

Generating Random Sequences from Fingerprints

Shkodran Gerguri, Václav Matyáš, Zdeněk Říha, Luděk Smolík

Faculty of Informatics
Masaryk University, Brno
sgerguri@mail.muni.cz

November 14, 2008

- 1 Introduction
- 2 Biometrics and Cryptography – Current Approaches
- 3 Random Sequence Generation using Fingerprints
- 4 Entropy Estimation Tests
- 5 Conclusion

- Biometrics – measurable human characteristics of physical or behavioral nature.
- Current use involves user authentication and (physical) access control, with a possible employment in novel cryptographic key management and access control schemes.
- Advantages: ready availability, low requirements on the user
- Disadvantages: not entirely secret, correction required on measured data, false acceptance and false rejection

Current biometric authentication systems focus on eliminating the differences in measured data. On the other hand, the random perturbations can, in theory, be exploited for random sequence/number generation.

Biometrics and Cryptography

- Traditional key management and access control mechanisms based on secret values, usually passwords, with a secure storage.
- The drawback? Passwords are not very secure and are susceptible to automated dictionary attacks; they are also easily forgotten.
- Biometrics provide a measure of protection against artificial attacks by employing liveness tests and, unlike passwords, cannot be forgotten.
- Research in the applications of biometrics in cryptography focuses on key management.

A major challenge is compensating for the random perturbations introduced into the biometric data by the measurement process itself. To avoid security issues, it is also desirable to avoid storage of the biometric template that is used to verify the authenticity of a user.

Biometric samples (or information extracted from these) are combined with the secret value to form a hardened template, which is then stored on a storage.

- *Fuzzy Commitment Scheme* – proposed by Juels and Wattenberg. Biometric data are treated as code words and XORed with the secret value to “lock” or retrieve the secret key.
- *Biometric Key Binding* – proposed by Soutar *et al.* Fingerprint images are transformed and information from stable regions is used to encode/decode the secret key.
- *IrisCode approach* – proposed by Hao *et al.* Secret key padded and XORed with IrisCode, then stored on a smart card.

Keys are re-generated using information obtained from a biometric sample. No hardened template is actually stored.

- *Online Handwritten Signatures* – proposed by Feng and Wah; uses El-Gamal key material. Dynamic features are quantized, concatenated and hashed to form the private key.
- *FingerCodes and Support Vector Machines* – proposed by Ramírez-Ruiz *et al.* Employs classifiers that are trained on test data to generate a binary keystring for each fingerprint.
- *FingerCodes and Fuzzy Extractors* – proposed by Tong *et al.* The key is hidden using n random points on a polynomial, which are then XORed with subparts of the FingerCode. The encoded points, along with a corresponding FingerCode, are later used to regenerate the key.

Random Sequence Generation using Fingerprints

- Biometric measurements are affected by random perturbations, which effectively represent random data.
- The idea: extract random data in form of a bit sequence.
- Aim: lightweight random sequence generation method, suitable for use in mobile devices equipped with fingerprint readers.

The Proposed Method (1)

- 1 Obtain a set of fingerprints

$\mathcal{F} = \{fingerprint_1, \dots, fingerprint_n\}$, where $n \geq 2$ is a system parameter.

- 2 Compute

$random = fingerprint_1 \oplus fingerprint_2 \oplus \dots \oplus fingerprint_n$.

- 3 Compute $uniform = h(random)$, where h is a suitable hash function.

The Proposed Method (2)

- Hash function employed as a provisional randomness extractor, as the bit sequence will likely have a non-uniform distribution.
- The extracted bit sequence can then be used directly, or fed into a PRNG as a seed.
- A different approach at generating random numbers from biometrics has been proposed a few years ago by Szczepanski *et al.*, based on continuous measurement of neural impulses. Requires large datasets for generation of pseudorandom bit sequences.

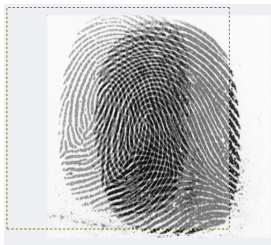
Entropy-Contributing Factors

- The overall entropy of the produced bit sequences is difficult to establish.
- Factors contributing to the entropy – introduced by the user, environmental conditions, or caused by the measurement device itself.
- Focus on user-induced error, specifically fingerprint shift and rotation.

Fingerprint Shift

- Fingerprint shift occurs when the user presents his finger to the reader in different positions during two or more consecutive measurements.
- Metric for description of fingerprint shift – *shift vectors*.
- Both automated and manual measurements have been performed on a dataset of 218 fingerprints.
- Vectors were calculated for every possible pair from the dataset, for a total of 23653 pairs.
- Vector frequencies and vector length frequencies (in intervals of length 5) were used to estimate Shannon and min-entropy of fingerprint shift.

Fingerprint Shift – Automated Measurement



- One fingerprint image is shifted on top of another, until the best pixel match is obtained. Image alignment implemented by RNDr. Vladimír Ulman from the Centre for Biomedical Image Analysis at FI MU.
- The shift vector describes the distance and direction of the shift of one pixel inside the fingerprint area between the two images.

Fingerprint Shift – Manual Measurement



- Coordinates of two reference points inside the fingerprint area of the image were manually measured.
- Measured coordinates were then used to construct shift vectors, while inner vectors were used for calculation of fingerprint rotation.

- Inner vectors were constructed from coordinates of reference points and used to calculate fingerprint rotation.
- Fingerprint rotation was expressed both in angles and rotation vectors.
- Measured angles and rotation vectors were rounded to degrees and pixels, respectively.

- Fingerprint shift has a larger impact than rotation – 13.344/10.877 bits Shannon entropy, 10.931/6.177 bits min-entropy (manual measurement/automated measurement)
- Even a partial information about the shift, like shift vector length, decreases the entropy dramatically – 4.766/2.969 bits Shannon entropy, 3.783/2.074 bits min-entropy
- Fingerprint rotation has smaller effect – 3.651/4.601 bits Shannon entropy, 2.770/3.604 bits min-entropy (degrees/angles)

Conclusion

- While the focus of current research efforts is on eliminating the randomness in biometrics, we show it is possible to use it for random number generation.
- Estimation of guaranteed overall entropy is difficult and not straightforward.
- Experiments using the shift vectors show that fingerprint shift has a significant impact on the overall security of the bit generation process.
- We are currently in the process of estimating entropy of fingerprint pressure and fingerprint reader noise. Future efforts will now concentrate on the approximation of the overall entropy the generated bit sequences contain, as well as possible extensions to the generator to accommodate further biometrics.