingerprints

In a controlled indoor environment we recorded samples with two microphones at various distances. The samples were played back by a single audio source. Microphones were attached to the left and right ports of an audio card with audio cables of equal lengths and placed at 1.5 m, 3 m, 4.5 m and 6 m distance to the audio source. The samples were emitted at quiet ($\approx 10-23$dB), medium ($\approx 23-33$dB) and loud ($\approx 33-45$dB) volume. They consisted of several instances of music, a person clapping her hands, snapping her fingers, speaking and whistling.

We created audio-fingerprints for both microphones and compared their Hamming distance. Overall, 7500 comparisons between fingerprints are conducted in various settings. From these, 300 comparisons are created for simultaneously recorded samples. Figure 3 depicts the median percentage of identical bits in the fingerprints for simultaneously and non-simultaneously recorded samples and several positions of the microphones and loudness levels. The error bars in the figures show the variance in the Hamming distance.

The similarity in the fingerprints is significantly higher for simultaneously sampled audio. Only about 3.8 % of the comparisons from non-matching samples have a similarity of more than 0.58 and only 0.4583 % have a similarity of more than 0.6. Similarly, only 2.33 % of the comparisons of synchronously sampled audio have a similarity of less than 0.7. We observed that the distance of the microphones to the audio source and the loudness level has no impact on the similarity of fingerprints.

The remaining bit errors for synchronously recorded samples can be corrected by error correcting codes (Reed-Solomon in our case) as detailed in section 3.

4.2 Entropy of Fingerprints

Although these results suggest that it is unlikely for a device in another audio context to generate sufficiently similar fingerprints, an active adversary might analyse the fingerprints created to identify and explore a possible weakness in the encryption key. Such a weakness might be repetitions of subsequences in the key or an unequal distribution of symbols. When an adversary overhears a message encrypted with a key biased in such a way, the cypher may leak information about the encrypted message, provided that the adversary is aware of the bias.

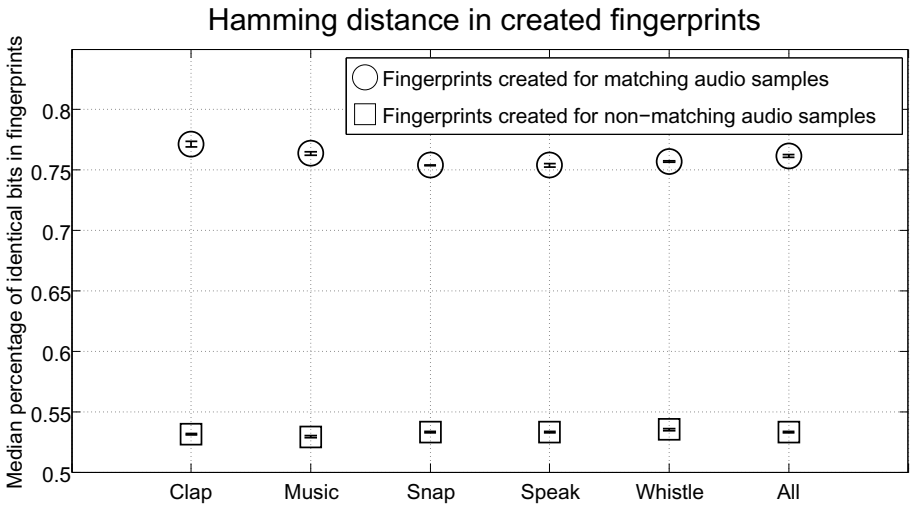


Fig. 3. Median percentage of identical bits in fingerprints created for synchronised and on-synchronised audio recordings over all distances and loudness levels

We tested the entropy of fingerprints generated for audio-sub-sequences. We apply various statistical tests on the distribution of bits in an audio-fingerprint. In particular, we utilise the dieHarder [3] set of statistical tests. This battery of 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. We applied all tests to a set of fingerprints of 480 bits length. We utilised the samples obtained in section 4.1 and additionally sampled audio in various outdoor settings (a crowded canteen environment, a heavily trafficked road, an office environment).

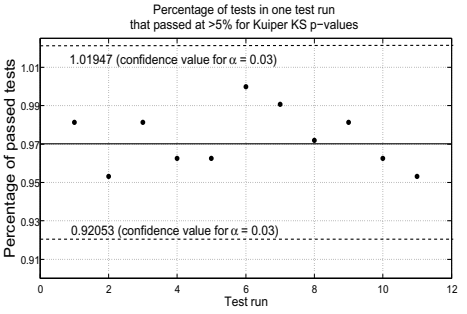
In the 7490 test-batches for the fingerprints described in section 4.1 which consisted of 100 repeated applications of one specific test each, only 173 batches, or about 2.31% resulted in a p-value of less than 0.05.[1] Each specific test was repeated at least 70 times. The p-values are calculated according to the statistical test of Kuiper [14].

Figure 4 depicts for all test-series conducted the fraction of tests that did not pass a sequence of 100 consecutive runs at $> 5\%$ for Kuiper KS p-values [14] for all 107 distinct tests in the DieHarder battery of statistical tests.

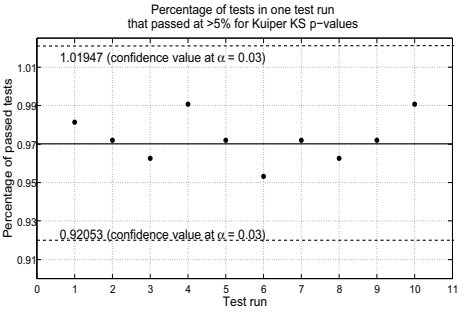
Generally, we observe that for all test runs conducted, the number of tests that fail is low. It is in all cases within the confidence interval with a confidence value of $\alpha = 0.03$. The confidence interval was calculated for $m = 107$ tests conducted as $1 - \alpha \pm 3 \cdot \sqrt{\frac{(1-\alpha)\cdot\alpha}{m}}$.

Also, we could not observe any distinction between indoor and outdoor settings (cf. figure 4a and figure 4b) so that we conclude that also the increasing

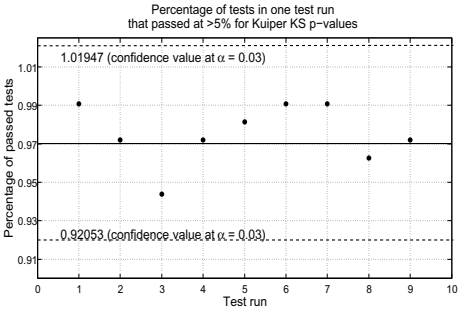
[1] All results of the statistical tests are available at http://www.ibr.cs.tu-bs.de/users/sigg/StatisticalTests/TestsFingerprints_110601.tar.gz



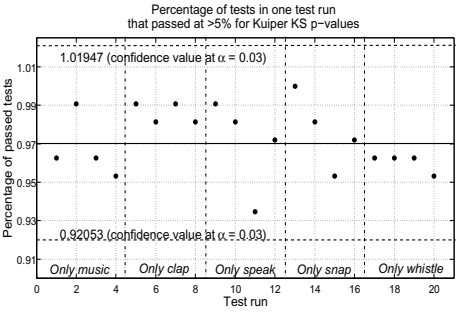
(a) Proportion of sequences from an indoor laboratory environment passing a test



(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

Fig. 4. Illustration of P-Values obtained for the audio-fingerprints from applying the DieHarder battery of statistical tests

noise figure and different hardware utilised [2] does not impact the test results. Since music might represent a special case due to its structured properties and possible repetitions in an audio sequence, we considered it separately from the other samples. We could not identify a significant impact of music on the outcome of the test results (cf. figure 4c).

Additionally, we separated audio samples of one audio class and used them exclusively as input to the statistical tests. Again, there is no significant change for any of the classes (cf. figure 4d).

Summarising, we conclude that we could not observe any bias in fingerprints based on ambient audio. Consequently, the entropy of fingerprints based on ambient audio can be considered as high. An adversary should gain no significant Information from an encrypted message overheard.

[2] Overall, the microphones utilised (2 internal, 2 external) were produced by three distinct manufacturers.

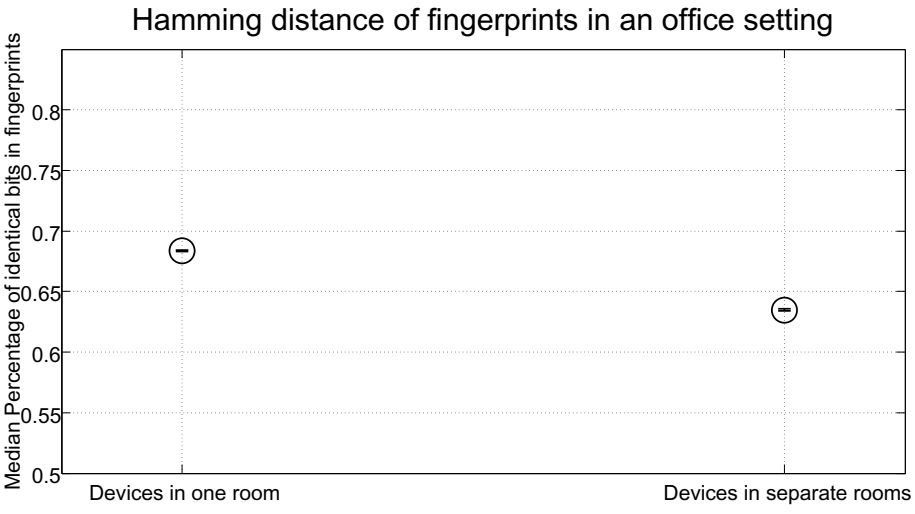


Fig. 5. Median percentage of bit errors in fingerprints from two devices in an office. Audio context was dominated by an FM radio tuned to the same channel.

4.3 Case Study

We consider an environment in which two laptop computers are situated in an office while a third device is located in a neighbouring office. The door to the office was closed but in both rooms we placed two FM-radios, tuned to the same frequency in both rooms. The audio context was dominated by the synchronised music and speech from the FM-radio channel. The distance to the audio source was identical for all devices. The loudness level of the audio source was tuned to about 50 dB in both rooms. Figure 5 depicts the median bit-similarity achieved when the devices were placed in the same room and in different rooms respectively. In both cases the variance in the bit errors achieved is below 0.1 %. When both devices are placed in the same room, the median Hamming distance between fingerprints is only 31.64 %. When the devices are placed in different rooms, the variance in bit error rates is still low with 0.008 %. The median Hamming distance rose in this case to 36.52 %. Consequently, although the dominant audio source in both settings generated identical and synchronised content, the Hamming distance drops significantly when both devices are in an identical room. With sufficient configuration of the error correction method conditioned on the Hamming distance, an eavesdropper can be prevented from stealing the secret key even though some information on the audio context might be leaking.

5 Conclusion

We have proposed a generic framework for device-pairing based on contextual information. The distinct modules of the framework are flexible and can be put

into effect by arbitrary implementations. The framework utilises fuzzy cryptography schemes to share a common secret at remote devices without revealing information about the secret. Possible variations in the context samples utilised are corrected by error correcting codes. We demonstrated the feasibility of the framework in an implementation for ambient audio. The implementation was successfully applied in an office setting. Additionally, we analysed the properties of the audio-fingerprints generated and estimated the entropy in statistical tests. In these tests, no bias could be observed.

Acknowledgment. This work was supported by a fellowship within the Postdoc-Programme of the German Academic Exchange Service (DAAD).

References

1. Bichler, D., Stromberg, G., Huemer, M.: Innovative key generation approach to encrypt wireless communication in personal area networks. In: Proceedings of the 50th International Global Communications Conference (2007)
2. Bichler, D., Stromberg, G., Huemer, M., Löw, M.: Key Generation Based on Acceleration Data of Shaking Processes. In: Krumm, J., Abowd, G.D., Seneviratne, A., Strang, T. (eds.) UbiComp 2007. LNCS, vol. 4717, pp. 304–317. Springer, Heidelberg (2007)
3. Brown, R.G.: Dieharder: A random number test suite (2011), `http://www.phy.duke.edu/~rgb/General/dieharder.php`
4. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory IT-22(6), 644–654 (1976)
5. Dunning, J.P.: Taming the blue beast: A survey of Bluetooth based threats. IEEE Security Privacy 8(2), 20–27 (2010)
6. Dupuy, C., Torre, A.: Local Clusters, trust, confidence and proximity, Clusters and Globalisation: The development of urban and regional economies, pp. 175–195 (2006)
7. Gellersen, H.W., Kortuem, G., Schmidt, A., Beigl, M.: Physical prototyping with smart-its. IEEE Pervasive Computing 4(1536-1268), 10–18 (2004)
8. Haitsma, J., Kalker, T.: A Highly Robust Audio Fingerprinting System. Journal of New Music Research 32(2), 211–221 (2003)
9. Ben Hamida, S.T., Pierrot, J.B., Castelluccia, C.: An adaptive quantization algorithm for secret key generation using radio channel measurements. In: Proceedings of the 3rd International Conference on New Technologies, Mobility and Security (2009)
10. Hershey, J., Hassan, A., Yarlagadda, R.: Unconventional cryptographic keying variable management. IEEE Transactions on Communications 43, 3–6 (1995)
11. Holmquist, L.E., Mattern, F., Schiele, B., Alahuhta, P., Beigl, M., Gellersen, H.W.: Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) UbiComp 2001. LNCS, vol. 2201, pp. 116–122. Springer, Heidelberg (2001)
12. Jansen, W., Scarfone, K.: Guidelines on cell phone and PDA security. Technical Report SP 800-124, National Institute of Standards and Technology (2008)
13. Karlson, A.K., Brush, A.J.B., Schechter, S.: Can I borrow your phone?: Understanding concerns when sharing mobile phones. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems, CHI 2009 (2010)

14. Kuiper, N.H.: Tests concerning random points on a circle. In: Proceedings of the Koinklijke Nederlandse Akademie van Wetenschappen, vol. 63, pp. 38–47 (1962)
15. Kunze, K., Lukowicz, P.: Symbolic Object Localization Through Active Sampling of Acceleration and Sound Signatures. In: Krumm, J., Abowd, G.D., Seneviratne, A., Strang, T. (eds.) UbiComp 2007. LNCS, vol. 4717, pp. 163–180. Springer, Heidelberg (2007)
16. Madiseh, M.G., McGuire, M.L., Neville, S.S., Cai, L., Horie, M.: Secret key generation and agreement in UWB communication channels. In: Proceedings of the 51st International Global Communications Conference, Globecom (2008)
17. Madlmayr, G., Langer, J., Kantner, C., Scharinger, J.: Nfc devices: Security and privacy. In: Third International Conference on Availability, Reliability and Security (ARES 2008), pp. 642–647 (March 2008)
18. Mathur, S., Miller, R., Varshavsky, A., Trappe, W., Mandayam, N.: Proximate: Proximity-based secure pairing using ambient wireless signals. In: Proceedings of the Ninth International Conference on Mobile Systems, Applications and Services, MobiSys 2011 (2011)
19. Mayrhofer, R.: The Candidate Key Protocol for Generating Secret Shared Keys from Similar Sensor Data Streams. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) ESAS 2007. LNCS, vol. 4572, pp. 1–15. Springer, Heidelberg (2007)
20. Mayrhofer, R., Gellersen, H.-W.: Shake Well Before Use: Authentication Based on Accelerometer Data. In: LaMarca, A., Langheinrich, M., Truong, K.N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 144–161. Springer, Heidelberg (2007)
21. Mayrhofer, R., Gellersen, H.W.: Shake well before use: Two implementations for implicit context authentication. In: Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp 2007), pp. 72–75 (2007)
22. Mayrhofer, R., Gellersen, H.W.: Spontaneous mobile device authentication based on sensor data. Information Security Technical Report 13(3), 136–150 (2008)
23. Nehmadi, L., Meyer, J.: A system for studying usability of mobile security. In: Proceedings of the 3rd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (2011)
24. Seifert, J., De Luca, A., Conradi, B., Hussmann, H.: TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones. In: Floréen, P., Krüger, A., Spasojevic, M. (eds.) Pervasive 2010. LNCS, vol. 6030, pp. 130–137. Springer, Heidelberg (2010)
25. Siewiorek, D., Smailagic, A., Furukawa, J., Krause, A., Moraveji, N., Reiger, K., Shaffer, J., Wong, F.L.: Sensay: A context-aware mobile phone. In: Proceedings of the 7th IEEE International Symposium on Wearable Computers
26. Sigg, S.: Context-based security: State of the art, open research topics and a case study. In: Proceedings of the 5th ACM International Workshop on Context-Awareness for Self-Managing Systems, CASEMANS 2011 (2011)
27. Sigg, S., Budde, M., Ji, Y., Beigl, M.: Entropy of Audio Fingerprints for Unobtrusive Device Authentication. In: Beigl, M., Christiansen, H., Roth-Berghofer, T.R., Kofod-Petersen, A., Coventry, K.R., Schmidtke, H.R. (eds.) CONTEXT 2011. LNCS, vol. 6967, pp. 296–299. Springer, Heidelberg (2011)
28. Smith, G.: A direct derivation of a single-antenna reciprocity relation for the time domain. IEEE Transactions on Antennas and Propagation 52, 1568–1577 (2004)
29. Tuyls, P., Skoric, B., Kevenaar, T.: Security with Noisy Data. Springer (2007)
30. Varshavsky, A., Scannell, A., LaMarca, A., de Lara, E.: Amigo: Proximity-based authentication of mobile devices. International Journal of Security and Networks (2009)