Randomized resonators as uniquely identifiable anti-counterfeiting tags

B. Škorić[1], T. Bel[1], A.H.M. Blom[2], B.R. de Jong[2], H. Kretschman[1], and A.J.M. Nellissen[2]

[1] Philips Research Europe
[2] Philips Applied Technologies

Abstract. We discuss how LC circuits with randomized properties can be used as anti-counterfeiting tags. Work in progress is presented. Test circuits made using thin film technology easily achieve 20 to 30 bits of identification capacity. We describe our experimental setup, the radiofrequent response curves, and the stable features that can be extracted from them.

1 Introduction

1.1 The counterfeiting problem

Counterfeiting is a serious problem affecting many areas of industry. According to some estimates [7], 9% of all goods in the market is counterfeit. This number is even bigger if parallel trading, brand misuse and look-alike products are included. The growing popularity of manufacture outsourcing will make the situation worse.

The severity of the problem is reflected in the large number of anti-counterfeiting (AC) technologies: security inks, gratings, holograms, magnetic dots, fluorescent and phosphorescent materials, watermarks, rare chemicals, electromagnetic codes etc. The AC arena is in constant flux as counterfeiters succeed in breaking protections and new techniques are introduced to replace them. In this arms race, it is important to have cheap authenticity markers that can be generically applied to broad ranges of products.

Radio Frequency Identification (RFID) is being employed as an AC measure, for instance by Pfizer in its Viagra bottles sold in the US since 2005. With the boost given to RFID by the Food and Drug Administration in the US and Article 18 of Regulation 178/2002/EC in Europe, this technology will see a big growth. However, in many applications RFID tags are too costly for item-level tagging. A very promising alternative is the use of so-called chipless RFID [5], i.e. completely passive tags that do not contain an integrated circuit.

It must be noted that (chipless) RFID is a track-and-trace technology vulnerable to cloning of the tags.

1.2 The role of chaotic physics in anti-counterfeiting

As noted by Simmons in [9], there is a fundamental problem with most AC technologies. An authenticity marker is associated with a product, e.g. a watermark in a banknote. *The marker is the same in every product.* Hence the marker is clonable by default, which defeats its purpose.

Simmons proposed a completely different AC approach. The authenticity feature should be something that cannot be controlled by its maker. (We call this property 'manufacturer-resistance'.) An example of such an unclonable feature could be the fiber structure in a piece of paper. It can be thought of as the 'biometric' of an object. Ideally, the feature is intrinsic to the product that has to be protected. When such a feature is not present in the product itself, the product can be tagged with a marker that does possess an unclonable feature. Preferably, the marker is attached irremovably, i.e. any attempt to remove the marker should damage the unclonable feature.

An *enrolment* step is required, in which a measurement is done of the physical feature. The result of the measurement is compactly summarized in so- called *enrolment data*. The enrolment data has to be stored in a tamper-proof way. One possibility is storage in a secure database. Another possibility is to store the helper data next to the product, e.g. as a barcode, digitally signed by a trusted authority. Note that the enrolment data is not secret.

Verification consists of the following steps

- Read the enrolment data associated with the product. Check the authenticity of the enrolment data. If the data is not authentic (e.g. the digital signature does not match) consider the product to be counterfeit.
- Perform a new measurement of the physical feature.
- Compare the result of the measurement to the enrolment data. If the difference between the two is too large, consider the product to be counterfeit.

The best manufacturer-resistant features are those that result from random mixtures and interference effects[1]. Other good features result from local measurements that are very sensitive to random microscopic details. In general, classical 'chaos' is needed.

Manufacturer-resistance is closely related to Physically Obscured Keys (POKs) [3] and Unclonable Physical Functions (PUFs) [8], although the security objectives are different. For an overview we refer to [12].

1.3 Related Work

In the past few years several papers have appeared on the use of randomness for anti-counterfeiting. The company Ingenia [1] has developed a method of uniquely recognizing the structure of paper using reflected laser light. In [10] it

[1] True unclonability exists in quantum physics: an unknown quantum state cannot be cloned. However, as long-term quantum coherence is problematic in practice, one is forced to use classical physics.

was described how RFID tags can be made unclonable by applying a randomized coating [11]. Microsoft has published on two types of randomized identifier: one based on a mixture of glass fibers [6] and one based on the radio frequency response of a piece of metal [2]. In [4] a method was described to uniquely identify Field-Programmable Gate Arrays (FPGAs) using random intrinsic properties.

1.4 Organization of this paper

In this paper we present a new type of anti-counterfeiting tag: randomized resonator circuits that can be read out wirelessly. This represents a special case of chipless RFID where the identifier is determined by the resonance frequency of the circuit.

In Section 2 we describe the circuits. In Section 3 we treat the detection method. Experimental results are shown in Section 4. In Section 5 we briefly discuss the issue of manufacturer resistance.

2 Randomized resonator circuits

2.1 Theory

A simple resonator circuit (also known as 'tank circuit' or LC-circuit) consists of a coil (with self inductance L) and a capacitor (with capacitance C) connected in series. The complex impedance of these components at frequency ω is $i\omega L$ and $1/(i\omega C)$, respectively[2]. The resonance frequency, defined as that frequency where the absolute value of the impedance has a minimum, is given by

$$\omega_{\mathrm{res}} = \frac{1}{\sqrt{LC}}. \tag{1}$$

When placed in an electromagnetic field whose magnetic part couples well into the coil, the circuit will absorb a frequency-dependent amount of power from the field, with a peak at ω_{res}.

The inductance of a coil is a complicated function of the coil geometry. The capacitance of a parallel plate capacitor is given by

$$C = \frac{A\varepsilon_0\varepsilon_r}{D}, \tag{2}$$

where A is the plate area, ε_0 the dielectric constant of the vacuum, ε_r the relative dielectric constant of the material between the plates, and D the separation between the plates. From (1) and (2) it is clear that the resonance frequency is affected by changes in A, ε_r, D and the coil shape. Random resonance properties can be obtained by making any of these parameters random. For technical reasons we have used deterministic coil and capacitor shapes[3]. We also did not

[2] Here Ohmic resistances are ignored

[3] Randomization has the potential danger of causing shorts and other defects. However, this problem may be overcome by careful design.

randomize ε_r. A dielectric mixture as used in [11], when placed between large (>50μm) plates, loses much of its randomness due to averaging effects. We chose to randomize the thickness D instead.

We wish to be able to distinguish between many different LC circuits. In analogy with biometrics we define the *identification capacity*, expressed in bits, as

$$C_{\rm ID} = \log_2(\#\text{distinguishable circuits}). \tag{3}$$

For large scale systems with millions of distinct tags, $C_{\rm ID} > 20$ is needed. The difficulty of cloning a tag grows with the number of identifier bits (see Section 5). On that ground one may even require $C_{\rm ID} > 30$.

The $C_{\rm ID}$ of an LC-circuit is determined by the signal to noise ratio (SNR), where 'signal' refers to the width of the band where the resonance can lie, and 'noise' is the experimental uncertainty in the location of the resonance peak. The available frequency band is limited on the low side by the small tag size and the smallest value of D that can still prevent shorts. The band is in principle unlimited at the high-frequency side, but in practice skin effects start spoiling the measurements above several GHz. The noise in the peak location depends on the signal strength, which in turn depends on the peak width $\triangle\omega$, which is of order R/L, with R the Ohmic resistance of the circuit. Hence, in order to get a sharp peak we need to make Ohmic losses as small as possible. (The so-called 'Q factor' has to be high.) The reproducibility of measurements is affected by various sources of noise, such as temperature differences, bending, moisture etc. It is important to keep these under control.

2.2 The basic circuit

We made test circuits using thin film deposition on 6" glass wafers. The basic circuit, comprising only a single coil, looks as follows. It contains two conductive layers separated by dielectric. The lower layer is 1μm thick Al, containing only a capacitor plate. The upper layer is 10μm thick Cu, containing the opposite capacitor plate and a coil. The dielectric consists of a 100 nm layer of SiO_2 and a randomized layer of HPR504 resist. Here 'randomized' means that the thickness locally varies between zero and 1μm; the correlation length is shorter than the distance between circuits on the wafer, so that knowledge of one capacitance still leaves neighbouring capacitances unpredictable. The random thickness pattern is made by exposing a uniform layer of resist to ultraviolet light through a randomized mask. (The mask contains a liquid with carbon particles that settle in a random pattern. With each new exposure, the liquid is shaken and the particles settle in a new configuration.) The statistical thickness distribution is not completely uniform, but close enough to give high entropy.

The purpose of the SiO_2 layer is to prevent shorts at those locations where the resist gets completely removed.

The area of the coil is slightly less than 1mm^2. In order to have a good antenna functionality, we positioned the coil at the perimeter of the available

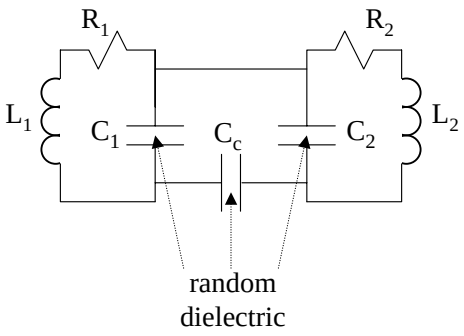

Fig. 1. *Schematic picture of two coupled oscillators with random coupling capacitance* C_c.

area. Additional coil windings closer to the center would not improve the signal strength.

The cost of the circuits is of course very important for their deployment as AC tags. Cost estimates indicate that the use of LCD (Liquid Crystal Display) manufacturing equipment can bring the price of the LC circuits below 0.1 cent/mm^2.

2.3 Coupled circuits

In practice, a single LC-circuit cannot achieve an identification capacity of 20 bits (see the requirements in Section 2.1 and the experiments in Section 4.3). A higher C_{ID} can be obtained by using multiple LC-circuits. However, if done in a trivial way, this opens the possibility for an attacker to clone all the LC-circuits independently, which is not more difficult than cloning a single LC-circuit. A more secure way of combining multiple circuits is to couple them. Then the response curve depends on the parameters of all the components in a nontrivial way; any attempt at cloning will have to reproduce all neighbouring components correctly.

An example of a coupled circuit is shown in Fig. 1. Note that this circuit has three capacitors, but only two coils. Since the tag area is mostly taken up by the coils, this architecture has a high 'C_{ID} density' (bits/mm^2). More than two coils can be connected if necessary.

3 Detection method

3.1 Measurement setup

We used a HP8753E network analyzer to measure the one-port S_{11} scattering parameter (basically the complex impedance $Z(\omega)$) of LC-circuits. We constructed a short extension mounted directly onto the 50Ω coaxial output of the impedance

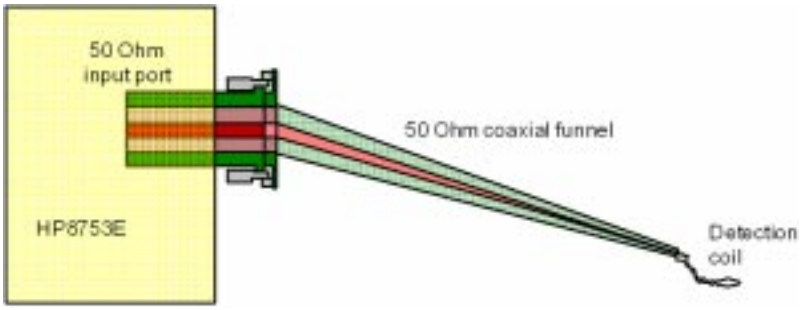

Fig. 2. *Connection of the pickup coil to the network analyzer socket.*

test socket of the HP8753E. The extension allows the pickup coil to be soldered to the setup. This pickup coil is a single-winding coil of 1 mm diameter, made with 355 micron posyn winding wire. The leads are twisted from the single-turn coil up to the solder joints on the extension, over a length of approximately 6mm. This geometry has a resonance at 2 GHz, limiting the maximum scan frequency to about 1.8 GHz.

With this construction, the LC-circuits, which comprise coils of area of order 1mm^2, can be detected up to a distance (normal to the plane of the circuit) of 1.5 mm. The analyzer can perform a broad frequency scan with low frequency resolution, useful for roughly locating resonance peaks, or a 'zoomed in' scan of a more narrow band, with a frequency resolution of 0.1 MHz.

The network analyzer suppresses noise by subtracting from each measurement $Z(\omega)$ a calibration trace $Z_0(\omega)$, made far away from LC-circuits.

It is of course infeasible to use an expensive network analyzer for anti-counterfeiting of consumer goods. A dedivated reader device has to be developed. This is still work in progress. The estimated cost of such a reader is around $100.

3.2 Stable features

Without giving a derivation we mention the following theoretical result for 'ideal' components. When the pickup coil is positioned directly above one of the coils (without loss of generality denoted as coil '1') in a coupled two-coil circuit (see Fig. 1), then theory predicts the following response,

$$Z(\omega) - Z_0(\omega) = -Z_{01}^2 \frac{Z_2 Z_c - Z_{2c}^2}{Z_1 Z_2 Z_c - Z_1 Z_{2c}^2 - Z_2 Z_{1c}^2 - Z_c Z_{12}^2 + 2 Z_{12} Z_{1c} Z_{2c}}. \quad (4)$$

In this expression Z_{01} stands for the mutual impedance between the pickup coil and coil '1'; in the ideal case of purely inductive coupling it is given by $Z_{01} = i\omega L_{01}$, with L_{01} the mutual inductance. Hence L_{01}^2 appears as a number multiplying the strength of the signal $Z - Z_0$.

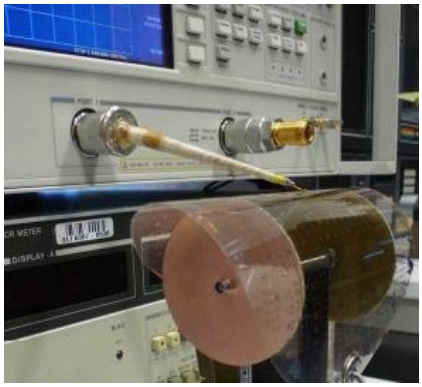

Fig. 3. *Photo of the measurement setup for bending tests. Note that only the pickup part of the twisted wire can be seen; the rest is shielded off by a conical sheet of copper hardened with epoxy. The transparent flexible substrate contains the circuits.*

The other quantities in (4) are expressed as follows in terms of the component properties in Fig. 1: $Z_j = R_j + i\omega L_j + 1/(i\omega C_j)$, $j \in \{0, 1, 2\}$; $Z_c = [C_1^{-1} + C_2^{-1} + C_c^{-1}]/(i\omega)$; $Z_{1c} = -1/(i\omega C_1)$; $Z_{2c} = -1/(i\omega C_2)$; $Z_{ab} = i\omega L_{ab}$.

A graph of $|Z - Z_0|$ according to (4) is given in Fig. 4. In general there are two resonance peaks.[4]

We briefly comment on the reproducibility of the impedance measurements. In practice the calibration $Z \to Z - Z_0$ does not get rid of the pickup coil properties perfectly. Consequently, the magnetic coupling parameter L_{01}, which is experimentally hard to control, affects the shape of the response curve in other ways than just being an amplitude multiplier. The question then is how to extract robust, reproducible features from $Z(\omega)$. It turns out that the location of the upward peaks depends only very weakly on L_{01}. The occurrences of an upward peak basically correspond to a vanishing of the denominator in (4), which is independent of L_{01}. Without giving any details, we mention that the resonance frequencies are found as the solutions of a quadratic[5] equation in ω^2, where it does not matter to which of the circuit coils the pickup coil is coupled.

Hence, we use the locations of the upward peaks as stable features by which we can distinguish circuits from each other. However, this only corresponds to two different functions of the random parameters in the circuit, while there are *three* random capacitances. Additional distinguishing information can be obtained by looking at other stable features of the response. We have observed that the ratio of peak heights is fairly stable, but this has not been fully explored yet.

[4] The case of a single LC-circuit is obtained in the limit ($C_c \to 0, L_{12} \to 0$) and yields $Z = Z_0 - Z_{01}^2/Z_1$.

[5] In the case of n coupled coils, there are n peaks whose locations are the solutions of an n'th order polynomial equation.

4 Experimental results

4.1 Response curves

We have measured response curves from various types of coupled and uncoupled LC-circuits. The response curves look very similar to the 'ideal-component' theoretical curves. An example is shown in Fig. 4. Notice that the pickup coil directly probes one of the two coils (giving rise to the highest peak in the figure) while it can access the other coil, and hence the other resonance, only through the capacitance C_c. If $C_c \ll C_1$, then probing coil 1 will hardly excite coil 2; the second peak will have a low amplitude. Similarly, if $C_c \ll C_2$, then probing coil 2 will hardly excite coil 1.

Signals can be obtained up to a distance of 1.5 mm between the pickup coil and the circuit. At larger distances the noise makes it impossible to see resonance peaks.

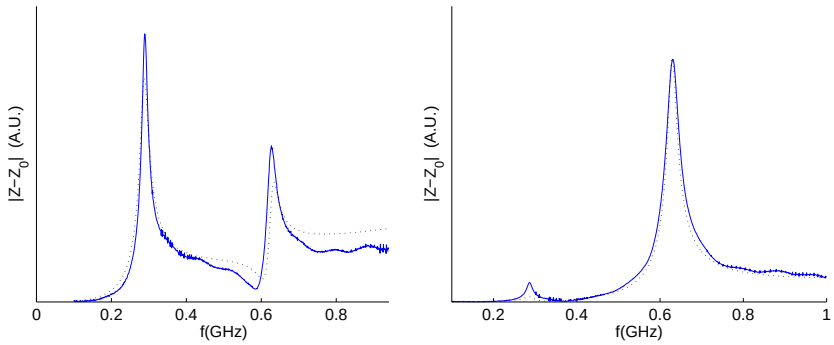

Fig. 4. *Measured response* $|Z - Z_0|$ *(solid lines) of a two-coil circuit, plotted together with theoretical curves (dotted lines). Left: pickup coil coupled to coil '1'. Right: pickup coil coupled to coil '2'. The parameter values of the theoretical curves are* $(2\pi)^{-1}/\sqrt{L_1 C_1} = 0.35\,GHz$, $(2\pi)^{-1}/\sqrt{L_2 C_2} = 1.3\,GHz$, $C_1 : C_2 : C_c = 15 : 1 : 5$, $L_{12} = -0.02\sqrt{L_1 L_2}$.

4.2 Robustness tests

Repositioning noise. We have tested how much noise there is in the measured resonance frequency of a single-coil circuit upon repositioning the circuit in the measurement setup. This was done in two ways: (i) repositioning in the xy-plane, i.e. the plane of the circuit. (ii) repositioning in the x, y and z direction. The nominal distance between the circuit and the pickup coil was 0.5mm. Each measurement was repeated 30 times, at constant temperature. We focused on the location of the upward peak.

It turns out that in case (i) the standard deviation of upward peak frequencies is less than 0.15 MHz for low frequency peaks, and less than 0.3 MHz for high frequency peaks. When vertical repositioning errors are considered as well, these numbers change to 0.3 MHz and 1 MHz, respectively.

We conclude that resonance frequencies can be located with high accuracy even when the alignment of the circuits in the setup is not perfect. This is in sharp contrast with the RF tokens of [2], which need to be carefully repositioned.

Temperature effects. We studied the effect of temperature between 25°C and 75°C. The temperature of a glass wafer with circuits on it was controlled from below by a hotplate. The wafer was covered with 2mm of foam on the top side to prevent cooling. The location of the upward peak was measured for a number of different single-coil circuits, with steps of 1°C.

As expected, the resonance frequency is a monotonously decreasing function of temperature. (Thermal expansion causes both L and C to increase.) The effect is quite small and hence can be considered linear. The magnitude of the frequency change is 65 ppm/K. For instance, a peak that lies at 1GHz at room temperature shifts by -3MHz at 75°C. We conclude that deviations due to temperature are easy to compensate.

Bending. We manufactured circuits on a flexible substrate (foil) for the purpose of bending tests. The foil was bent by placing it on a pair of discs and weighing down the edges of the foil (see Fig. 3). Discs were used with a radius r of 6mm and larger. At each bending radius resonance frequencies were determined. The measurements showed that there is no monotonous relationship between the frequency and the amount of bending. Sometimes the frequency difference is positive, sometimes negative. The magnitude of the effect is of the order of 5MHz. At curvature stronger than $r = 15$mm, many circuits start to break, but some survive to $r = 6$mm.

4.3 Identification capacity

The results of Section 4.2 allow us to estimate the identification capacity. On the one hand, the frequency band has a width of approximately 1.7 GHz. On the other hand, the number of distinguishable peak positions in this band is determined by the level of inaccuracy in measuring the peak frequency. We make two estimates, a pessimistic one and an optimistic one. In the worst case our circuits are subject to bending. As discussed in Section 4.2, this leads to a frequency uncertainty of approximately 5MHz. The corresponding C_{ID} for a single-coil circuit is $\log(1.7\mathrm{GHz}/5\mathrm{MHz}) = 8.4$ bits.

On the other hand, if we assume that there is no bending and that the z coordinate is well under control, then the frequency uncertainty is at most 0.3 MHz. The corresponding C_{ID} is $\log(1.7\mathrm{GHz}/0.3\mathrm{MHz}) = 12.5$ bits.

A precise computation of the C_{ID} of a multi-coil circuit is highly non-trivial, since it strongly depends on the actual response features that are being examined. Let's assume for the moment that we only look at the locations of the upward peaks. These peak locations are not independent functions of the random capacitance values. The joint probability distribution of the peak locations is a complicated function. This function, together with the measurement resolution on the frequency axis, determines the entropy (the number of bits of extractable information) of the random capacitances when one is looking merely at the peaks. For a two-coil circuit as in Fig. 1, the C_{ID} then lies between one and two times the single-coil C_{ID}. As we mentioned in Section 3.2, however, one can look at more response features than just the peak locations. The precise details of stable data extraction are still work in progress.

The improved 'resolving power' will bring the result close to three times the single-coil C_{ID}. (Note the factor 3, which arises from the three random capacitors, even though there are just two peaks.)

Hence, if the signal processing is done correctly, then as a rule of thumb the C_{ID} of the combined circuit can be estimated as (almost) the single-coil C_{ID} multiplied by the number of randomized capacitors. The circuit in Fig. 1 has $C_{\mathrm{ID}} > 20$ in the pessimistic case and $C_{\mathrm{ID}} > 30$ in the optimistic case.

5 Manufacturer-resistance

It is difficult to precisely quantify the level of 'unclonability'. A good anti-counterfeiting feature has a strong asymmetry between the original cost of manufacturing and the cost of cloning. This factor, which we will denote as F ($F > 1$), is estimated as follows. The attacker aquires N random authentic tags, e.g. by intercepting, inspecting or buying authentic goods. He measures the resonance properties of these circuits (which is very easy) and then tries to clone them. We assume that he has access to a factory that makes authentic circuits. He does not use the randomized mask (Section 2.2) for exposing the resist, but constructs a special mask corresponding to the properties of his N circuits. Let's assume that spreading the mask cost over N tags in this way renders the mask cost per cloned tag negligible. Due to inherent manufacturing inaccuracies, there is a probability p that a capacitor gets its intended value. On average, $1/p$ attempts are required to get the capacitance right. In a circuit with k capacitors, this applies k times independently; hence $F = 1/p^k$.

A different analysis applies if the attacker does use the same randomized process as the original manufacturer. This attack, which is much weaker, has $F = 2^{C_{\mathrm{ID}}}/N$, which grows exponentially with C_{ID}.

Unfortunately we do not yet have enough data to estimate p. However, it turns out that there are significant variations in the metal components even on wafers that do not contain the random resist layer. The effect on the resonance frequencies is a standard deviation of approximately 10 MHz for peaks around 1GHz.

Estimating manufacturer-resistance is made even more difficult by the existence of attacks such as 'laser trimming', where the attacker uses a laser beam to remove parts of capacitor plates. It is not yet clear to us if such attacks are simple to detect in an automated way. On the other hand, laser trimming requires expensive equipment ($>\$10^5$) and it is a rough process causing shorts in the capacitances with high probability.

Whatever the answers are to the above questions, the F-factor will certainly be improved if random variations are introduced in the coils. Furthermore, good signal processing should allow us to extract more robust features out of the response curves than just the frequencies and relative amplitudes of the upward peaks (Section 3.2). Such improved characterization automatically makes cloning more difficult.

6 Summary

We have presented a new type of cheap, randomized anti-counterfeiting tag that is read out wirelessly. Random thickness variations of the dielectric layer in the capacitors give rise to random resonance frequencies, which serve as a unique identifier.

Test circuits were made using thin film deposition on glass wafers. The circuits contain a 1μm layer of Al, a thin layer of resist and a 10μm layer of Cu.

If the tags are not bent, the upward peaks in the amplitude of the impedance can be localized with sub-megahertz accuracy. More than 30 bits of identification capacity are then achieved by coupling two LC circuits via an additional randomized capacitor.

The level of manufacturer-resistance has not yet been determined. If necessary, cloning can be made more difficult by randomizing not only the dielectric but also the conducting parts of the circuits.

Acknowledgements

We kindly thank Geert-Jan Schrijen and Claudine Conrado for many fruitful discussions.

References

1. J. D. R Buchanan, R. P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan. Forgery: 'fingerprinting' documents and packaging. *Nature, Brief Communications*, 436:475, July 2005.
2. G. DeJean and D. Kirovski. Radio frequency certificates of authenticity. In *IEEE Antenna and Propagation Symposium – URSI*, 2006.
3. Blaise Gassend, Dwaine E. Clarke, Marten van Dijk, and Srinivas Devadas. Controlled physical random functions. In *ACSAC*, pages 149–160. IEEE Computer Society, 2002.

4. Jorge Guajardo, Sandeep Kumar, Geert-Jan Schrijen, and Pim Tuyls. FPGA intrinsic PUFs and their use for IP protection. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007)*, 2007.
5. Peter Harrop and Raghu Das. Printed and chipless rfid forecasts, technologies & players. Technical report, IDTechEx Ltd., `www.idtechex.com`, 2007.
6. Darko Kirovski. Toward an automated verification of certificates of authenticity. In Jack S. Breese, Joan Feigenbaum, and Margo I. Seltzer, editors, *ACM Conference on Electronic Commerce*, pages 160–169. ACM, 2004.
7. Gerry O'Kane and Shanker Gopalkrishnan. The future of anti-counterfeiting, brand protection and security packaging III. Technical report, Pira International Ltd., `www.piranet.com`, 2005.
8. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297:2026–2030, Sept. 2002.
9. G. J. Simmons. Identification of data, devices, documents and individuals. In *Proceedings of the 25th Annual IEEE International Carnahan Conference on Security Technology*, pages 197–218, 1991.
10. P. Tuyls and L. Batina. Rfid-tags for anti-counterfeiting. In D. Pointcheval, editor, *Topics in Cryptology - CT-RSA 2006*, LNCS, pages 115–131. Springer Verlag, February 13-17 2006.
11. P. Tuyls, G.J. Schrijen, B. Škorić, J. van Geloven, R. Verhaegh, and R. Wolters. Read-proof hardware from protective coatings. In L. Goubin and M. Matsui, editors, *Cryptographic Hardware and Embedded Systems —- CHES 2006*, volume 4249 of *LNCS*, pages 369–383. Springer-Verlag, 2006.
12. P. Tuyls, B. Škorić, and T. Kevenaar. *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer, 2007.