Random Profiles of Laser Marks

S. Saloomeh Shariati[1] François-Xavier Standaert[1] Laurent Jacques[1]
Benoit Macq[1] Mohamed Amin Salhi[2] Philippe Antoine[2]
[1]Information and Communication Technologies,
Electronics and Applied Mathematics (ICTEAM)
[2]Institute of Condensed Matter and Nanosciences (IMCN)
Université catholique de Louvain, B-1348 Louvain-la-Neuve
saloomeh.shariati@uclouvain.be

Abstract

In this paper, we propose a secure anti-counterfeiting solution based on the extraction of a unique identifier out of the random profile of laser marks that are engraved on the surface or in the bulk of physical objects. Given today's technology, the 3D profile of a laser mark can be considered uncloneable. Indeed, reproducing a mark would be so expensive that it thwarts any attempt to build a twin of a given mark. Actually, we rely on the resolution difference that can be achieved between the engraving which can be seen as pretty coarse, and the much more precise reading process. The solution we propose exploits these physical features in the design of a comprehensive anti-counterfeiting system based on existing tools. Experimental results demonstrate the feasibility of using the framework for real applications.

1 Introduction

The growing trade in counterfeit goods continues to affect every economy worldwide. Many companies use the so-called *overt* physical identifiers such as hologram and inks that visibly alter under light. Despite their simplicity, overt physical identifiers normally can be easily cloned [1, 2]. *Covert technology*, instead, apply identifiers that are not readily visible by naked eye. Invisible inks and *proprietary photonic inks* [1] are examples of covert physical identifiers. Another widely used covert physical identifier is Radio Frequency Identification (RFID) Tag that contains digital identifier used to authenticate the product [2]. Uncloneability is still a big concern for covert identifiers and if the digital identifier is cloned, the counterfeit product could easily cheat the anti-counterfeiting system.

Intrinsic random features of physical objects seem a good indicator of their unique identity; because they are random and there is no extra effort needed to add physical identifier to the object and they cannot be removed from one object or copied into another one. For example, almost all paper documents, plastic cards and product packaging contain intrinsic random features that can serve as an unique identifier [3, 4]. Nevertheless, generating identifiers using intrinsic random features of physical objects is highly dependant on the object material, which raises some difficulties in the design procedure. Furthermore, for some materials, these features may not be sufficiently random and/or robust against some likely changes such as paper shrinking and etc.

Another alternative is to adhere a tag containing sufficient physical random features to the product. In 2002 Pappu introduced optical Physical Uncloneable Function

SS and MAS are funded by the Walloon Region. LJ is the Postdoctrol Researcher and F.X.S is the Associate Researcher of the Belgian National Science Foundation (FNRS). SS thanks Dr. Philippe Bulen (ICTEAM/UCL) for sharing his experiments in the subject and help writing the paper.

(PUF) [5]. Optical PUF consists of a transparent material containing randomly distributed light scattering particles. It is attached to a physical object like a credit card and serves as an identification tag. For a more in-depth view of PUF and its use in cryptography, we refer to Pim Tuyls *et al.*'s book [6]. When using a dedicated tag as physical identifier, the authentication process should include an integrity check of the product/tag link to ensure it was not broken.

In our method, we use the random 3D profile of laser marks engraved either on the surface or in the bulk of material as a Physical Uncloneable Function. The detail profile of laser marks is practically uncloneable since it cannot be reproduced or at the cost of such an expensive manufacturing process that it renders it worthless. This method provides some advantages over current methods: given the tiny size of the marks (in range of micrometer), the density of the random information generated out of laser marks is high. Furthermore, it offers the benefits of being more robust against normal distortion like ageing. The main contribution of this paper is to introduce Laser-written PUF (or LPUF) and propose a secure anti-counterfeiting system based on this PUF. The rest of the paper is organized as follows: Section 2 briefly describes the proposed anti-counterfeiting system. Section 3 presents the system ingredients and gives a detailed description of the main components, i.e. LPUF and identifier extractor using binarized robust Gabor coefficients of the LPUF images. Finally, Section 4 demonstrates the applicability of the proposed system by providing experimental results on a database of LPUFs.

2 Description of Anti-Counterfeiting Scheme

In this section, a general view of the proposed anti-counterfeiting system is sketched (Fig. 1). The scheme is split in two different parts. The first one (registration) is performed once on the object before it is released on the market while the second step (verification) can be performed each time someone wants to be convinced the good is a genuine one. The components of the scheme will be discussed afterwards.

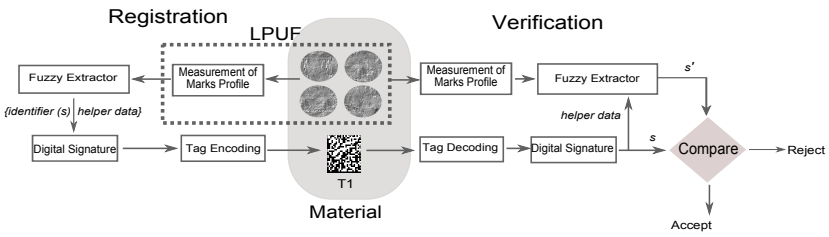


Figure 1: Anti-counterfeiting Scheme based on LPUF.

First, during the registration phase, a unique physical identifier is built from the object and embedded on it as follows:

- Laser marks are engraved on the surface or in the bulk of the object material.
- The 3D profile *(or topography)* of one or more engraved marks are accurately measured by means of optical interferometry.
- A string of bits consisting of the *identifier (s)* and the *helper data* is generated out of 3D profile of the selected marks.(The exact descriptions of these terms are given in Section. 3.2)
- The string of extracted bits is signed by the private key of authority that forms the marks signature.

- The signature is encoded into a tag T1 and engraved into the object by means of conventional laser marking (e.g. Datamatrix).

Second, in order to check whether the object is a genuine one or not, the verification phase performs as follows:

- The 3D profiles of the selected laser marks are accurately measured again.
- Tag T1 is scanned, decoded and decrypted by public key of authority that provides the *identifier* and the *helper data*.
- The new identifier of the marks is built out of their 3D shape with the aid of the *helper data*.
- If both *identifiers* (*s* and *s'*) match, the object is accepted as the genuine one; otherwise it is rejected as a fake.

3 Anti-Counterfeiting Ingredients

Proposals for the system ingredients are given in the present section. We mention that these choices are not expected to be optimal but they provide a solution that reasonably fits the requirements of our target application. Hence, they could be improved or tuned for other applications. Due to the significance of the LPUF and identifier extractor in our contribution, we pay a particular attention in describing them in detail. And for other ingredients, namely Digital Signature and Tag En-/De- Coding, we rely on existing solutions and references.

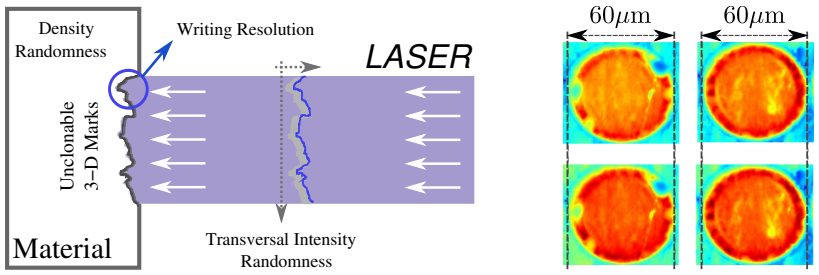
3.1 Laser-written PUF

Physical systems that are produced by an uncontrolled production process, i.e. one that contains some intrinsic randomness, turn out to be good candidates for PUFs. In this paper, as a technological achievement of the TOMO3D project [7], we propose a PUF based on the 3-D profile (or *topography*) of laser marks, with a diameter of 60μm, engraved on the surface of a physical object.

The uncontrollability of the laser marking process is mainly caused by laser instability and characteristic of the object material. The mark profile shows therefore a spatial variability that cannot be reproduced, at least with reasonably inexpensive technology. Fig. 2(a) shows the laser engraving principle illustrating the two main sources of randomness. To exploit this randomness, it requires to measure the profile with a (reading) resolution finer than the laser beam diameter (writing resolution). In our scheme, this reading (not illustrated) is performed by White Light Interferometry (WLI) that achieves a sub-micrometer transverse resolution and a nanometer longitudinal resolution [8]. Fig. 2(b) is an illustration of the profiles of two marks engraved in identical conditions (as far as controllable by engraving method) measured by WLI method. The measurement is done twice for each mark. Each column corresponds to the measured profiles of the same mark. The comparison of the four images clearly indicates that the profiles of the two marks are far more different than the profiles of two measurements of the same mark. In other words, the accuracy of the measurement is well adapted to pinpoint the differences between the profiles of marks.

3.2 Fuzzy Extraction of LPUF Images

The simple image of a PUF cannot be used as an identifier of the marked object. First, different observations of the same PUF are subject to noise (e.g., for LPUFs, due to



(a) (b)

Figure 2: (a) Laser engraving principle. (b) Topographic profiles of two different laser marks (left/right) engraved in identical conditions. Top and bottom rows are two different WLI observations.

small variations in the measurement setup or because of slight mark degradations) and therefore they cannot be perfectly reproduced. Second, any observation needs to be reduced and digitized in a limited binary string, or fingerprint, for further comparison, storage or transmission of data for object authentication. Finally, the extracted fingerprints from a set of similar objects may not produce the uniform distributions required by most of the cryptographic applications. Turning noisy physical information into cryptographic keys can be achieved using fuzzy extractors [9]. A fuzzy extractor reliably extracts nearly uniform randomness from its noisy input; the extraction is error-tolerant in the sense that the output will be the same even if the input changes, as long as it remains reasonably close to the original. In this Section we adapt the scheme proposed by [9, 10] to our special database. The whole pipeline follows a Fuzzy Extractor procedure [9] composed of a Registration stage and a Verification stage, as summarized in Fig. 3 on the left and on the right sides respectively.

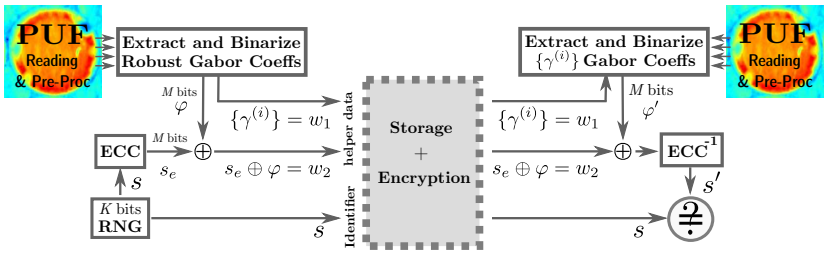


Figure 3: LPUF Fuzzy Extractor: registration stage (left) and verification stage (right).

Image Preprocessing: A WLI observation is obtained from the PUF with some preprocessing aiming at reducing observation noises corresponding to the changes in the relative position of the object and camera. We use a synchronization scheme based on the boundary of each mark. First, to avoid oversegmentation, we use gray scale morphological filtering to simplify the image and remove small details. Then, the boundary detection tool is applied to the image and the exact area of each mark is extracted from the original image.

Registration Stage: The registration stage consists in the reduction of a preprocessed image $I \in \mathbb{R}^{N_1 \times N_2} = \mathbb{R}^N$ of $N = N_1 N_2$ pixels into a robust string $\varphi \in B^M = \{0,1\}^M$ of M bits, or *fingerprint*, followed by the encoding of this reduction with an *identifier* for further verification into a *helper data*.

Similarly to [10], the reduction relies on the use of 2-D Gabor filters. These are elementary functions $g_\gamma(x) \in \mathbb{R}$ defined on $x = (x_1, x_2) \in \mathbb{R}^2$ and parameterized by $\gamma = (a, \nu, b) \in \mathbb{R}_+ \times \mathbb{R}^2 \times \mathbb{R}^2$ in the following way

$$g_\gamma(x) = \tfrac{1}{a\sqrt{2\pi}}\ \sin(\nu \cdot (x-b)) \exp(-\tfrac{1}{4a^2}\|x-b\|^2), \tag{1}$$

with $u \cdot v = u_1 v_1 + u_2 v_2$ and $\|u\|^2 = u \cdot u$ for $u, v \in \mathbb{R}^2$. The function $g_\gamma(x)$ is the product of a plane wave with wave vector $\nu \in \mathbb{R}^2$ and a Gaussian with variance (or *scale*) $a \in \mathbb{R}_+$ centered on $b = (b_1, b_2) \in \mathbb{R}^2$. It is a efficient directional feature detector used in many image processing applications [11].

The image identifier of I is built from its Gabor coefficients, i.e. from the values

$$G(\gamma) = \langle g_\gamma, I \rangle = \int_{\mathbb{R}^2} \mathrm{d}^2x\ g_\gamma(x) I(x), \tag{2}$$

where the last integral is well approximated by a finite sum for a larger than few pixels.

In our experiment, we restrict γ to a finite set of values $\Gamma_{a,\nu_0,\Delta} \subset \mathbb{R}_+ \times \mathbb{R}^2 \times \mathbb{R}^2$ defined as

$$\begin{aligned} \Gamma_{a,\nu_0,\Delta} \ = \ \big\{(a, \nu_\ell, b_m) : \quad & \nu_\ell = \nu_0(\sin\theta_\ell, \cos\theta_\ell),\ \theta_\ell = 2\pi\ell/L,\ 0 \le \ell < L, \\ & b_m = (m_1\Delta, m_2\Delta),\ 0 \le m_i < \lfloor N_i/\Delta \rfloor, i \in \{1,2\}\big\}. \end{aligned} \tag{3}$$

The size of $\Gamma_{a,\nu_0,\Delta}$ is $\#\Gamma_{a,\nu_0,\Delta} = L\lfloor N_1/\Delta \rfloor \lfloor N_2/\Delta \rfloor$, and it induces the coefficient set $\mathcal{G}_{a,\nu_0,\Delta} = \{G(\gamma) : \gamma \in \Gamma_{a,\nu_0,\Delta}\}$ of same size. The effects of a, ν_0 and Δ are evaluated in the experimental tests of Section 4.

The M components of the fingerprint $\varphi \in B^M$ of the image I are simply given by $\varphi_i = Q[G(\gamma^{(i)})]$, where $Q[\lambda]$ is the 1-bit quantizer equals to 1 if $\lambda > 0$ and 0 else, and $\gamma^{(i)}$ is the parameter vector of the i^{th} strongest value* of $\mathcal{G}_{a,\nu_0,\Delta}$.

The M parameter vectors of $\{\gamma^{(i)} : 1 \le i \le M\}$ constitutes the first part of the *helper data* and they can be efficiently encoded into a string w_1 of $M_\gamma < \#\Gamma_{a,\nu_0,\Delta}$ bits.

In parallel, an identifier s of $K < M$ bits is generated by a Random Number Generator (RNG) and *extended* into a string $s_{\text{e}} \in B^M$ by an Error Correcting Code encoding (ECC) of error-correction capability $T < K < M$. Finally, φ is XORed ($\oplus$) with s_{e} to form $w_2 = s_{\text{e}} \oplus \varphi \in B^M$. The full helper data of $M + M_\gamma$ bits is composed of (w_1, w_2). This data constitutes, together with the identifier s, the information required to authenticate the object. In our anti-counterfeiting scheme (See Fig. 1), this data is signed, encoded and embedded in the Tag T1.

Verification Stage: During the *verification* stage, the PUF is reobserved into a image $I' \in \mathbb{R}^N$ undergoing the same preprocessing and extraction of Gabor robust components. From the helper data, w_1 is decoded into the M parameter vectors $\gamma^{(i)}$ to compute $\varphi'_i = Q[\langle g_{\gamma^{(i)}}, I' \rangle]$. After XORing this later with w_2 and sending the output to the ECC decoder (ECC^{-1}), a final K-bits string s' is produced. Since $(u \oplus v) \oplus v = u$ for any two strings $u, v \in B^M$, if the ECC capability T is set higher than the maximal hashing distortion of different observations of the same PUF, and if we do observe the same object with the same PUF, then the system guarantees $s = s'$ [9].

To avoid confusion, it is worth clarifying that in this work, fingerprint denotes φ or φ' bit strings built from the physics (during registration or verification), whereas identifier stands for the K-bit string s generated from a RNG. The properties of the proposed method are evaluated in Section 4.

*In absolute value sense.

3.3 Digital Signature

Digital signature is a well-studied field in cryptography and a variety of solutions are available for different applications. Some well-known schemes are: RSA signature, Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) [12]. Based on the size of the key and security requirements of the system, one of the mentioned schemes can be used to sign laser marks identifier.

3.4 Tag En-/De- Coding

There are a large number of existing visual codes such as 1-D or 2-D Barcode, Aztec Code, Data Matrix and so on [13]. Out of these, the Datamatrix seems a good candidate for our application thanks to its high density.

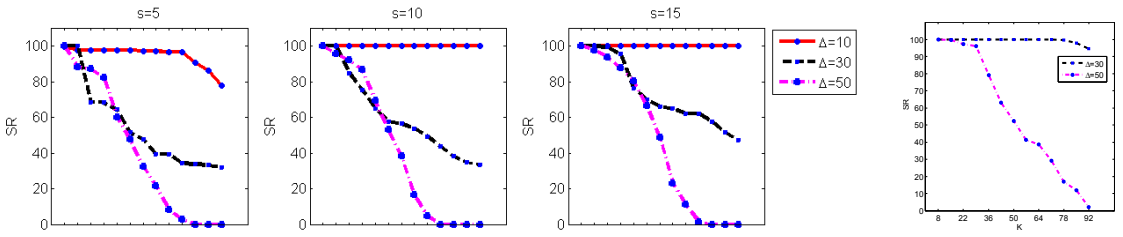
4 Experimental Results and Analysis

4.1 Robustness

We need to ensure that a mark will provide the same identifier through different scanning. So, essentially we have to evaluate the robustness of the framework against misalignment and noises that usually happen during the image acquisition process. For that, an automatic scanning procedure was set up to provide different sets of images and we have recorded a database $\mathcal{S} = \{I_{pq} = \tau_p + n_{pq},\ 1 \leq p \leq P,\ 1 \leq q \leq Q\} \subset \mathbb{R}^N$ of $P = 20$ different marks τ_p of $N = 115\,600$ pixels (i.e. 340×340) observed $Q = 10$ times each in I_{pq} with an unknown noise $n_{pq} \in \mathbb{R}^N$. Notice that each image has been preprocessed to reduce misalignment by selecting only the framed region of each mark. We have also renormalized all images so that $\|I_{pq}\| = 1$. For each of 20 mark images, the registration phase is performed once with one of the scan to build the uncloneable identifier and its corresponding helper data by the method described in Section 3.2. Then, the verification phase is performed for the remaining 9 scans. Robustness is estimated through the success rate that is simply computed as the ratio between the amount of correctly extracted identifiers and the amount of measures.

Apparantly, we deal with the trade-off between robustness and randomness. However, we focus our attention to the cases where enough entropy, extracted from the fingerprint, can be robustly recovered. As the entropy is upper bounded by the number of bits extracted, we aim at the longest possible fingerprint that can be recovered with high confidence. To this end, in order to select the extraction parameters, we used the scheme excluding ECC. We first examined group of wave vector ks and finally we select $\omega_0 = \pi/3$ and $t = 4$ (See Eq. 3). Then, we examined the success rate for different values of the parameters, namely s, the variance of the gaussian, Δ, the filter interval (in pixels) and M, the number of robust Gabor components. An excerpt of the results obtained are shown in Fig. 4(a) where the success rate of exactly reproducing fingerprints versus M are given for different choices of s and Δ.

Notice that for fixed Δ and s, increasing the fingerprint's length, M, leads to a reduction of SR (because of interfering more noise components). On the other hand, by decreasing s, we focus on more details of mark image (higher probability of noise incidence)and we see that robustness is increasing. According to the results shown in Fig. 4(a) , $s = 15$ seems an appropriate choice showing the highest SR. We then investigate the success rate after the ECC, i.e. BCH(M, K, T), where M is set to 127, K is the length of the identifier and T is the error-correction capability of the ECC code (Fig. 4(b)). For each Δ, maximum M is selected providing that success rate is higher than 90 % In Section 4.2, we compare the entropy of two cases: $(\Delta = 30, M = 90)$ and $(\Delta = 50, M = 30)$.



(a) (b)

Figure 4: (a) Success rate and entropy versus M for different s and Δ before ECC. (b) Success rates after BCH $(127, K, T)$ for $\Delta = 30$ and $\Delta = 50$.

4.2 Entropy

We need to estimate the real amount of information contained in each mark and then determine how many physical objects can be identified by each laser mark. For that, we have recorded another database of $\mathcal{S}' = \{\tau_p + n_p \in \mathbb{R}^N,\ 1 \leq p \leq P'\} \subset \mathbb{R}^N$ of $P' = 1000$ different marks, each of them scanned once and run well-known entropy estimators to evaluate how much randomness is in the physical fingerprints (assuming the noise n_p negligible). The fingerprints need to be unique for every physical object to prevent copy-paste attack. The basic idea behind utilized entropy estimators is that it should not be possible to significantly compress the bit sequence when it behaves randomly. The results obtained from *Maurer*'s test [14] and the *Context Tree Weighting* (*CTW*) methods [15] are shown in Table 1. It is done for two sets of $\{\Delta = 30, M = 90\}$ and $\{\Delta = 50, M = 30\}$ as discussed in Section 4.1.

Table 1: Estimated entropy (bits per fingerprint).

	$\Delta = 30, M = 90$	$\Delta = 50, M = 30$
Maurer	$90 \times 0.64 = 57.6$	$30 \times 0.73 = 21.9$
CTW	$90 \times 0.65 = 58.5$	$30 \times 0.82 = 24.6$

In case of $(\Delta = 30, M = 90)$, a fingerprint of approximately 57-bit can be built from each laser mark profile. This can be further increased by using more than one mark.

4.3 Security Analysis and Uncloneability

In the proposed anti-counterfeiting system, we avoid *forgery* at two different levels: first the attacker cannot reproduce a physical structure (laser marks) that builds the same identifier, and second if he attempts to introduce his own laser marks with own randomness, he does not have the correct private key of the authority to generate the correct signature. In general, according to the object to be protected, it is sufficient that the cost of forgery per object is roughly more than the price of the genuine object. We may use this lower bound of forgery cost as a criterion to estimate the resolution needed to engrave laser marks (writing resolution). Then, it suffices to measure the profile a much higher resolution than the engraving resolution. The ratio between the resolutions of writing and reading is dependent on the amount of entropy needed. Evaluation of the relation between the unclonability of the laser marks and the read/write resolution of current technologies is an interesting scope for further research.

5 Conclusion

In this paper, we have presented a complete method to utilize random characteristic of the laser mark pattern to produce Laser-written PUF. Since laser engraving can be performed on various types of material, it will have many advantages over current anti-counterfeiting methods: laser engraved marks can serve as complex PUF as the density of the random information is high (about 57-bits with a 60 micron diameter). This offers the possibility to protect small objects or to be combined with other authentication methods.

References

[1] S. Bastia. Next generation technologies to combat counterfeiting of electronic components. *IEEE Trans. on Components and Packaging Tech.*, 25:175–176, 2002.

[2] C. N. Chong et al. Anti-counterfeiting with a random pattern. In *Int. Conf. on Emerging Security Information, Systems and Tech.*, pages 146–153, 2008.

[3] J. Buchanan. Fingerprinting documents and packaging. *Nature*, page 475, 2005.

[4] P. Bulens, F.-X. Standaert, and J.-J. Quisquater. How to Strongly Link Data and its Medium: the Paper Case. *To appear in IET Information Security*, 2010.

[5] R. Pappu et al. Physical one-way functions. *Science*, 297, 2002.

[6] P. Tuyls, B. Skoric, and T. Kevenaar. *Security with Noisy Data*. Springer, 2007.

[7] TOMO3D project-WIST2 Program contract n°616444 Wallon Region-Belgium.

[8] D. Malacara. *Optical Shop Testing*. Wiley-Interscience, second edition, 1992.

[9] Y. Dodis et al. Fuzzy extractors: How to generate strong secret keys from biometrics and other noisy data. In *Eurocrypt'04*, pages 523–540, 2004.

[10] P. Tuyls et al. Secure key storage and anti-counterfeiting. *Springer*, pages 255–268, 2008.

[11] S. Mallat. *A Wavelet Tour of Signal Processing: The Sparse Way*. Academic Press., 3rd ed edition, Dec. 2008.

[12] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.

[13] Unibar inc. bar code page., `http://www.adams1.com/stack.html`.

[14] J.-S. Coron and D. Naccache. An accurate evaluation of maurer's universal test. *Lecture Notes in Computer Science*, 1556:57–71, 1998.

[15] F. Willems, Y. Shtarkov, and T. Tjalkens. The context-tree weighting method: Basic properties. *IEEE Trans. on Information Theory*, 41:653–664, 1995.