Anti-Counterfeiting: Mixing the Physical and the Digital World

Darko Kirovski

Microsoft Research, Redmond, WA 98052, USA
darkok@microsoft.com

Abstract. In this paper, we overview a set of desiderata for building anti-counterfeiting technologies that rely upon the difficulty of manufacturing randomized complex 3D objects. Then, we observe how this set is addressed by RF-DNA, an anti-counterfeiting technology recently proposed by DeJean and Kirovski. RF-DNA constructs certificates of authenticity as random objects that exhibit substantial uniqueness in the radio frequency domain.

Key words. Anti-counterfeiting, RF-DNA, certificates of authenticity

1 Introduction

Counterfeiting is as old as the human desire to create objects of value. For example, historians have identified counterfeit coins just as old as the corresponding originals. Archeological findings have identified examples of counterfeit coins from 500 B.C. netting a 600+% instant profit to the counterfeiter [1]. Test cuts were likely to be the first counterfeit detection procedure – with an objective to test the purity of the inner structure of the coin. The appearance of counterfeit coins with already engraved fake test cuts initiated the cat-and-mouse game between counterfeiters and original manufacturers that has lasted to date [1].

It is hard to assess and quantify the market for counterfeit objects of value today. With the ease of marketing products on-line, it seems that selling counterfeit objects has never been easier. Industries under attack include the software and the hardware, the pharmaceutical, the entertainment, and the fashion industry. For example, it is estimated that between 7-8% of world trade,[1] 10% of the pharmaceuticals market,[2] and 36% of the software market[3] is counterfeited. Consequently, there exists demand for technologies that can either resolve these problems or significantly reduce the breadth of the search space for origins of counterfeits.

[1] According to the Interpol, World Customs Organization and International Chamber of Commerce estimates that roughly 7-8% of world trade every year is in counterfeit goods.

[2] In a study with the US Food and Drug Administration, Glaxo-Smith-Kline estimated that counterfeit drugs account for 10% of the global pharmaceuticals market.

[3] The Business Software Alliance estimates that 36% of software sales worldwide are counterfeit.

Dagstuhl Seminar Proceedings 09282
Foundations for Forgery-Resilient Cryptographic Hardware
http://drops.dagstuhl.de/opus/volltexte/2010/2406

1.1 Classification

We classify the related illegal trade into two groups:

- **Piracy** – where the buyer is confident that the purchased object is not genuine due to an uncharacteristically low price or some other form of discrepancy with respect to the original product. However, the buyer still willingly executes the trade. Such transactions do not gain substantial revenue to the pirate, hence, it is arguable what percentage of losses due to such events could be accounted as lost revenue for the legal copyright owner. First, buyers of such products are usually unlikely to purchase the original product. Second, one could argue that frequently pirated products, due to their public display and widespread usage, actually establish the pirated brand and consequently raise its value.
- **Counterfeits** – where the seller fools the buyer into believing that the merchandise is authentic and collects the full "legal-market" price on the product. In this case, the adversary collects substantial revenue with profit margins typically higher than that of the original manufacturer due to lack of development and marketing costs.

This classification is important as one could argue that it is perhaps impossible to address the first class using only technological means. On the other hand, we recognize that a suspecting buyer or a supply chain inspector could engage in a test of authenticity to address the latter problem. Clearly, a technology designed to help the buyer in the latter case is of no use in the case of piracy.

To the best of our knowledge there does not exist a study which breaks down illegal trade estimates into the above categories, however for certain markets such as pharmaceuticals and supply chains for airplane parts nearly all illegal trade can be claimed to be counterfeited. Looking into hundreds of billions of dollars lost to counterfeits each year, we want to establish a set of requirements for a growing class of anti-counterfeiting technologies that construct certificates of authenticity using random hard-to-copy objects whose multidimensional features are cryptographically signed to ensure reliable and convenient authentication.

2 Desiderata for Anti-Counterfeiting Technologies

A certificate of authenticity (COA) is a digitally signed physical object of fixed dimensions that has a random unique structure which satisfies the following requirements:

R1 **inexpensive to manufacture** – the cost of creating and signing original COAs is small, relative to a desired level of security,

R2 **expensive to copy** – the cost of manufacturing a COA instance is several orders of magnitude lower than the cost of exact or near-exact replication of the unique and random physical structure of this instance,

R3 inexpensive to authenticate off-line – the cost of verifying the authenticity of a signed COA off-line is small, again relative to a desired level of security, and

R4 robust – COA must be robust to the environmental elements such as changes in humidity and temperature, and ordinary wear and tear.

The key to the analysis of a COA instance is the extraction of its "fingerprint," i.e., a set of features that reliably represents its multi-dimensional structure. This process is typically based on a specific physical phenomenon and produces a cardinality-N vector of numbers $\mathbf{x} \in \mathbb{R}^N$. This imposes that:

R5 physical one-way function – it should be computationally difficult to construct an object of fixed dimensions with a "fingerprint" $\mathbf{y}$ such that $||\mathbf{x}-\mathbf{y}|| < \delta$, where $\mathbf{x}$ is a given "fingerprint" of an unknown COA instance and δ bounds the proximity of $\mathbf{x}$ and $\mathbf{y}$ with respect to a standardized distance metric $||\cdot||$.

This requirement establishes COA instances as physical one-way functions. By having access only to the "fingerprint" the adversary should face a difficult task of producing an object that has a near-equivalent "fingerprint." For example, when such a COA is attached to a credit card, it would prevent its physical replication by an adversary who obtains all the digital information stored on the card. Such an attack, often referred to as skimming, according to a Nielsen Report is responsible for about US$2B annual loss relative to a US$16B aggregate profit to credit card companies world-wide (data from 2008) [2].

R6 repetitiveness – the noise that stems from reading the "fingerprint" for a specific COA instance by different readers, in different environments, and/or at different read-out misalignments should be such that the probability of a false negative is smaller than a certain desired constant, $\Pr[||\mathbf{x}-\mathbf{y}|| < \delta] \leq \varepsilon_{FN}$, where $\mathbf{x}$ denotes the "fingerprint" read-out of an issued COA instance and $\mathbf{y}$ denotes a "fingerprint" read-out for the same instance during an arbitrary in-field verification,

R7 non-collision – the probability of a false positive should be smaller than a certain desired constant, $\Pr[||\mathbf{x}-\mathbf{y}|| < \delta] \leq \varepsilon_{FP} \ll \varepsilon_{FN}$, where $\mathbf{x}$ denotes the "fingerprint" read-out of an issued COA instance and $\mathbf{y}$ denotes the "fingerprint" read-out for any other distinct instance, and

R8 "fingerprint" interdependence – "fingerprint" samples collected over a large topological neighborhood should be mutually dependent. In addition, accurate mathematical modeling of this dependence should be as computationally expensive as possible. This dependence ensures that an adversary cannot forge the "fingerprint" one sample at a time – if such an attack is possible with a high success rate, typically its cost is linearly proportional to the number of "fingerprint" samples [3].

Requirement **R8** is one of the crucial requirements in thwarting attacks that do not aim at manufacturing a near-exact copy of the authentic COA instance.

Instead, the adversary aims to launch a simple search process that adjusts the object topography so to fit an authentic "fingerprint." Each iteration of this process would adjust a group of samples at a time. This attack could be even computational if requirement **R5** is not satisfied.

For example, COAs based upon fibers relatively sparsely embedded in paper typically do not satisfy **R8** [3]. Positioning of a single fiber in this case is not dependent upon the remaining fibers, thus, the adversary can orient these fibers on paper one by one. If this process is accurate, the cost of recreating a single COA instance is small.

R9 tamper-evidence – a COA instance could be conceived to represent a tamper-evident feature, i.e., a seal. If opening a specific package can be done exclusively via destroying the COA instance, and reproduction and reassembly of the signed seal is not easily attainable, then we could use such an instance as a tamper-evidence.

R10 visual inspection of the verification path – the observed randomness is scanned using a hardware device, however the verification path from the random object to the measurement circuitry/COA scanner must not be obstructed by adversarial hardware and/or software. That's why random features in COA instances should have relatively large minimum geometries so that they can be inspected visually. In addition, contactless (optical, wireless) measurements are preferred as static points of contact between a COA instance and a related scanner represent a perfect opportunity for the adversary to intercept the verification path.

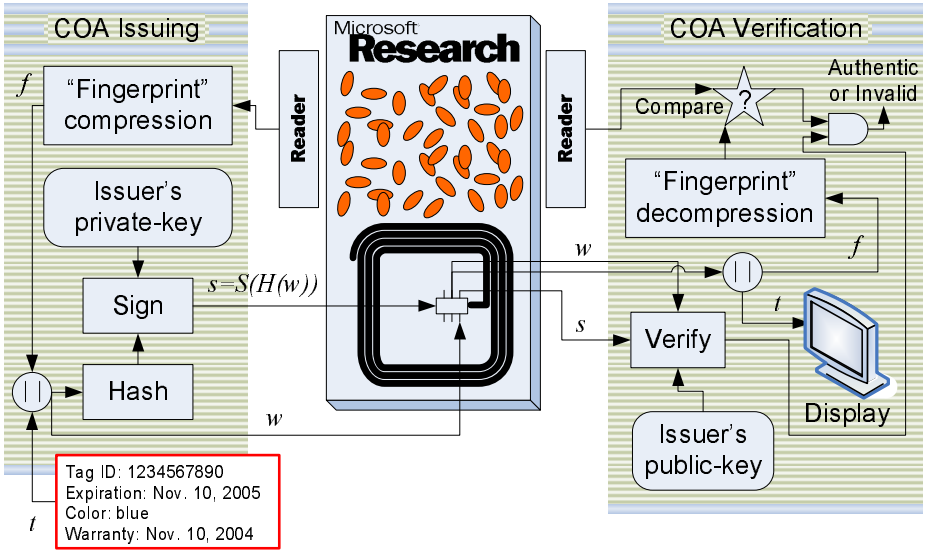

Fig. 1. Block diagram of the key steps involved in issuing and verifying a COA instance.

3 Digitizing the Physical World

COA systems as defined in Section 2 enable elegant off-line verification using a trusted device that contains the public key of the COA issuer. In this section, we review how traditional public-key cryptography can be used to bind a product instance, COA's physical random features, and arbitrary information that the issuer desires to associate with the product. A simple protocol is adopted from [3, 10, 11] and presented in Figure 1.

When creating a COA instance, the issuer digitally signs its "fingerprint" using traditional public-key cryptography. First, the "fingerprint" is scanned, digitized, and compressed into a fixed-length bit string f. Next, f is concatenated to an arbitrary information t that the issuer wants to associate with the product instance (e.g., product ID, expiration date, MSRP, coupon offers). The combined bit string $w = f||t$ is then signed. Several signing protocols could be used here, for example:

- the Bellare-Rogaway protocol, PSS-R [12], for signing messages with message recovery where an arbitrary signing mechanism such as RSA [13] could be used; the resulting signature s is then encoded directly onto the COA instance using an existing storage technology such as an RFID, or
- the issuer could also use a traditional IEEE1363-like cryptographic signature [14, 15], s, attach the plain-text w, and then encode $s||w$ directly onto the COA instance using an existing storage technology such as an RFID.

The resulting tag that contains both the COA and the associated RFID is now attached to a product whose authenticity the issuer wants to vouch. The association of the COA's "fingerprint," the issuer's private key, and the product protected using the COA can be verified in-field off-line using a device that has trusted access to the issuer's public key. Secure delivery of this key calls for a simple public-key infrastructure where the device is only expected to maintain the public key of a certifying authority, and the issuer stores a certificate, i.e., its public key signed by the private key of the trusted party, onto the RFID.

Verification of the tag is done using a simple protocol. First, the corresponding signature, s, from the RFID is verified against the issuer's public key [12, 14]. In case the integrity test is successful, the original "fingerprint" f (stored in the RFID or extracted from a PSS-R signature) and the associated data, t, are extracted from w. The verifier proceeds to scan in-field the actual "fingerprint," f', of the attached COA instance, i.e., obtain a new reading of the instance's physical properties, and compare them with f. If the level of similarity between f and f' exceeds a pre-defined and statistically validated threshold δ, the verifier declares the instance to be authentic and displays t. In all other cases, the reader concludes that the COA instance is not authentic.

In order to counterfeit protected objects, the adversary needs to:

(i) compute the private key of the issuer – a task which can be made arbitrarily difficult by adjusting the key length of the used public-key crypto-system [13, 14], or

(*ii*) devise a manufacturing process that can exactly replicate an already signed COA instance – a task which is not infeasible but requires substantial expense by the malicious party – the forging cost dictates the value that a single COA instance can protect [3], or

(*iii*) misappropriate signed COA instances – a responsibility of the organization that issues COA instances. For example, one possibility is to collect tags from already sold products, attach them to counterfeits, and sell them as authentic merchandise. One way to address this problem is to assign two COAs for each product, one that vouches for product's genuineness, another that vouches that the product is new. Retailer's responsibility is to devalue (i.e., tear apart) the latter COA when the product is sold – an action that is trivial to verify at the back-end of the supply chain (i.e., the retailer would have to send all torn COAs back to the supply chain inspector). The same procedure can be used to signal and/or value product's "n^{th}-owner."

4 Applications

COA instances are generic "objects of value." They have a fully horizontal perspective of possible applications. The value that one COA instance could maximally represent, approximately equals the cost to forge this instance [3]. Inexpensive verification makes COAs particularly attractive for several traditional applications as well as for a myriad of new ones. Currency, checks, money orders, credit cards, license and product tags, warranties, receipts, endorsements, ownership documents, proofs of purchase/return, proof of repair, coupons, tickets, seals, tamper-evident hardware can all be produced using COAs.

COAs whose "fingerprints" satisfy requirement **R5**, i.e., they do not reveal their physical structure in a straightforward fashion, could be used against skimming credit cards and falsifying personal identification documents such as passports, visas, driver's licenses, and national ID cards. Then, by accessing full credit card information from a merchant database (e.g., holder's name, card's number and expiration date, PIN code, *and* COA's "fingerprint"), it would be still difficult for the adversary to create a physical copy of the original credit card produced by the issuing bank. To complete the operation, the adversary would have to gain physical access to the original credit card and accurately scan its 3D structure (e.g., using X-rays or other 3D imaging systems). Finally, the adversary would still have to build the 3D object, a task that requires significant cost due to **R2**.

5 Review of Existing Methodologies

COA instances can be created in numerous ways. For example, when covering a surface with an epoxy substrate, its particles form a low-rise but random 3D landscape which uniquely reflects light directed from a certain angle. COAs based upon this idea were first proposed by Bauder and Simmons from the Sandia National Labs and were used for weapons control during The Cold War

[16]. To the best of our knowledge this is the first design of COAs based upon the fact that individual instances are difficult to near-exactly manufacture by a malicious well-financed party.

Fiber-based COA. Bauder and Simmons were also the first to propose COAs created as a collection of fibers randomly positioned in an object using a transparent gluing material which permanently fixes fibers' positioning [16–18]. Readout of the random structure of a fiber-based COA could be performed in numerous ways using the following fact: if one end of a fiber is illuminated, the other end will also glow. Bauder proposed fiber-based COAs for banknote protection - fibers in that proposal were fixed using a semi-transparent material such as paper [17]. To the best of our knowledge, only few efforts have followed the pioneering work by Bauder and Simmons. Church and Littman have worked on extraction of random optical-fiber patterns in the context of currency anti-counterfeiting [19, 20]. The first COA system based upon fiber-infused paper and public-key cryptography was developed by Chen et al. [21, 3]. While efficient and inexpensive, fiber-based COAs do not satisfy **R5** and thus, could be vulnerable to malicious attackers who conquer a technology for fiber placement on paper. Although such a technology is not available, we categorize its objective as 2+D manufacturing and speculate that it is substantially easier than manufacturing purely random 3D topologies.

Speckle Scattering. Pappu was the first to create a class of physical one-way functions via speckle scattering [22, 23]. A speckle pattern is a random intensity pattern produced by the mutual interference of coherent wavefronts that are subject to phase differences and/or intensity fluctuations. Pappu focused on Gabor wavelets to produce short digests of the natural randomness collected from the optical phenomenon. His Ph.D. thesis has a solid survey of the related but scarce work [22]. Škorić was the first to match experimentation and theoretical bounds on the amount of randomness exhibited by keys formed from speckle [24]. Speckle scattering is a phenomenon sensitive to microscopic changes to the source of scattering hence, it is difficult to build practical COAs that satisfy **R4**; in addition, it is poorly understood how speckle filtering addresses **R6** and **R8**.

Far-field RF. Finally, COAs in the electromagnetic domain have been proposed by several companies [25–29], all of them aiming to detect COA's random structure in the far-field. The basic idea with these proposals was to identify a certain set of resonant features of dielectric and/or conducting materials in the far-field[4] as a complement to RFID communication. As a consequence all proposals suffer from the inability to satisfy **R5** and **R8**, thus presenting relatively easy targets to malicious parties who understand their re-radiation principles. In addition, far-field detection is prone to spoofing and jamming by a sophisticated attacker; thus, such schemes often have difficulties satisfying requirement **R10**. Because the detection is taking place in the far-field, these systems operate in the "expensive" 60GHz frequency range making COA verification unnecessarily expensive with current semiconductor technologies.

[4] We define far-field as distance which is multiple wavelengths away from the source of the electromagnetic (re)-radiation.

Physically unclonable functions based upon forced variability in semiconductor manufacturing have been reviewed in Section 5.2.

5.1 RF-DNA

The first technology that has focused on identifying radio-frequency "fingerprints" of dielectric and conductive resonators in the near-field was developed by DeJean and Kirovski [10, 11]. Their COA proposal, RF-DNA, is based upon the basic re-radiation (including radio-wave resonance, Rayleigh, and Mie scattering) principles described within the generalized extinction theorem [30–32]. RF-DNA is substantially different from far-field RF schemes, as it aims to capture in its "fingerprint" an accurate image of the variability exerted by the electromagnetic field close[5] to the source of re-radiation, i.e., COA instance. The imaging is done using a dense matrix of patch antennae, each of them capable of transmitting and/or receiving RF waves in the 5-6GHz RF sub-band.

The technology fares well with respect to the set of desiderata. Each COA instance costs less than a cent, with the COA reader expected to cost less than US$100 and as low as several dollars in mass production. Near-exact replicas would demand true 3D scanning and manufacturing of a specific 3D topology. It is robust to wear and tear as the "fingerprint" read-out is contactless. Its physical one-way function can be well formulated mathematically via the inverse design problem over the Maxwell equations [33], which is an ill-defined problem [34] of exceptional, yet never formally proven,[6] computational difficulty. Even solving the forward simulation problem over the Maxwell equations accurately is an exceptionally challenging task for state-of-the-art electromagnetic fields solvers [35]. Typically, the noise that stems from simulations is well over 3dB with respect to physical measurements [35], whereas the expected noise due to misalignment, environmental factors, and variances in the manufacturing of COA readers should be well within 0.5dB [11]. DeJean and Kirovski have shown that the detection performance in their system results in negligible rates of false positives and negatives [11]. The COA reader by design enforces that "fingerprint" readouts are dependent across different neighboring transmitter-receiver pairings, thus by minimally altering small part of her design, the adversary would affect the "fingerprint" components of many (or almost all) transmitter-to-receiver responses.

One of the open issues related to RF-DNA is its weak "fingerprint" robustness with respect to noise stemming from re-radiating objects that could be attached to COA instances as products. This is a limitation within requirement **R4** that has not been yet explored.

5.2 Challenge/Response COA Systems

COA systems that rely on small, imperceptible features, such as distinct semiconductor circuits created using manufacturing variability, cannot be verified

[5] Less than one wavelength from the resonator.
[6] To the best of the author's knowledge.

using a passive protocol because the adversary can always hard-wire the resulting digitized "fingerprint" into an appropriate part of the hardware state and fool the verifier that it is measuring the actual unique manufacturing variability [4]. An active, challenge-based protocol on the other hand, would require that the verifier contains either: ***i***) an accurate but private description of the distinct circuitry in each COA instance so that it can compute the expected response from the COA under test or ***ii***) a limited set of valid challenge/response pairs.

One major disadvantage of type-***i*** solutions is the fact that the private circuit description must be kept away from the adversary (otherwise, the adversary can use this description to manufacture the exact same circuit[7]); thus, the verification process must be launched on-line. To the best of the author's knowledge circuits of type-***i*** have not been proposed to date.

There exist several proposals for type-***ii*** circuits [5–8], often referred to as physically unclonable functions, PUFs. The disadvantages of type-***ii*** proposals are: necessity for on-line verification and high cost of storage and bandwidth that needs to be allocated to support the overall COA system among others. Table 1 presents a comparison of expenses related to enabling anti-counterfeiting using type-***ii*** semiconductor-based PUFs and RF-DNA. As one can observe a major cost factor is the secure connectivity with the issuing server that needs to be established for a PUF to be verified. Conversely, if PUFs are embedded within an existing semiconductor product, i.e., integrated chip, in order to protect it, their manufacturing cost is negligible, yet their verification still requires a communication channel to the issuing server.

Apart from probing and brute-force reverse engineering semiconductor PUFs, one specific group of attacks that has not been launched on imperceptive challenge/response PUF systems yet, is collusion of correct challenge/response pairs from a single and/or multiple distinct PUF instances with an objective to reverse engineer the underlying random circuit and its points of enforced variability. In addition, power and delay analysis attacks are also possible against such schemes [9]. We note that such attacks are not viable against COA systems outlined using requirements **R1-10**.

6 Conclusion

Randomness is natural to many processes in the physical world. Early ideas by Bauder and Simmons have resulted in a growing list of technologies that aim at using such randomness to create distinct, cryptographically secure, and hard-to-forge certificates of authenticity, i.e., physically unclonable functions. In this paper, we introduced a set of desiderata for such technologies and showed how state-of-the-art fares with respect to this set. We identified RF-DNA, a proposal by DeJean and Kirovski, as a technology that appears to address well all of the requirements from this set.

[7] We remind the reader that the variability is enforced, not unavoidable when manufacturing such circuits.

Property	Semiconductor circuit PUF	RF-DNA
Storage at server	K challenge-response pairs need to be stored, where K equals the anticipated number of verifications per PUF.	None.
Storage at tag	Yes, on-chip. Needs to store public key of certification authority.	Yes, passive RFID. Cost: 2-6 cents.
Cost of tag	$\sim$ zero if embedded to protect chip **or** several cents if used to protect object, i.e., similar to cost of smartcard.	$\sim$ cost of RFID + cost of signing the RF "fingerprint."
Communication w/ server during in-field verification	Server-auth TLS handshake with key exchange, then ask for challenge, receive challenge, compute/send response, receive decision.	None.
Cost of server farm	Linearly proportional to expected peak number of concurrent server-PUF connections.	None.
Verification requirements	Communication channel to server.	RF-DNA scanner.

Table 1. Comparison table of expenses related to enabling anti-counterfeiting using type-***ii*** semiconductor-based PUFs and RF-DNA.

References

1. K. Barry. Counterfeits and Counterfeiters: The Ancient World. Available on-line at: `http://www.ancient-times.com/newsletters/n13/n13.html`.
2. P. Britt. Credit Card Skimming: Growing Trend or Media Hype? Transaction World Magazine, September, 2001. Available on-line at: `http://www.transactionworld.com/articles/2001/september/riskmanagement1.asp`.
3. D. Kirovski. Toward An Automated Verification of Certificates of Authenticity. ACM Electronic Commerce, pp.160–9, 2004.
4. K. Lofstrom, W.R. Daasch, and D. Taylor. IC Identification Circuit Using Device Mismatch. IEEE ISSCC, pp.372–373, 2000.
5. B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Silicon Physical Random Functions. ACM Computer and Communication Security Conference, 2002.
6. J.-W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits with identification and authentication applications. IEEE VLSI Circuits Symposium, 2004.
7. J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls. FPGA intrinsic PUFs and their use for IP protection. Cryptographic Hardware and Embedded Systems, 2007.
8. P. Tuyls and B. Škorić. Strong Authentication with Physical Unclonable Functions. In "Security, Privacy and Trust in Modern Data Management," M. Petković, W. Jonker (Eds.), "Data-Centric Systems and Applications," Springer, 2007.
9. P. Kocher, J. Jaffe and B. Jun. Differential Power Analysis. CRYPTO, pp.388–397, 1999.
10. G. DeJean and D. Kirovski. Radio Frequency Certificates of Authenticity. IEEE Antenna and Propagation Symposium, 2006.
11. G. DeJean and D. Kirovski. RF-DNA: Radio-Frequency Certificates of Authenticity. Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Vol.4727, pp.346–363, 2007.

12. M. Bellare and P. Rogaway. The exact security of digital signatures how to sign with RSA and Rabin. EUROCRYPT, pp.399–414, 1996.
13. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Vol.21, (no.2), pp.120–126, 1978.
14. IEEE 1363-2000: Standard Specifications For Public Key Cryptography, 2000. Availabel on-line at: `http://grouper.ieee.org/groups/1363`.
15. T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. Internet draft, available on-line at: `http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc4346-bis-09.txt`.
16. D.W. Bauder. Personal Communication.
17. D.W. Bauder. An Anti-Counterfeiting Concept for Currency Systems. Research report PTK-11990. Sandia National Labs. Albuquerque, NM, 1983.
18. G.J. Simmons. Identification of data, devices, documents and individuals. IEEE International Carnahan Conference on Security Technology, pp.197–218, 1991.
19. S. Church and D. Littman. Machine reading of Visual Counterfeit Deterrent Features and Summary of US Research, 1980-90. Four Nation Group on Advanced Counterfeit Deterrence, Canada, 1991.
20. Commission on Engineering and Technical Systems (CETS). Counterfeit Deterrent Features for the Next-Generation Currency Design. The National Academic Press, 1993.
21. Y. Chen, M.K. Mihcak, and D. Kirovski. Certifying Authenticity via Fiber-Infused Paper. ACM SIGecom Exchanges, Vol.5, (no.3), pp.29–37, 2005.
22. R. Pappu. Physical One-Way Functions. Ph.D. Thesis, MIT, 2001.
23. R. Pappu, et al. Physical One-Way Functions. Science, Vol.297, (no.5589), pp.2026–30, 2002.
24. B. Škorić. The entropy of keys derived from laser speckle. Journal of Optics A: Pure and Applied Optics, to appear, 2008.
25. J. Collins. RFID Fibers for Secure Applications. RFID Journal, 2004. Available on-line at: `http://www.rfidjournal.com/article/articleview/845/1/14`.
26. CrossID, Inc. Firewall Protection for Paper Documents. Available on-line at: `http://www.rfidjournal.com/article/articleview/790/1/44`.
27. Inkode, Inc. Available on-line at: `http://www.inkode.com`.
28. Creo, Inc. Available on-line at: `http://www.creo.com`.
29. RF SAW, Inc. Available on-line at: `http://www.rfsaw.com/tech.html`
30. P.P. Ewald. Ann. der Physik, Vol.49, 1-56, 1915.
31. C.W. Oseen. Uber die Wechrelwirkung zwischen zwei elektrischen Dipolen und uber die Drehung der Polarisationsebene in Kristallen und Flussigkeiten. Ann. der Physik, Vol.48; pp.1 -56, 1915.
32. E. Wolf. A generalized extinction theorem and its role in scattering theory. Coherence and Quantum Optics, L. Mandel and E. Wolf (eds.), Plenum, New York, 1973.
33. D.B. Avdeev. Three-dimensional electromagnetic modelling and inversion: from theory to application. Surveys in Geophysics, Vol.26, pp.767–799, 2005.
34. A.N. Tikhonov and V.A. Arsenin. Solution of Ill-posed Problems. Winston & Sons, Washington, 1977.
35. Microwave Engineering Europe. CAD benchmark. October 2000 – February 2001. Available on-line at: `http://i.cmpnet.com/edtn/europe/mwee/pdf/CAD.pdf`