# **RETHINKING E-AUTHENTICATION**

## *From PIN to PIP*

By Ciprian Galaon

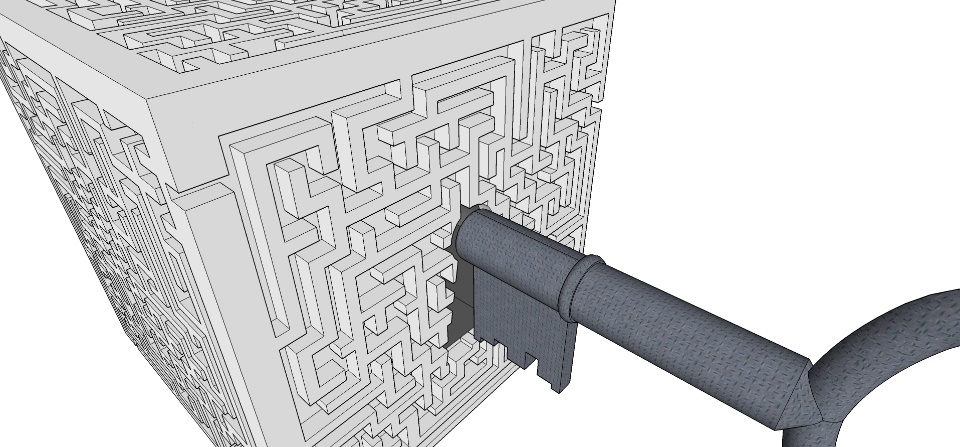
Manchester, UK, September 2014

cgalaon@hotmail.com

E-authentication stands for remote authentication of individual people over a network for the purpose of electronic government and commerce. Despite our façade of control and complacency, e-authentication still remains deeply an unavoidable technological challenge and a high level priority issue for individuals, companies and governments alike. The same goes for the security of credit and debit card transactions, both face-to-face and online.

A few years ago Steven Murdoch et al. published an [article](https://drive.google.com/file/d/0B3G_QeRwjH-VbEZrbE9Ha2xmMnc/edit?usp=sharing) about the security of, so desperately and naively trusted, authentication with chip and pin; it has been irremediably broken, increasing so the number of born-dead paradigms. This should not come as a surprise; it is something that all of us have been afraid of, and even seen coming, in the last decade. Equally bad news come from Tsutomu Matsumoto et al. in their [article](https://drive.google.com/file/d/0B3G_QeRwjH-VX3V0QlFOcFJneVE/edit?usp=sharing) defeating what was supposed to be one of our very last unbreakable authentication redoubts, our fingerprints. What is remarkable in Matsumoto’s point, and worrying in the same time I should say, is how cheap (around $10.00) may be crafting a gummy fingerprint and fool with it the “secure” devices announced again and again with great fanfare by competing manufacturers of commercial fingerprint systems. To practically all of us, after all, it is not only a question of money; it is above all about privacy, and even personal integrity and security (identity theft). The same could easily happen (following or emulating Murdoch’s method rather than Matsumoto’s) to iris authentication, if not already happened. A hacker named Jan Krissler, also known as starbug, reported that he replicated in 2014 the fingerprint of Germany’s defense minister Ursula von der Leyen by using several photographs of her right thumb taken at public events. Biometric authentication systems and, in general, e-authentication seem to be at a dead end. There are alternative methods (computer recognition software, e-mail or SMS one-time-password and OTP tokens, out-of-band verification, peripheral device recognition and scratch-off cards) which are claimed to be revolutionary safe, but to the user they are cumbersome and expensive (except maybe the scratch cards, although safe and opportune receipt and posterior safeguarding of the cards are important drawbacks that cannot just be ignored).

This article is about rethinking e-authentication, both being the user physically present −face-to-face and at E/POS− or not −over any telecommunications network−, aiming to improve the security of the process. Here is the challenge. We need a system complex enough on the inside which main characteristic being hard to break (ideally unbreakable) security, while simple and intuitive enough on the outside, on the user end, allowing for an easy and safe access to it; and this is precisely what the method proposed here intends to address.



If proved feasible, this method pledges to protect against any potential attack, directed either to the communication between the authentication device and the data base or to the devices themselves. Even if not absolutely unbreakable, the amount of time and the means needed to break the security provided by this method will stand as a significant deterrent even to the most perseverant and patient attacker. And most importantly, one-try/one-means/one-act will never again suffice to break the entire system.

A chain is as strong as the weakest link, and this is the major problem of all authentication systems today. Either the device is deceived or the communication is intercepted and corrupted with illegal and illegitimate ends; the entire system fails after each and every first successful try. In other words, devices and communication protocols have a Single Point of Failure to attacks, they share the same apparently unavoidable weakness. Once inside, attackers can succeed in their purposes and even do it again and again without being, most of the times, detected and blocked, let alone being prevented to do it. They have the choice of either stealing the PIN and/or the fingerprints or intercepting the communication. Once succeeded, they have it all, well, until detected, which does not mean in any case that a potential attacker is prevented to try it again and exploit the vulnerability of that or any similar system. Nevertheless what is highly concerning is not so much the PIN, which can be changed, but the fingerprint, which cannot.

Aware that extraordinary claims require extraordinary proof, I start with the disclaimer that the method proposed here is currently at the experimental stage and further processes of trial and error are required (provided, of course, that it will win favourable reviews and sufficient commercial interest).

Authentication by means a Personal Identification Number is no longer secure and improved methods are needed. The PIP proposed stands for Personal Identification Pattern and it is exactly that, authentication by entering one or more easy to remember patterns. A picture is worth more than a thousand words and, more so, numbers, I may say. Despite being very useful in electronic authentication and communication, numbers, especially large numbers, as any other abstract concept, are always hard to remember, if not impossible, to practically all human minds. As any other fictitious entity created ad hoc, they work very well as intermediary tools (they are the native language of computers and their raison d'être), but fail to attract friends among humans. Indeed, complex numbers/mathematics proved very useful in many aspects of our lives and allowed us developing advanced technologies (including artificial intelligence), but our minds do not seem to like them too much, particularly when it comes to authentication. Written notes, devices or cards that need to be kept under lock and key and even caches memories, as sine qua non reminders or access tools proved to be a not so good idea: cumbersome, open to failure and susceptible to being stolen or lost. The complexity of the technologies used in modern security systems, based on the understanding and development of numbers and equally complex algorithms, has entered an exponential competing spiral fuelled by a large variety of methods and technologies publically available to, and fully exploited by, increasingly creative, perseverant and highly sophisticated, cyber gangs.

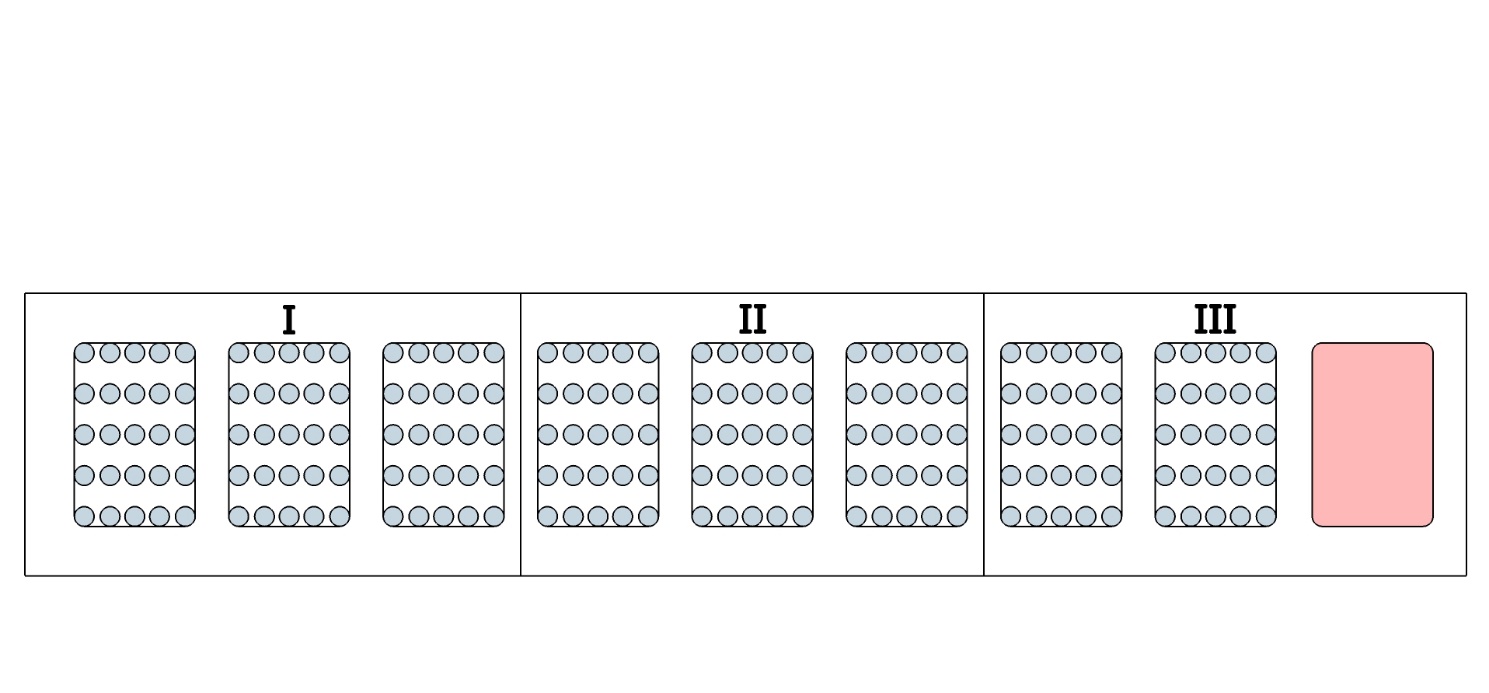
Sadly, the individuals in the middle seem left their arbitrary whim; or maybe not! Not accidentally, one of the most effective techniques of memorisation is the Peg System that involves combining numbers with images. The method proposed here fully exploits this (science) fact. Using a pattern as a means of authentication has another powerful advantage. The pattern chosen could always be partially used during the process of authentication while still allowing the system to preserve its more important function: secure unbreakable authentication (and communication). The best part of the PIP method proposed here is that not only does not get rid of numbers, but makes a better and complex use of them towards an unbreakable secure system. Its increased complexity is due to the fact that numbers and mathematical operations (the basic “+”, “−”, “x” and “÷”, at least) are introduced in the virtual layers beneath the analogic layer. As a result, a unique one-off PIN (also, one-time-password) is produced for each and every transaction, without making the authentication process more complicated (numbers or actions hard to remember with precision and so open to failure) for the enrollee. For her/him it will always mean to enter in the analogic layer (i.e. the interface of the device) the same personalised pattern/s (along with the fingerprint, finger’s veins or even iris, scanned by the device, as we will further see). For the system in turn, for each and every session, there will always be a different number. The system will have the ability to add complexity in the middle of the process -between the server and the user-, gaining so considerable amounts of security, without making authentication more difficult or unfamiliar to human minds, i.e. it is user friendly. Comparatively, the method proposed here is also a multifactor authentication system (i.e. it combines something physically possessed -a card or a token-, something known -a password and/or a pattern- and something inherent -a fingerprint or iris). In a few words, the PIP method pretends to be a convenient and adaptable technological bridge between our familiar, physical and analogic world and the intricate, complex and abstract world of numbers that pledges to offer a high level of secure e-authentication. Let’s see how it works!

Many of us are already familiar with the use of a pattern instead of a PIN; not so many years ago, smartphones implemented this method as an alternative to the use of digits. The method proposed here takes the use of patterns a step further and fully exploits its potential by connecting them with numbers in a dynamic manner rendering a high level of security.

In any pattern authentication method resembling this one, the level of security would admittedly increase depending on the number of patterns used in the authentication process; the higher the number, the securer the process.

This article is more about an idea than about a rigid and prescriptive method of authentication; a further process of trial and error is required. Therefore, for the sake of the clarity of exposition and for offering a reasonable level of security and easiness for the user to remember it, I considered an array of 9 identical −and equally distributed in space− pads, 8 of which have 25 equally distributed dots/buttons. Imagine a touchscreen of a device/card with the following arrangement[[1]](#footnote-1):

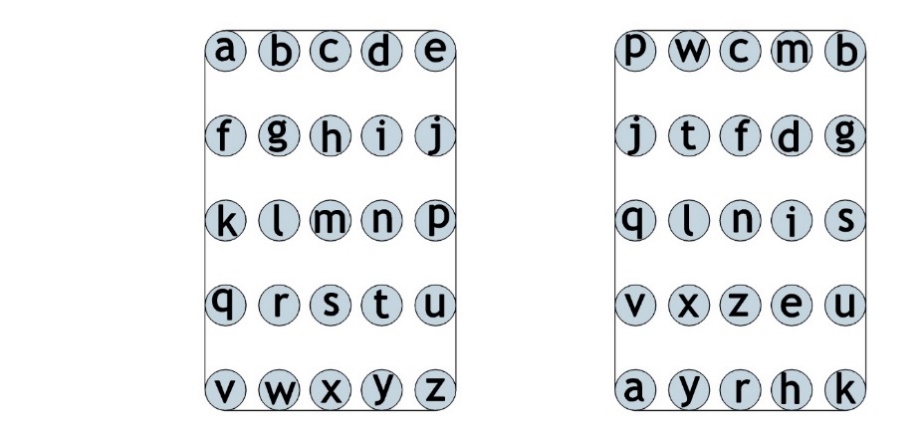
**Fig. 1**



The last pad on the right could function by default for authentications in low-value/importance every day transactions, without requiring the intervention of the enrollee and so it does not need to be visible for him during the operation. I will come back with details.

To improve the security of the communication device/data base, every dot could be also representative of, and it is proposed so in this method, a letter of the English alphabet (all except “O” which anyway, in written texts, it is often confused with the numerical digit zero; O ≠ 0), distributed either in a personalised consequent and logic order or following a random one generated by default, both shared by and known only to the server and the user/enrollee.

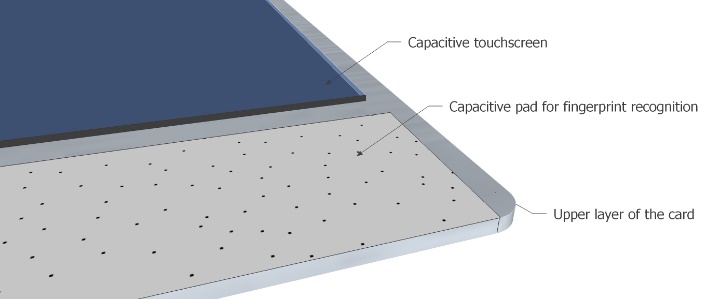
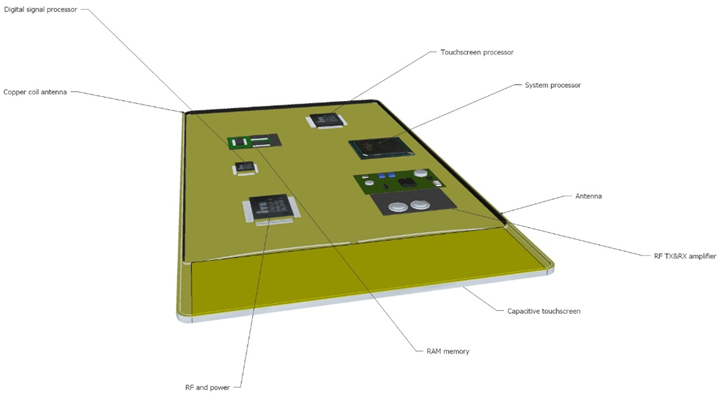
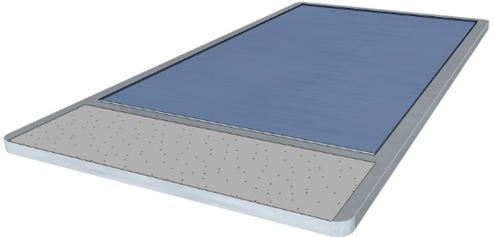
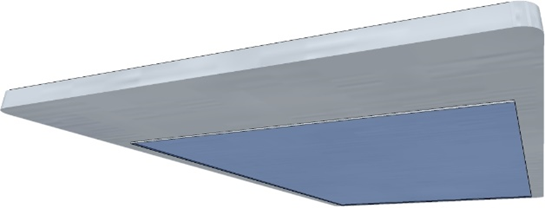
**Fig. 2**



This is how far the user interface or analogic layer goes. Apart from that provided by the personalised pattern, the security of the process is ensured and results in its most part from the virtual layers beneath.

Let’s consider a card equipped with at least the following features and technologies[[2]](#footnote-2):

**Fig.3**



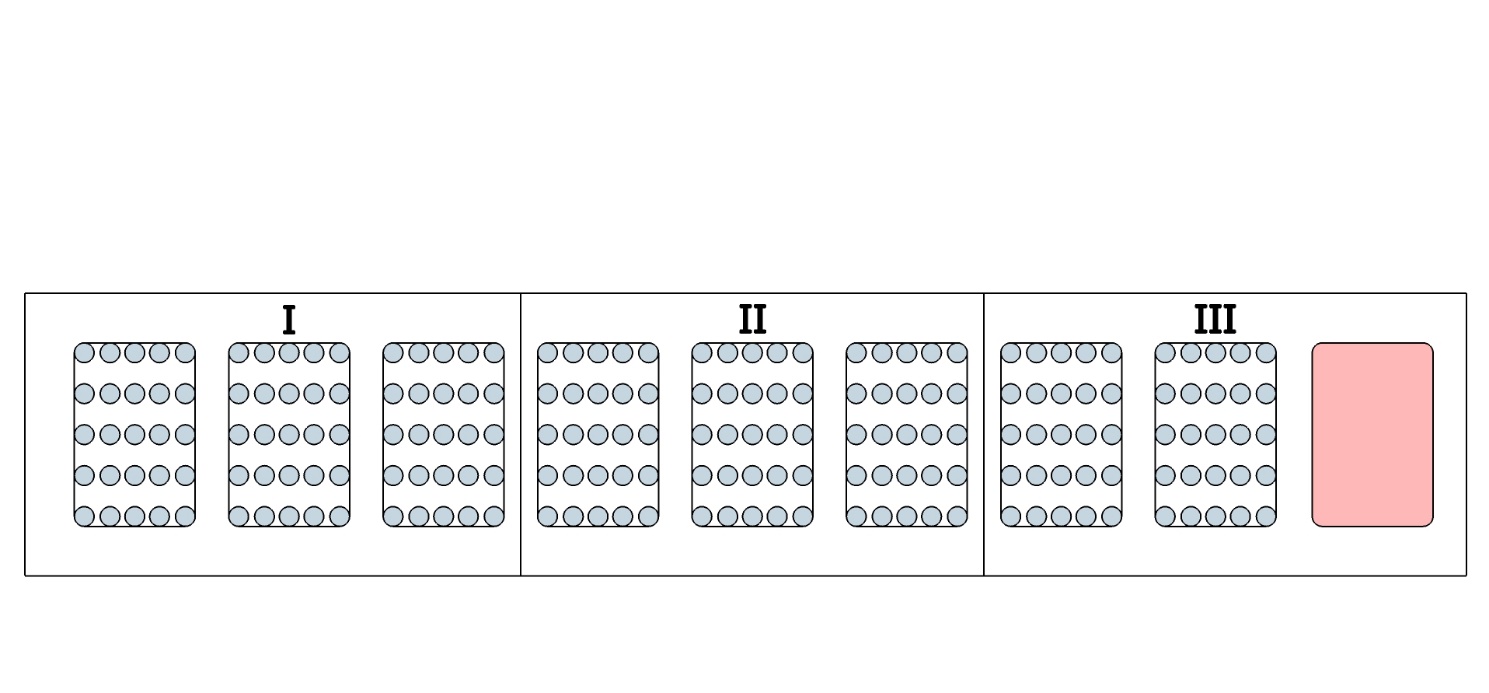
All the technologies considered here exist and are used today in many commercial devices like the one hypothetically proposed here or with similar functions. The nanoscale of the technologies in the components performing its diverse functions will allow for the card to have a size no larger than a usual debit/credit card, maybe a few millimetres thicker, while performing all its functions securely and with precision. Sensors could also be fitted inside the card to protect it against the corruption of the hardware by brutal force with the intention of extracting the operating software permanently stored in the device; given certain negative of positive conditions depending on the type of sensor, they should be able to completely purge the memory of the device when triggered.

**Inside the PIP authentication method**

1. On the analogic layer

A pattern or patterns that also mean something to us are always much easier to remember than, say, a series of abstract symbols composed of bars and/or curves. This is a notable ability, and an advantage in terms of security, of ours that built up along thousands of years of evolution and that the method proposed here fully benefits from, giving it a new (technologically and evolutionary) utility. This will depend on the imagination and the memorisation techniques familiar or instinctive to the enrollee in the process; any of this variables will have no diminishing effect on the security. So, in our example, I will consider the word “letter” as compound authentication pattern. Consider that the user chooses to start the pattern on the second pad. The enrolment process could be represented like this:

**Fig. 4**



Entering the character-like-pattern/s will be done as writing by hand and following natural ways of execution; it will always depend on the natural handwriting style of each enrollee. The best part of it is that she/he does not have to write down or save and keep safe this information making so the entire system open to failure/attacks. This precise inflection point is where the system becomes simple and intuitive for the user: a natural, unreflecting and instant retrieval from his memory of the information that encodes the patterns. The way the strokes are made, i.e. the direction and the order in which the starting and intermediary dots are entered, connected and repeated (here the drawing of “r” is continuous, but could well be built up by at least two strokes that coincide in one or more dots), will have a crucial bearing in the output number that results from the numbers and the operations they stand for in the virtual layer. I will come back with more details. If one or more of the pads are left blank, in our example the first and the eighth (any other two among the eight ones available could also be), the device will always render a default output value, i.e. a real number, which, as such, could be negative, positive and with, say, two decimals, and will allow for the production of an indefinite amount of them, all except zero (which, it is well known, multiplied by any number the result will be always zero and also that no number can be divided by zero), and this, of course, will amount to increase the security of the authentication process.

1. The virtual layers

From a conceptual point of view, the working of the virtual layers beneath is quiet simple. It basically combines and gives mathematical form and meaning to the information provided by the user −her/his fingerprint or finger’s veins, a four digit PIN and the chosen patterns− and the numbers and operations generated by and contained in the software of the device. The entire process is composed by at least these stages:

1. One or more parties who electronically identify (in the sense that identification ≠ authentication) her/himself, in our example by means of a card, and the operation she/he intends to carry out. All the information, along with the unique number identifying the authentication device, is then sent to the server. I may describe this stage as “the hand shake”; if intercepted by an attacker, little could happen.
2. Subsequently, the server generates a random series of patterns and transcribes them into letters according to their correspondence in the arrangement of pads and dots. Each pad is identified by a colour code and each dot inside them is identified by a letter, being all the information pre-established and shared only by the parties of each end of the process. Then a particular and unique string of data is generated and electronically sent to the enrollee/user.

Operation ID; including date and time.

At least one pattern for each one of the dividing blocks: I, II and III, in our example.

Colour code + letter that corresponds to the relevant dot.

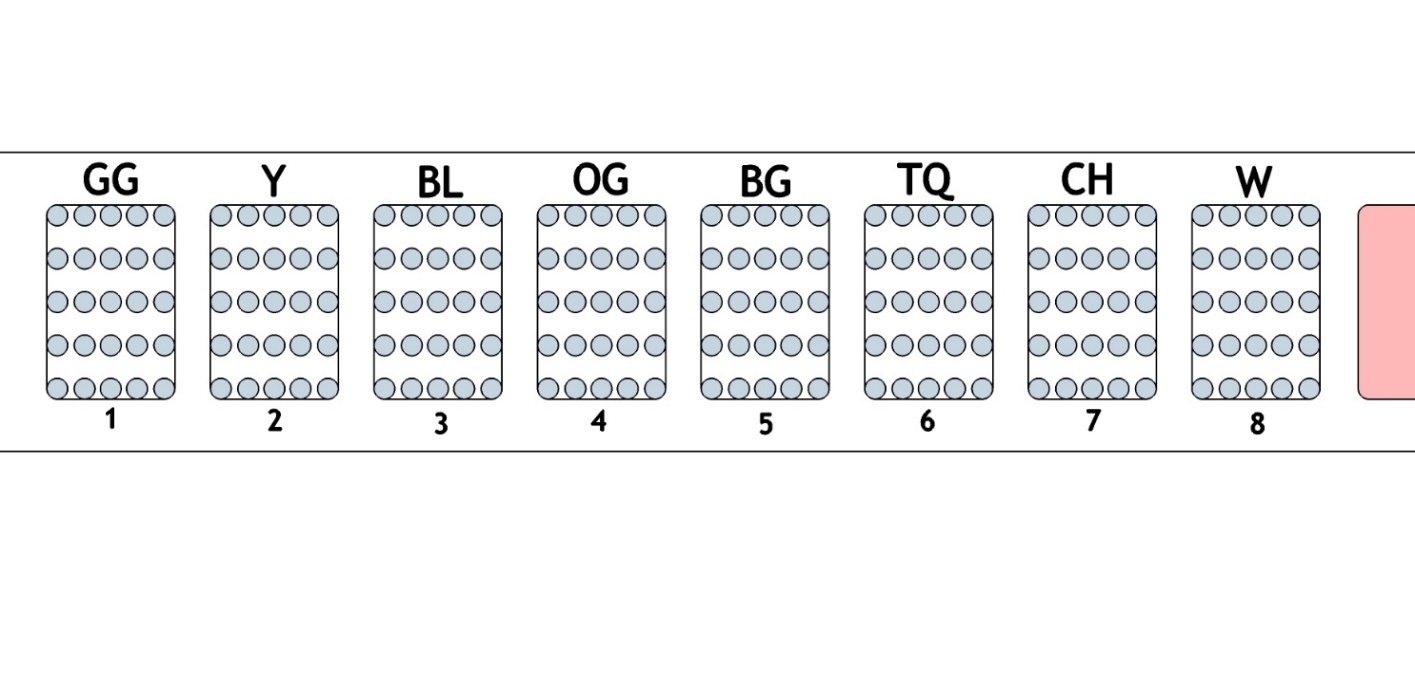
|  |  |  |
| --- | --- | --- |
| nnnnnnnnnnnnnnnnnnnn | + | aa+a/…/aa+a |

1. Once the string of data is received, the authentication device interprets and digitally distributes it to the relevant pads and dots in the virtual layer.
2. The device, using the numbers corresponding to the activated dots and the device pre-established operations that correspond to each of them, calculates and renders an OTP, i.e. a unique one-off PIN, which is then communicated to the server; if it corresponds with the one calculated in parallel by the server, using the same correspondences of letters, numbers, operations and sequences, the user is authenticated and the operation is authorised.

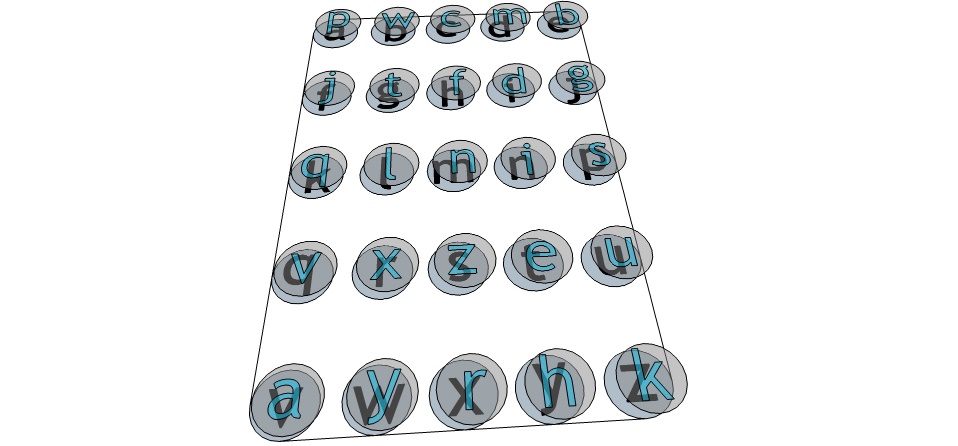
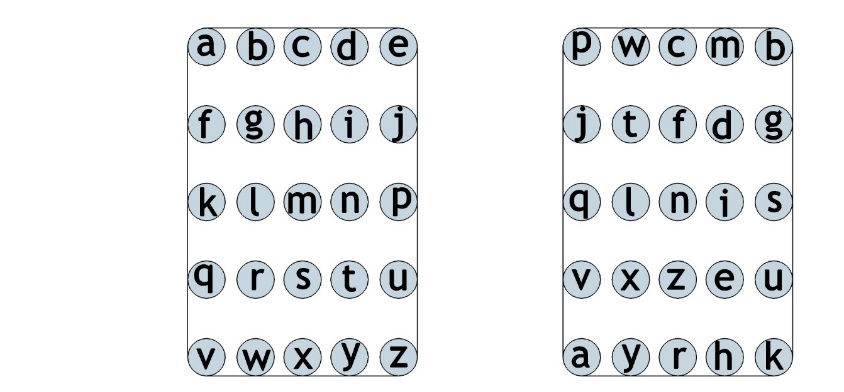
In our example, take the followings:

*Colours pre-assigned to each pad*. 1. grass green (GG), 2. yellow (Y), 3. blue (BL), 4. olive green (OG), 5. beige (BG), 6. turquoise (TQ), 7. charcoal (CH), 8. white (W).

**Fig. 5**



*Letters pre-assigned to each dot.*

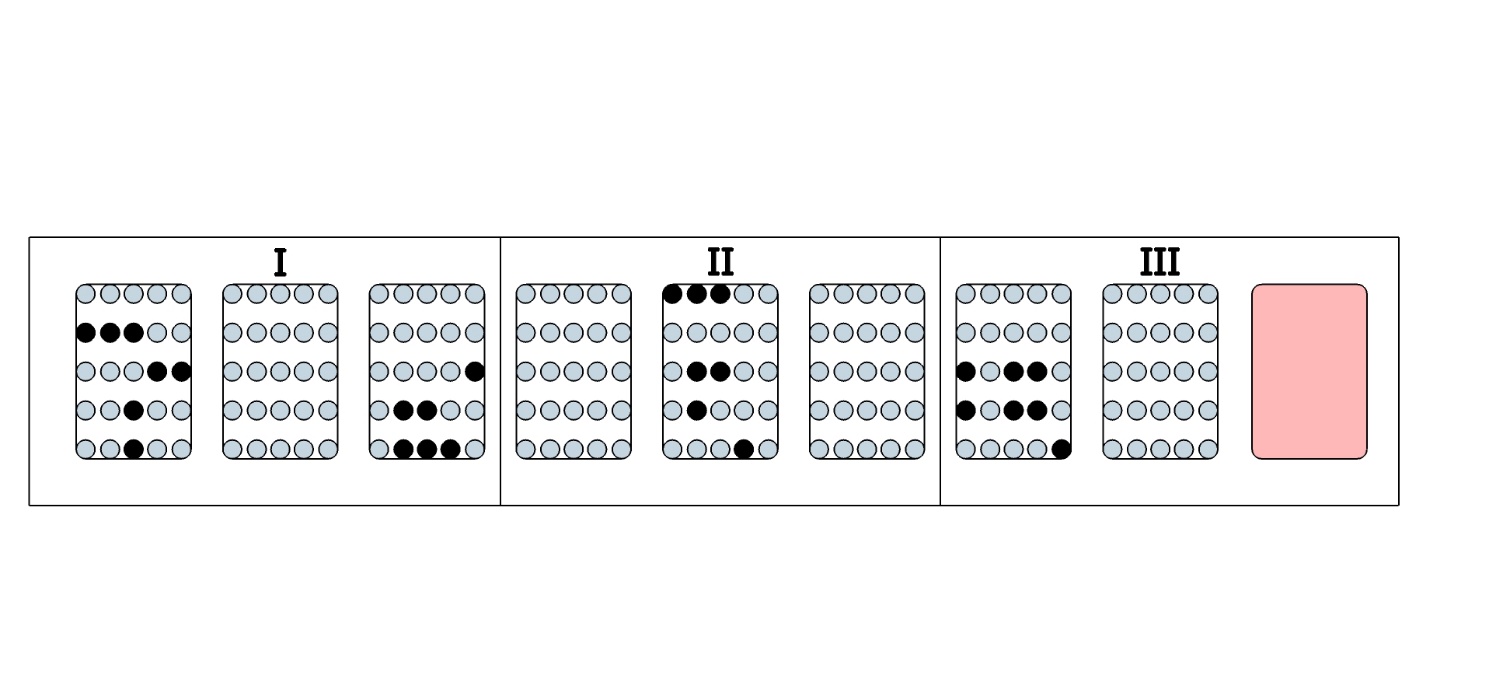


**Fig. 6**

To make exposition and understanding easier, the same distribution of letters has been considered for each of the 8 pads. However, establishing different and unique arrangements for each one of the pads is advisable to increase the security of the system.

*Server-generated patterns.*

**Fig. 7**



The patterns generated by the server translate, in our example, into the following string of characters:

*BG-pwclnxh/BL-sxzyrh/CH-qnivzek/GG-jtfiszr*\*

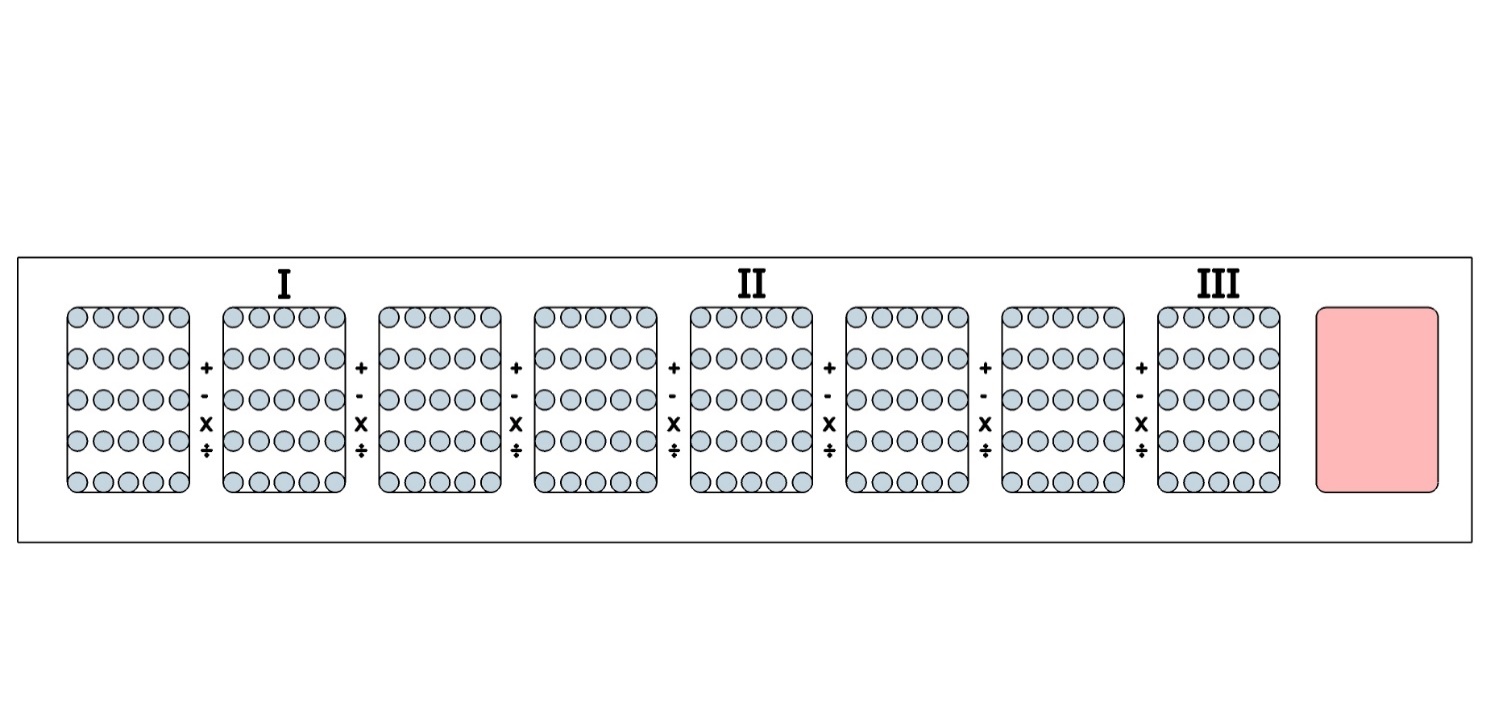
\* For communication purpose only, the sequence 1,2,3… of the pads has been shuffled in order to increase security.

As the virtual layers and the software only understand numbers, the patterns, and the fingerprint[[3]](#footnote-3), need to be converted into numbers.

*Converting patterns into numbers*:

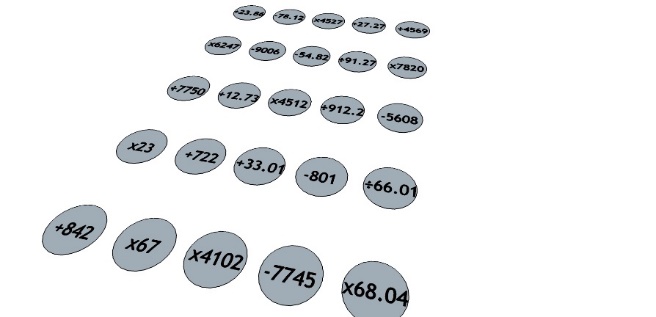
The mathematical operations (+, -, x or ÷) between the pads and the ones corresponding to each dot could be permanently integrated in the card, in its basic software.

**Fig. 8**



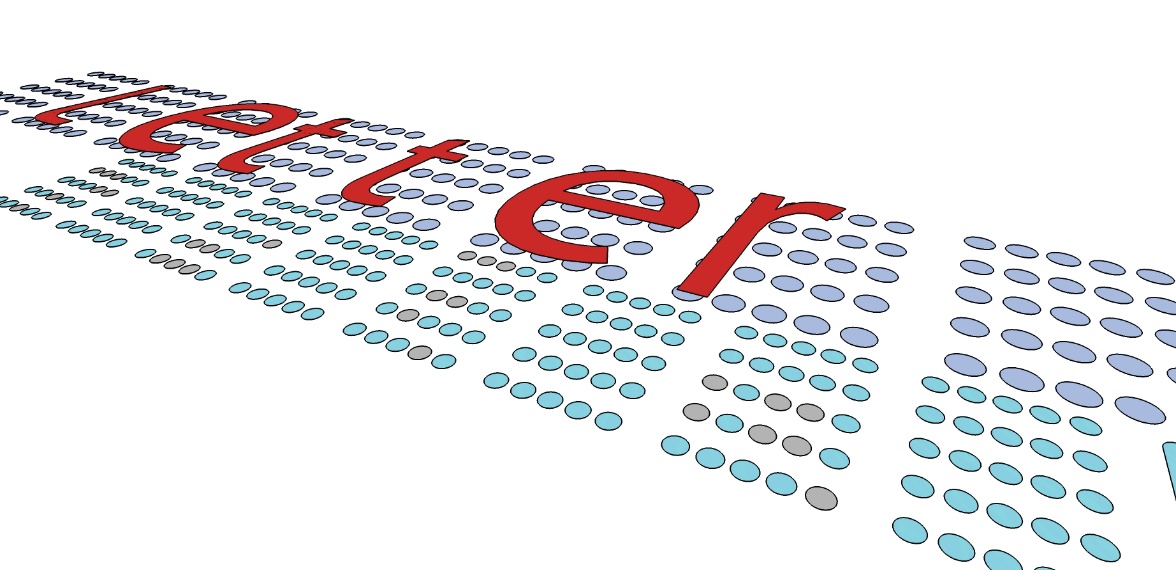
The numbers corresponding to each dot could be permanently integrated into the software of the card. However, to increase the security of the system, these numbers could be drawn from the numbers generated by the fingerprint of the user and distributed according to specific instructions given by operational algorithms included also in the software of the card. Algorithms could also establish the position for each number and operation. In order to increase its security, it is preferable that the device/card contains as little information as possible in its permanent memory; being of little use in the event that the device is stolen or lost. A PIN entered by the user at the beginning of each operation or series of operations and for a certain amount of time, say two hours, could make work these algorithms and ensure a considerable level of security.

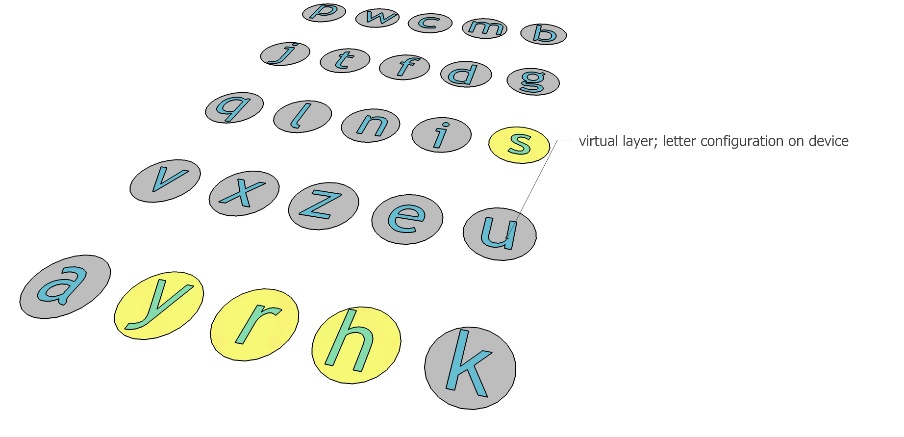
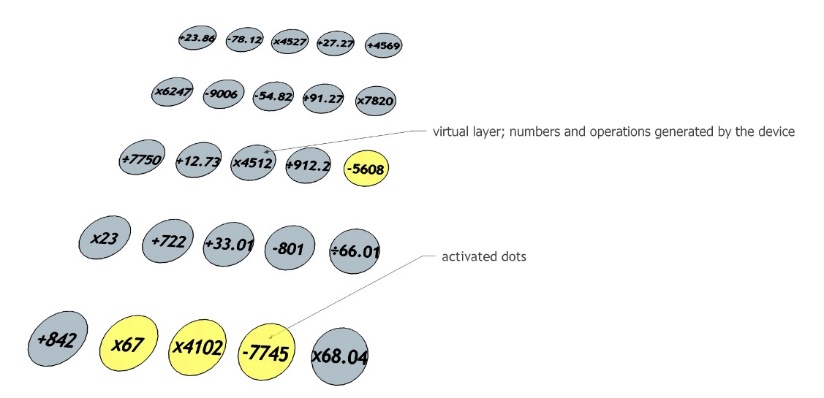
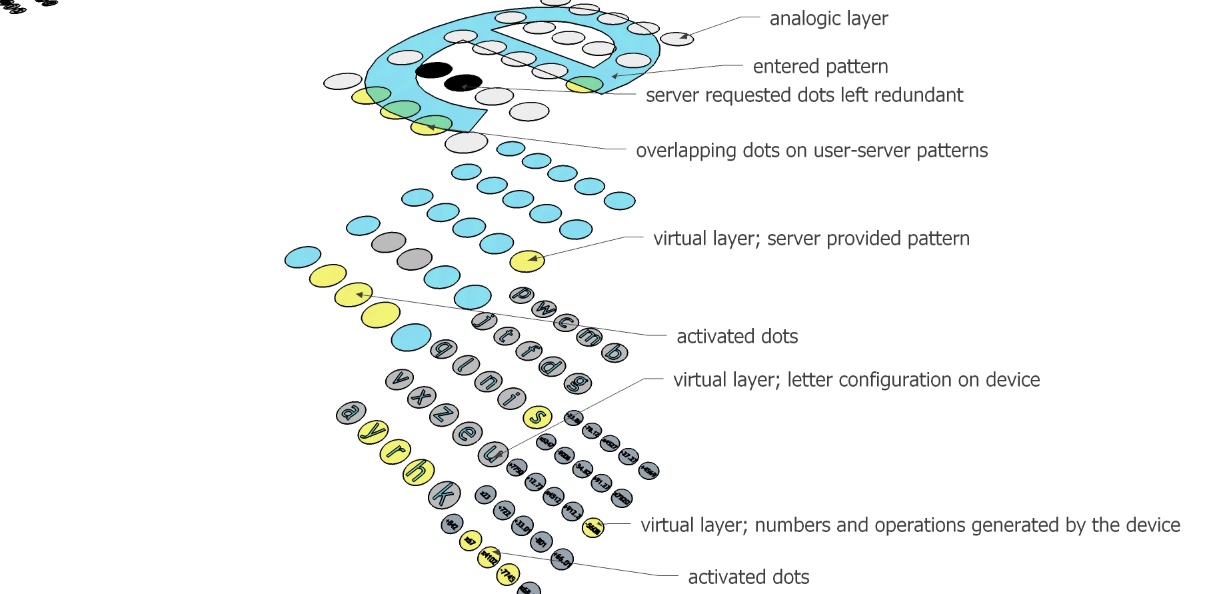
**Fig. 9**



In our example, the patterns entered by the enrollee on the analogic layer and the ones generated by the server on the virtual layer will overlap as follows:

**Fig. 10**





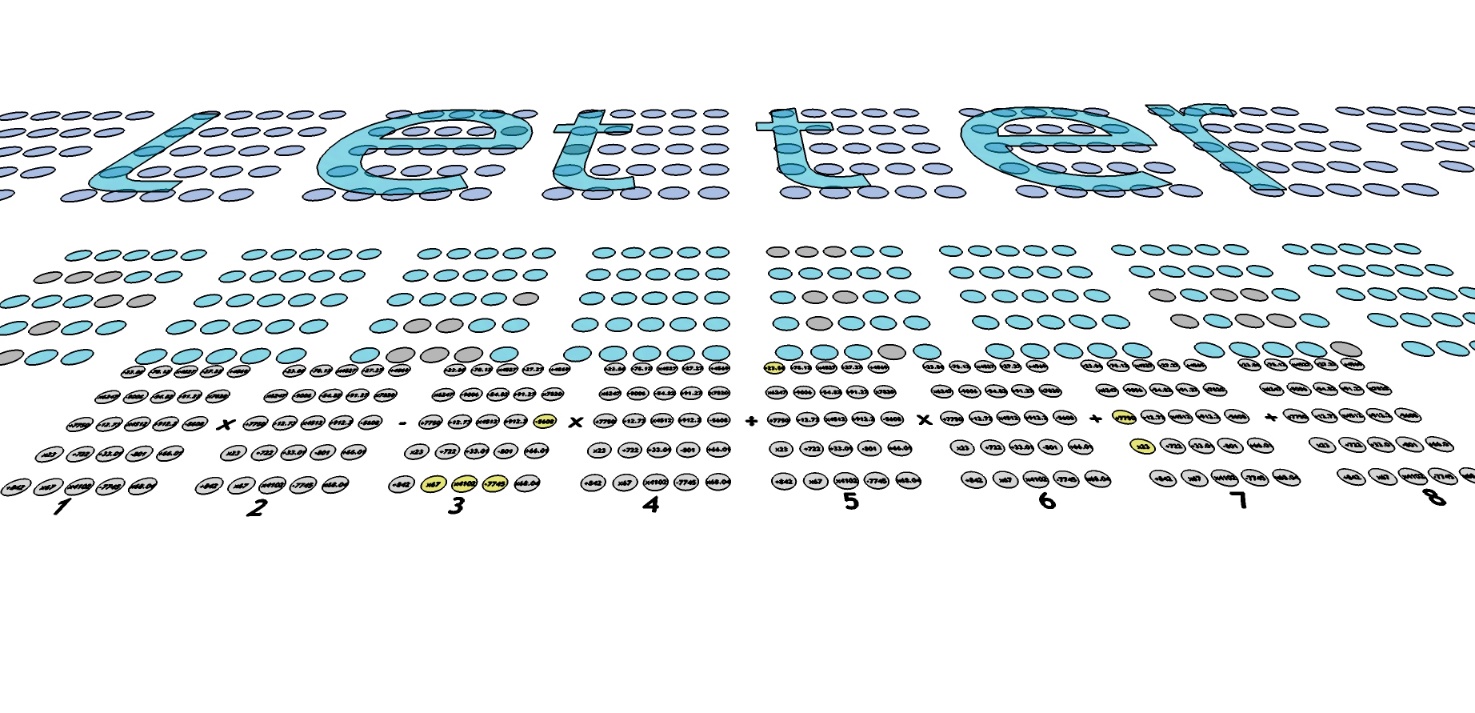
The resulting overlapping layers of, for example, the 3rd pad will look as follows:

**Fig. 11**

1. The one-time-password

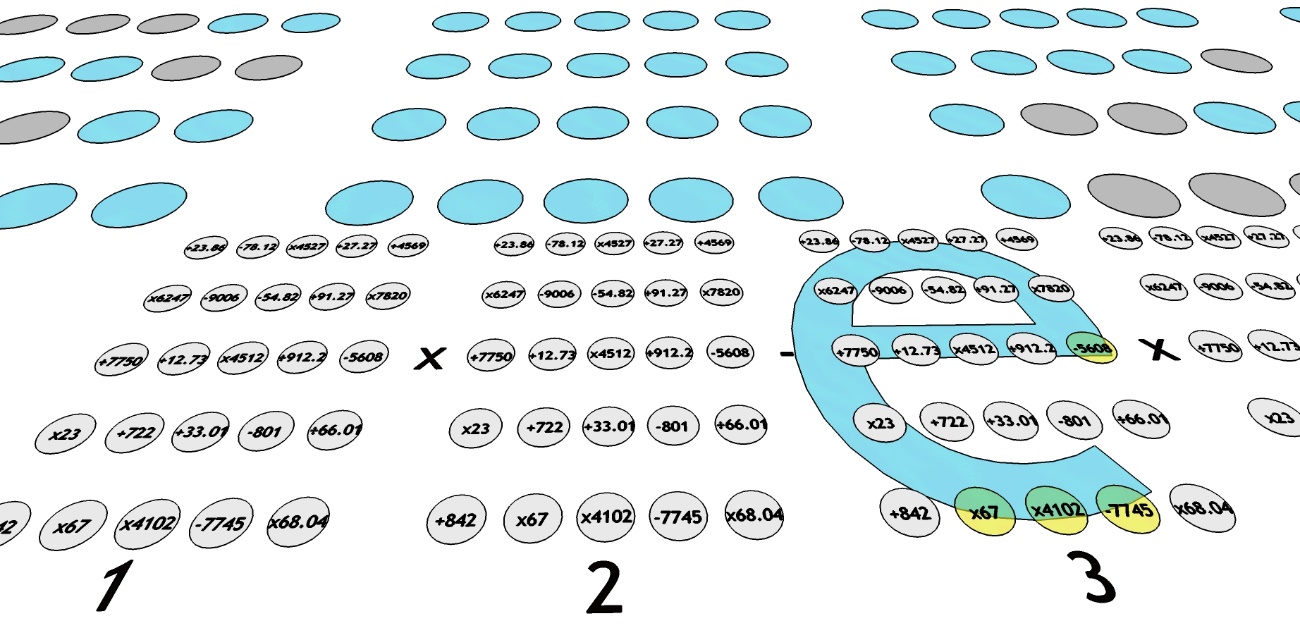
Now that the device has assigned numbers and operations to each dot contained in each one of the 8 pads, the server has provided the pattern, and the user has entered the fingerprint, the PIN and the personalised pattern, the final and most important stage develops: the calculation of the OTP which authorises the operation.

**Fig. 12**



To each pad and to every single dot corresponds an operation (except the first of the pads or of the dots, where the series of calculations start). First, the calculations on each pad containing active dots are made, then the default numbers corresponding to the pads resulted blank are added to the string of operations.

**Fig. 13**



In our example, the 1st, the 2nd, the 4th, the 6th and the 8th resulted blank, either because the server did not ask for a pattern on that pad or the user did not enter any; there should always be a dual correspondence on the pads of server/user layers for the device layer of numbers and operations to give a different number than the default one already filled.

So, the default number/value is calculated as follows:

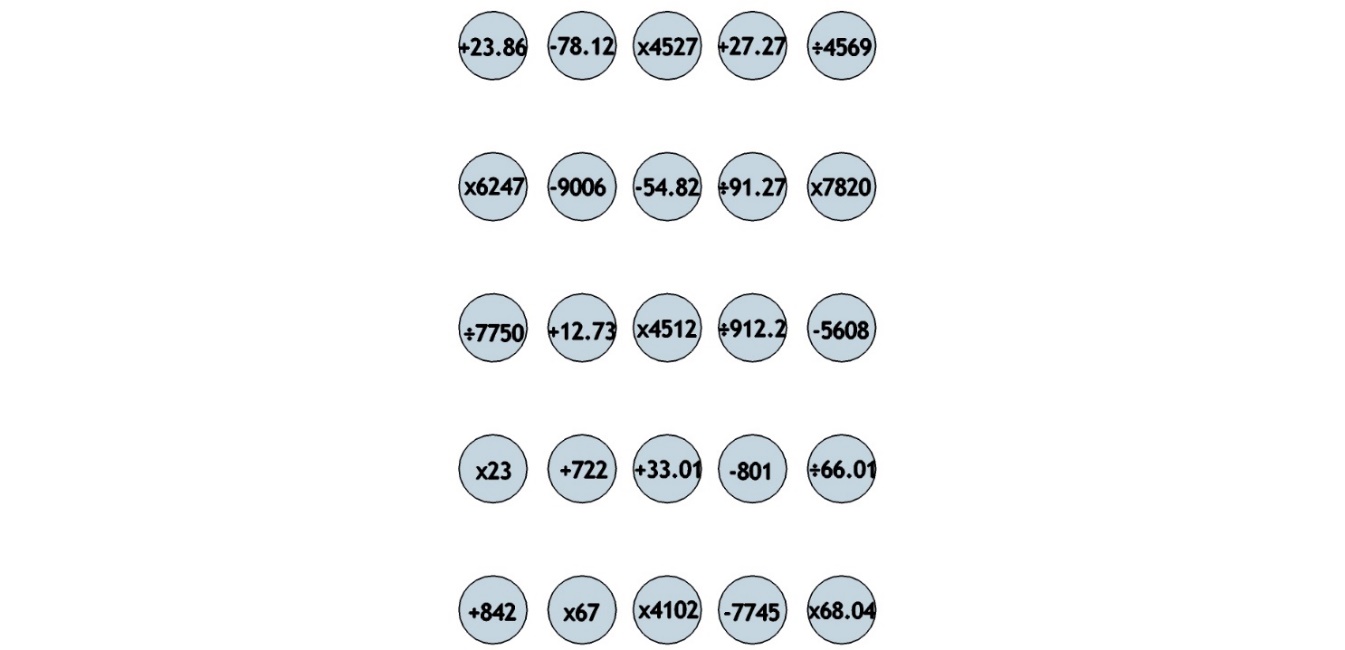
23.86[[4]](#footnote-4) - 78.12 x 4527 + 27.27 ÷ 4569 x 6247 - 9006 - 54.82 ÷ 91.27 x 7820 ÷ 12.73 x 4512 ÷ 912.20 -5608 x 23 + 722 + 33.01 - 801 ÷ 66.01 + 842 x 67 x 4102 - 7745 x 68.04 =

**[[5]](#footnote-5)**

**- 928,369,080,805.94**

This number, in our example, is also assigned to the 9th pad, i.e. it will be the default value that the card transmits during the authentication process in operations/transactions of low importance or value. The card, in all these situations, will work as an e-wallet.

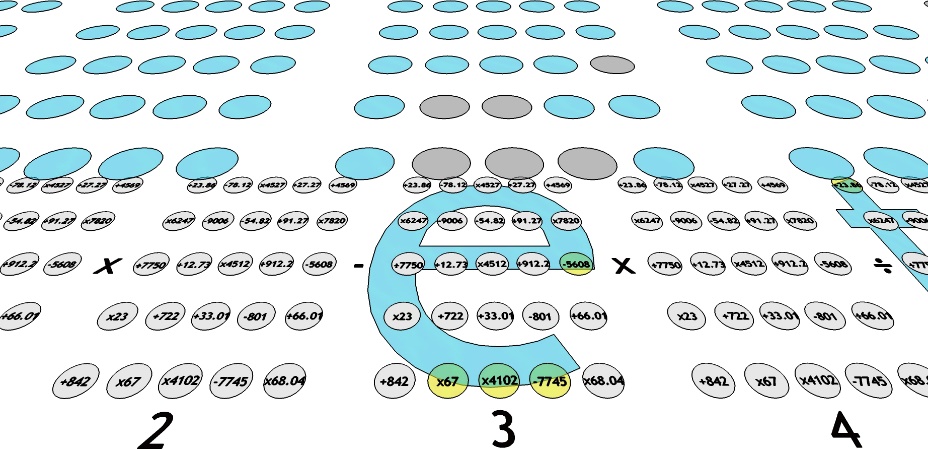
**Fig. 14**



The other three pads, the 3rd, the 5th and the 7th, will render the following numbers:

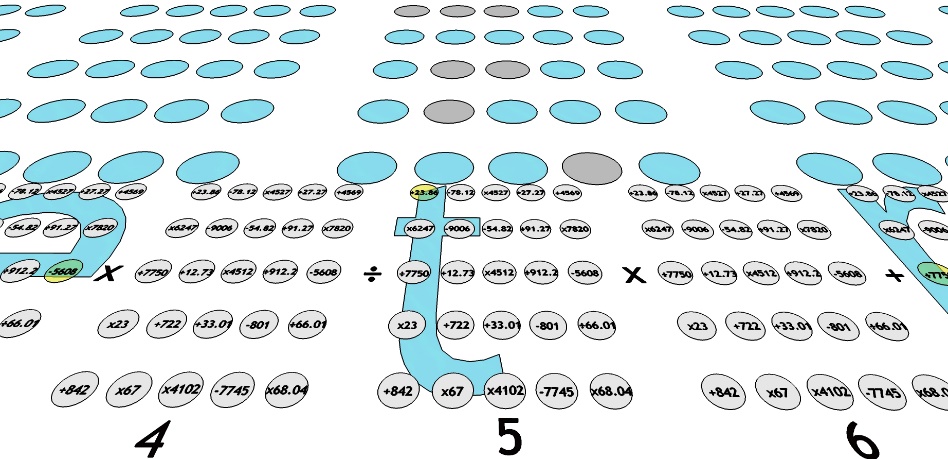
* the 3rd, **+1,541,261,327.00** (5608 x 67 x 4102 - 7745[[6]](#footnote-6));

**Fig. 15**



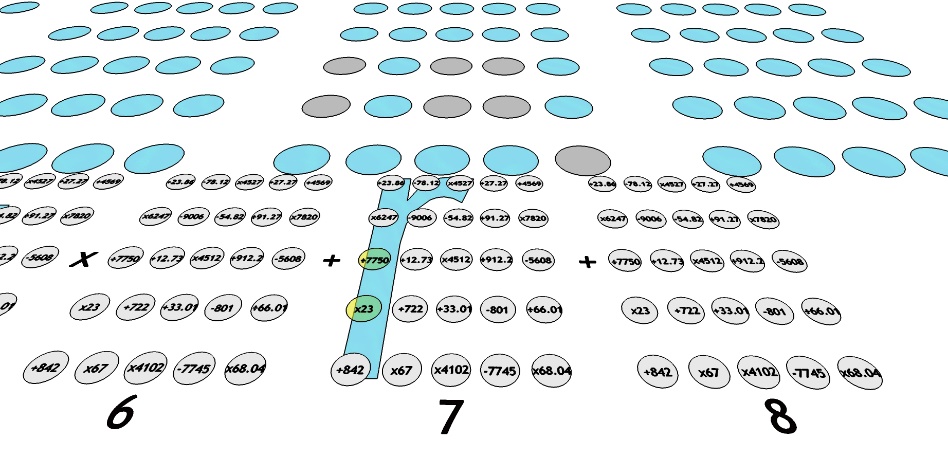
* the 5th, **+23.86**

**Fig. 16**



* and the 7th, **+ 529** (7750 x 23 x 23 ÷ 7750[[7]](#footnote-7)).

**Fig. 17**



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Pad # | 1 |  | 2 |  | 3 |  | 4 |  | 5 |  | 6 |  | 7 |  | 8 |  |  |
| Concept | D | O | D | O | C | O | D | O | C | O | D | O | C | O | D | O | Total |
| Value | −928,369,080,805.94 | x | \_,,\_ | − | +1,541,261,327 | x | \_,,\_ | ÷ | +23.86 | x | \_,,\_ | ÷ | + 529 | + | \_,,\_ | = | **−5.885136770261759 E+43** |
| D = default value  C = customised value  O = operation | | | | | | | | | | | | | | | | | |

Finally, the OTP is obtained as follows:

Not surprisingly, the OTP in our example resulted in a very large number (x 1043). This, and the fact that works one-off, will make the cracking of the system practically impossible.

All the data generated during the authentication process will be stored in the volatile memory of the device and deleted upon completion of the operation, i.e. once the authorisation is granted and safely received by the user/s. Some data may last for longer in the RAM, like the one representing the default value in the pads left blank, i.e. there was no patterns coincidence, and in the operations of low-value pad; this will depend on the user’s personalised configuration of the operating software of the card, but it will be deleted from the memory in any case by default after a reasonably useful period of time, say, 8 hours, counted from the first operation of the day on.

Finally, with regard to the minimal costs and amount of hardware needed to implement this method, the hypothetical card is supposed to make the process easier and simpler for the user. Nevertheless, other pieces of hardware, like analogic commercial devices equipped with keys and buttons and non-touch screens, instead of more technologically advances touch screens (which are more expensive), could well perform the same functions implied in the method and ensure the same level of security. What is more, the communications between the server and the user could be well done on cheaper devices or technologies commercially available, like analogic telephone handsets (communicating the colour codes and corresponding letters -see above- by means of human voice or telephone keypad frequencies of a push-button telephone, also known as Touch-Tone), or over the internet (by filling boxes on a screen, for instance) without using a device able to receive, send and capture patterns; i.e. the method could well work without the virtual layers in-between and the numbers involved. If this is the case, the OTP will be made up only by colour codes and letters. The process may require more actions and time on behalf of the user, i.e. being analogic in its most number of stages, but the sufficient level of security will be in any case preserved. This could also be an advantage and competitive edge over competitors as the initial investment required will be significantly lower. Considering that many users in the West have already smartphones equipped with advanced technologies, being able to adapt and perform non-native versatile functions/applications, the PIP method could be the next revolutionary authentication app.

1. Conclusion.

The method proposed here seeks to improve the security of e-authentications. Despite being in its incipient stage and requiring further feasibility tests, the method could nevertheless be considered as a starting point for debate and for alternative solutions to the existing methods, overcoming thus the actual, and apparently little acknowledged, technological stalemate.

It basically combines and converts analogic inputs possessed and/or known by the user into virtual/digital means of authentication.

Its mayor advantages towards security are:

* intuitive and simple on the user end, while intricate and complex in the middle;
* partial use of patterns in the authentication process, so that each transaction/operation will have a unique one-off authentication code; any potential attacker will never have access to the patterns entirely and will never be able to reconstruct them from the partial information illegally intercepted and
* low initial investment with potential rapid surpassing of the critical mass required for its success; the method could be implemented and used in existing commercial devices and technologies.

The drawbacks I see at this stage could come from developing the software needed, a field in which I have no academic backgrounds. Until the software is proved feasible, the method, audacious that may be, remains a mere exercise for the mind and a call for hope for a better security for millions of worried users who seem being left on their own *devices*. I personally hope that, at the very least, the idea depicted in this article, along with the encryption method I proposed in a previous [article](https://drive.google.com/file/d/0B3G_QeRwjH-VSHlweTZ3TGs5OE0/edit?usp=sharing), will draw sufficient attention and serve as a starting point for debate towards an improved security for all.

Ciprian Galaon

Lawyer-linguist

Email: cgalaon@hotmail.com

1. No IT programming is involved in or has been experimented for the purpose of the method proposed here. Given the ubiquity of commercial devices able to perform functions similar with the ones referred or expressed here, the method has been conceived based entirely on the assumption that the programming of the software and the algorithms needed to run the authentication process is reasonably feasible. Considering this and the speculative character of this article, the method should be able to stand on its own merits to any potential reviewer. [↑](#footnote-ref-1)
2. No IT programming is involved in or has been experimented for the purpose of the method proposed here. Given the ubiquity of commercial devices able to perform functions similar with the ones referred or expressed here, the method has been conceived based entirely on the assumption that the programming of the software and the algorithms needed to run the authentication process is reasonably feasible. Considering this and the speculative character of this article, the method should be able to stand on its own merits to any potential reviewer. [↑](#footnote-ref-2)
3. Converting fingerprints into numbers is reasonably achievable. In one of the forums on the Internet [this](https://drive.google.com/file/d/0B3G_QeRwjH-VdTBUV2ZIMFpocjA/edit?usp=sharing) is proposed. [↑](#footnote-ref-3)
4. “+”, according to the coherence rule, the first operation sign has been omitted. [↑](#footnote-ref-4)
5. although the digits after the comma are .9492, as a rule, only the first two are considered. [↑](#footnote-ref-5)
6. presuming that the user’s e-shape-pattern starts in dot “+12.73” and continues until dot “-7745”; also, first operation sign excluded. [↑](#footnote-ref-6)
7. again, excluding the first operation sign before the dot “7750” and following the strokes of the “r”, first downwards, then upwards. [↑](#footnote-ref-7)