Authenticating Medications with QR-Codes and Compact Digital Signatures

Julien Jainsky[1], David Naccache[3], Bassem Ouni[2], and Ofer Yifrach-Stav[3]

[1] DISkrete Security, Houston, TX, USA
julien.jainsky@diskretesecurity.com
[2] Technology Innovation Institute, Masdar City, Abu Dhabi, UAE
bassem.ouni@tii.ae
[3] DIÉNS, ÉNS, CNRS, PSL University, Paris, France
ofer.friedman@ens.fr, david.naccache@ens.fr

Abstract. This paper describes a way to protect medications against falsification, a long-standing problem in the world.

We combine several existing technologies to achieve the stated goal. The building-blocks used are inherent physical randomness generated during the packaging process, artificial vision, short digital signatures and QR-codes.

1 Introduction

A recent article[4] [9] reports that a the $200 billion pharma counterfeit drug market is growing by 20% *per annum*.

The issue of fake medications poses a significant and widespread global concern, endangering the health and well-being of countless individuals. According to the World Health Organization (WHO) [13], approximately 10.5% of medicines available worldwide may be counterfeit with this figure reaching an alarming levels in some regions. For example, In 2017, the WHO reported issues with 33.6% of hypertension, cancer, epilepsy, analgesic uterotonics and immunosuppressants drugs from 75 low- and middle-income countries (LMIC) [13]. On top of these, it is estimated that approximately 50% of the drugs sold via the internet are fake [2]. These counterfeit drugs not only fail to provide the intended therapeutic benefits but can also lead to adverse health effects, drug resistance, and even fatalities.

These revelations serve as a resounding call to action, emphasizing the imperative need for robust product verification and tracking capabilities within the healthcare realm. Hence, any cheap technological solution allowing to control or mitigate the problem is welcome.

[4] https://bit.ly/3BZPWPE

2 The solution

We seek to design a blister packaging solution which is cheap to manufacture, easy to check electronically and allows patients and pharmacists to instantly detect fakes. Ideally, such a solution should not include a chip in the medication's package (as this is costly) and rely on an application running on the patient's mobile phone.

Under such constraints, what comes to mind naturally is the use of QR codes, digital signatures and some unique hardly reproducible physical features. We will overview the different components of the proposed solution and combine them to reach the desired goal.

2.1 Drawing inherent randomness

Using the inherent characteristics of disordered systems is not new at all and solutions leveraging this idea were re-invented over and over again. In 1983, Bauder [1] made one of the earliest documented references to such systems, followed closely by Simmons in 1984 [11,12]. Building on these pioneering works, Naccache and Frémanteau introduced an authentication scheme specifically tailored for memory cards [6]. We hence naturally looked for already existing inherent randomness in the packaging process. We will describe here two such ideas.

Two colored pills. Current packaging techniques such as the one shown in Figure 1 provide some randomness. However, given that pills are usually packed by $n = 10$ to 20 relying on the pills' orientation alone does not provide enough entropy: Let T be the number of genuine packages needed to collect all 2^n pill combinations. It is known (coupon collector's problem) that:

$$E(T) = 2^n n \log 2 + \gamma 2^n + \frac{1}{2} + O(2^{-n}) \text{ and } \Pr\left(|T - E(T)| \geq c2^n\right) \leq \frac{\pi^2}{6c^2}$$

where $\gamma \simeq 0.5772$ is the Euler–Mascheroni constant.

Entropy can be cheaply increased (Figure 2, left), by randomly decorating each pill with k bars on one of the pill's sides. This adds 2^{k+1} bits per pill and an overall entropy of $2^{(k+1)n-1}$ bits per package[5]. For $(k, n) = (3, 10)$ we get 2^{39} combinations and an $E(T) \simeq 2^{39} \log 2^{39} \simeq 2^{43.76}$.

This solution offers only a modest form of security as a moderately sophisticated fraudster could still come-up with a manufacturing process placing the right pills in the right order to match a configuration copied from a genuine package.

[5] The -1 in the exponent comes from the fact that by rotating a package upside-down one more combination can be gained by the forger.

Fig. 1. A 10-bit random pattern formed naturally during packaging.

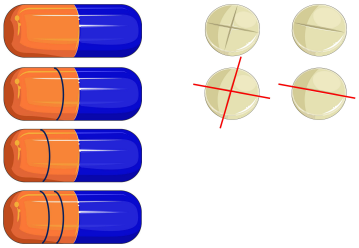

Fig. 2. Using $k = 2$ stripes to encode information in capsules (left) and Diameter detection (right). Source: `https://smart.servier.com/smart_image`, modified by the authors.

Orientation in circular pills. Another simple method consists in using the diameter naturally present in most pills as an angle encoding information. If this method is chosen, the packaging should be tight enough to forbid pills from spinning around after packaging. This is illustrated in Figures 2 (right) and Figure 3.

The detection of the pills' orientation is easy to extract using existing image processing tools. In our experiment, we placed 8 Prednisone pills on a black surface and photographed them using a common Samsung A5 smartphone.

The resulting image was named `image0.png`. `image0` was passed through a gradient filter[6] to generate `image1`. We then extracted 8 lines from `image1`[7] and superimposed the extracted lines on `image1` to get `image2`[8]. Indeed, all the angles were easily detected. Repeating the experiment (with `MaxFeatures->18`) in the presence of artefacts proved insufficient and required further filtering but such artefacts will not exist during field deployment.

The industrialization of this solution requires some easy technical refinements to deal with borderline angles using error correction on the signed data embedded into the QR-code and seems much harder to circumvent.

[6] `image1=GradientFilter[image0,10]//ImageAdjust`

[7] `lines=ImageLines[EdgeDetect[image1],MaxFeatures->8]`

[8] `image2=HighlightImage[image1,Orange,lines]`

Fig. 3. 30 pills encoding information using diameter orientation (illustration). Source: `https://smart.servier.com/smart_image`, modified by the authors.

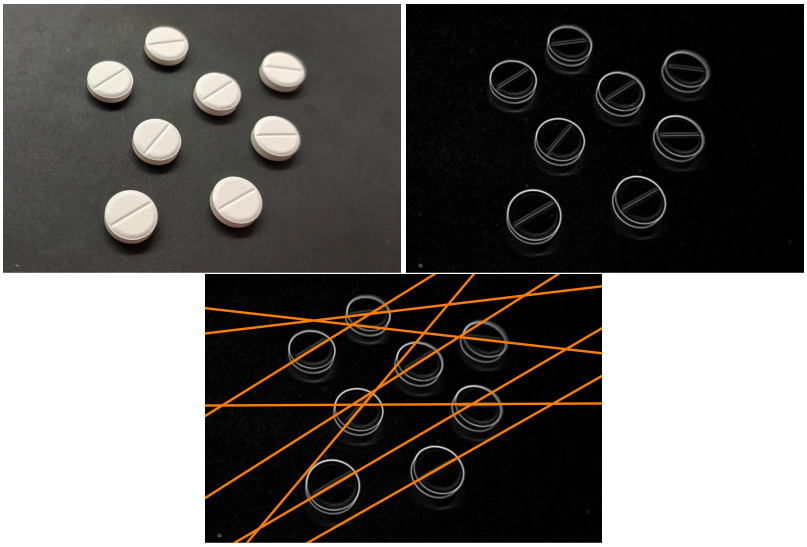

Fig. 4. Pill identification attempt in the absence of artefacts.

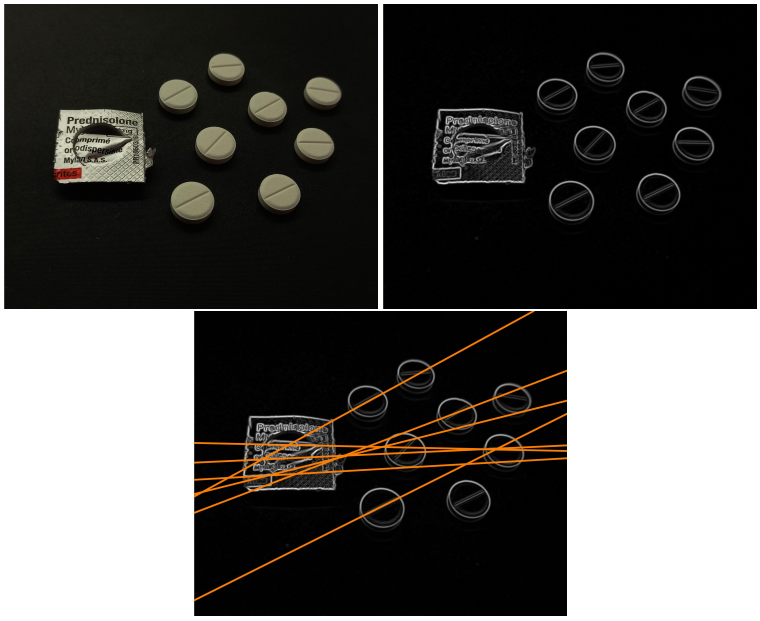

Fig. 5. Pill identification attempt in the presence of artefacts.

2.2 Packaging and QR-code printing

A QR can be either printed on the back of the blister package or on the back of the paper box containing the medications if the box is equipped with a transparent plastic window (such as the one shown in Figure 6) allowing the scanning of the QR code from outside the box using the smartphone.

Fig. 6. Simple paper box with a window.

If a standard box is used, we recommend to use micro QR-codes that can store up to 128 bits of information, such codes are shown in Figure 7. Such a solution requires compressing the signature on the inherent randomness into 16 bytes or spreading the signature over several micro QR-codes.

Fig. 7. Micro QR-codes on medications printed on a medication package. Source: `http://www.chinatimes.com/newspapers/20140805000894-260113`

Ideally, a second (constant) QR-code present on the box would allow the patients to install the application, thereby avoiding version issues.

An option, that we do not recommend, is to encode in the QR-code a URL redirecting to a digital signature stored online. Note that an online digital signature database is not expected to grow indefinitely as it could be sanitized when medications expire. This solution has the additional advantage of allowing to count the number of accesses to any given signature and hence blacklist copied URLs after too many verifications (e.g. 10). We discard this solution as it requires an online communication which might not always be available.

3 Short signatures

The current record in terms of signature size seems to be 110 bits, held by [4]. Truncating signatures to reduce their size was treated previously by [7] and [10], resulting in shorter DSA-like signatures without loss of security. Using those approaches, signature size is linearly reduce at the cost of additional exponential computations on the signer and/or the verifier side.

[7] proposed a solution for reducing the size of the DSA-like signatures by 2ℓ bits at an $O(2^\ell)$ work by signer and by the verifier. Typically $32 \leq \ell \leq 40$ bits. [10] improves this by requiring the 2^ℓ effort to be done only at the verifier's side. As [10] "frees" the signer again, we can now have the signer make a 2^ℓ effort to squeeze ℓ more bits by varying the DSA nonce k and searching for a short r. Note that because r does not depend on the message, a library of "good" r values could be constructed offline and used upon signing. Regularizing the flow of such r values during production can be important and there are known techniques for doing so, e.g. [3].

All in all, we can hence achieve a 3ℓ shortening gain at the cost of $O(2^\ell)$ operations by the signer and the verifier.

A typical EC-DSA signature is 56 bytes long, which means that choosing $\ell = 40$ yields a 41 byte signature. Legacy DSA produces 40 bytes signatures, in which case, with $\ell = 40$ bits will shorten the signature size to 25 bytes.

Note that another interesting way of shortening DSA-like signatures (to the best of our knowledge not reported so far) is the following: The signer generates 2^ℓ elements r and stops when a specific r is found. The form of this r is the following something$|\alpha|\alpha$ where α is any ℓ-bit string. Because there are 2^ℓ possible α values a good r is expected to be found in $O(2^\ell)$. By transmitting only the "something" part, the verifier can, using 2^ℓ verifications, retrieve α and verify the signature. This alternative to the discrete logarithm approach of [10] shortens a signature by 2ℓ bits at the cost of $O(2^\ell)$ work by both parties and its constant factor might prove smaller than the constant factor of [10] (unchecked). In addition DSA verifications lend themselves to batching which might also result in some constant gains [5].

4 Conclusion & an open question

We have described a way to protect medications against falsification, a long-standing problem in the world. The proposed solution does not require the

inclusion of chips in packages and relies on cheap existing technologies. The building-blocks used are inherent physical randomness generated during the packaging process, artificial vision, short digital signatures and QR-codes.

From a conceptual standpoint, the following question remains: *Given the collection of signature shortening ideas published so far can a Schnorr-like signature be shortened by more than 3ℓ bits at the cost of $O(2^{\ell})$ effort per party without loss of security?*

We conjecture that such is not the case given that all our attempts to combine different 2ℓ solutions ended-up in a total gain of 3ℓ at best. [8] is a useful reference to consult in that respect.

References

1. D. Bauder. An Anti-Counterfeiting Concept for Currency Systems. Technical Report PTK-11990, Sandia National Labs, Albuquerque, NM, 1983.
2. F. Clark. Rise in Online Pharmacies Sees Counterfeit Drugs Go Global. *The Lancet*, 386(10001):1327–1328, 2015.
3. H. Ferradi, R. Géraud, D. Maimuţ, D. Naccache, and A. de Wargny. Regulating the Pace of von Neumann Correctors. Cryptology ePrint Archive, Paper 2015/849, 2015. https://eprint.iacr.org/2015/849.
4. M. S. E. Mohamed and A. Petzoldt. The Shortest Signatures Ever. Cryptology ePrint Archive, Paper 2016/911, 2016. https://eprint.iacr.org/2016/911.
5. D. M'Raïhi and D. Naccache. Batch Exponentiation: A Fast DLP-Based Signature Generation Strategy. In *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, CCS '96, pages 58—61, New York, NY, USA, 1996. Association for Computing Machinery.
6. D. Naccache and P. Frémanteau. Unforgeable Identification Device, Identification Device Reader and Method of Identification, August 1992.
7. D. Naccache and J. Stern. Signing on a Postcard. In Y. Frankel, editor, *Financial Cryptography*, pages 121–135, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.
8. G. Neven, N. P. Smart, and B. Warinschi. Hash Function Requirements for Schnorr Signatures. *Journal of Mathematical Cryptology*, 3(1):69–87, 2009.
9. K. Overstreet. $200 Billion Pharma Counterfeit Drug Market Growing by 20% Per Year, 2019. Accessed on 16/09/2023.
10. T. Pornin. Truncated EdDSA/ECDSA Signatures. Cryptology ePrint Archive, Paper 2022/938, 2022. https://eprint.iacr.org/2022/938.
11. G. J. Simmons. A System for Verifying User Identity and Authorization at the Point-of-Sale or Access. *Cryptologia*, 8(1):1–21, 1984.
12. G. J. Simmons. Identification of Data, Devices, Documents and Individuals. In *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, pages 197–218, 1991.
13. World Health Organization. A Study on the Public Health and Socioeconomic Impact of Substandard and Falsified Medical Products. 2017.