The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs

T.V. Laptyeva[1], S. Flach[1] [(a)] and K. Kladko[2]

[1] *Max-Planck-Institut für Physik komplexer Systeme - Nöthnitzer Straße 38, D-01187 Dresden, Germany*
[2] *Axioma Research - 555 Bryant Street, Palo Alto, CA 94303, USA*

PACS 05.45.-a – Nonlinear dynamics and Chaos
PACS 89.20.Ff – Computer science and technology
PACS 89.75.Fb – Structures and organization in complex systems

Abstract. - Vulnerabilities related to weak passwords are a pressing global economic and security issue. We report a novel, simple, and effective approach to address the weak password problem. Building upon chaotic dynamics, criticality at phase transitions, CAPTCHA recognition, and computational round-off errors we design an algorithm that strengthens security of passwords. The core idea of our method is to split a long and secure password into two components. The first component is memorized by the user. The second component is transformed into a CAPTCHA image and then protected using evolution of a two-dimensional dynamical system close to a phase transition, in such a way that standard brute-force attacks become ineffective. We expect our approach to have wide applications for authentication and encryption technologies.

Introduction. – Computer and information security has been subject to intensive research for over 50 years. This included investigation of cryptographic methods, as well generic security of computing devices, operating systems and networks. However, it is only relatively recently the importance of the human factor has been given proper attention. Passwords are the common method for authentication and encryption used to secure digital life. Humans have limited capacity to remember passwords and tend to select passwords that are too simple and predictable. Security breaches related to weak passwords are widespread events. Consumers and enterprises around the world are looking for ways to address the weak password problem [1, 2]. In this paper we propose a method to address the problem by combining chaotic dynamics, phase transitions, and pattern recognition advantages of the human brain. A major building block of the proposed algorithm is the dynamic behavior of complex extended non-linear systems, in particular, Hamiltonian lattices close to a phase transition [3,4]. These systems display non-ergodicity, deterministic chaos [5], and spontaneous formation of coherent space-time structures. Building upon dynamical chaos and computational round-off errors and utilizing superiority of the human brain over computers with respect to pattern recognition, our method protects a secret token, which can be used, in combination with a regular password, to derive a secret key for data encryption.

It was estimated in 2009 that 86% of US companies use password authentication and encryption [6]. A weak password used with a strong encryption or authentication algorithm potentially makes a computer system vulnerable to brute-force password search attacks. Studies have shown that users will generally address the password complexity problem by using simple predictable passwords [7, 8]. Schneier examined 34,000 MySpace online passwords and concluded that 65% of them contained 8 characters, with most frequently used passwords being "password1", "abc123", "myspace1", and "password" [8]. Other user strategies include using the same password for every account, writing down passwords, storing passwords in files, and reusing or recycling old passwords. Horowitz reported that 15-20% of the users on a regular basis wrote down their password on a Post-it note attached to the computer monitor [8]. Another study found that 66% of users keep password paper records at work and 58% keep passwords in files [8].

Vulnerabilities related to weak passwords have significant economic effect globally. Results of a recent study [8,9] revealed that identity fraud affects nearly 5% of consumers, or nearly 10 million people in the USA per year.

[(a)] E-mail: flach@pks.mpg.de

The total annual cost of identity fraud in the United States was more than $55 billion in 2006 [9]. Vulnerabilities related to weak passwords have significant economic effect globally. Results of a recent study [8,9] revealed that identity fraud affects nearly 5% of consumers, or nearly 10 million people in the USA per year. The total annual cost of identity fraud in the United States was more than $55 billion in 2006 [9].

Cryptographic science utilizes discrete reversible functions that operate on bit strings and take a secret key as a parameter. As an example, Advanced Encryption Standard (AES) [10] specifies an encryption function approved for use by the US government. AES encrypts data in input/output blocks of 128 bits. The secret key lengths supported by AES are 128, 192, and 256 bits. These long key lengths were selected to make brute-force attacks infeasible.

Over the years, a number of more sophisticated cryptanalysis attacks were described for various cryptographic algorithms. Such attacks are usually very technical and algorithm-specific and rely on finding statistical correlations in the cryptographic function to extract information on the cryptographic key. However, an ideal cryptographic function depends on its inputs in a completely random way with no correlations present. Therefore, a brute search attack remains the essential attack used in real world to compromise cryptographic algorithms.

For a completely random secret key used with the AES algorithm, a brute-force attack is infeasible both presently and, probably, in the future. The situation changes dramatically, when the key is limited to a smaller subspace of keys. A common situation is that the key is either a password, memorized by a human, or is derived from a password using a function known to the attacker. A brute search over a small subspace can be done efficiently.

A typical brute-force search attack requires that the attacker is in possession of the encrypted text (Ciphertext) C, and that the true key belongs to a subspace of keys S. The attacker can mount a Ciphertext-Only Attack by iterating through the space S and attempting to decrypt C in each case into a Candidate Plain Text. Now the attacker needs to determine whether it is the True Plain Text. This Recognition Problem is, therefore, a necessary part of Ciphertext-Only Attack, and amounts to designing an efficient algorithm denoted as the Recognition Oracle (RO). Implementations of ROs make use of the block-encryption structure, standard file formats, and correlations in True Plain Text.

Scheme. – We assume that confidential data is encrypted by a symmetric encryption algorithm, such as AES. The encryption key used is a combination of a reasonable-strength password component (such as 10^5 combinations), which we denote as Short Password SP and an additional Strong Key SK. The difference between our method and existing cryptographic technologies is that the user is not asked to memorize SK. Instead, the graphical representation of SK is embedded into a two-dimensional image ISK of a momentary state of a nonlinear Hamiltonian two-dimensional lattice system. This embedding is similar to embeddings used for Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) [11–13], therefore, we also coin it password CAPTCHA or p-CAPTCHA. A time evolution of the two-dimensional lattice is then performed. The chaotic evolution transforms the p-CAPTCHA into a chaotic lattice state. Since our Hamiltonian system is close to a phase transition, this chaotic state will contain regularities at various space scales, such as a domain structures. If one encodes lattice site positions and velocities using floating point numbers, such regularities will be manifested in more-significant bits of such encoding, the less-significant bits will have pseudo-random nature due to the dynamical chaos in the system.

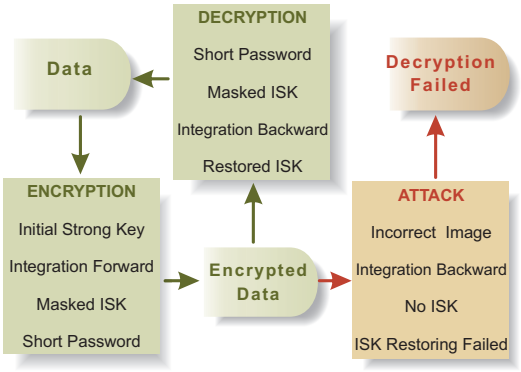

Fig. 1: Schematic flow of the encryption, decryption and attack processes.

This provides us an opportunity to split the state information for each lattice site into somewhat-regular and pseudo-random components by splitting each floating point number into, e.g., the most significant half and the least significant half. The most significant halves then form the somewhat-regular component of the state information that we store in plain text. The least significant halves form the pseudo-random component of the state information. We store this pseudo-random component in encrypted form, where encryption is performed using a regular password, memorized by a user. To restore the full state, one decrypts the pseudo-random component, and then combines it with the somewhat-regular component.

Let us now assume that both the somewhat-regular component (stored in plain text) and the pseudo-random component (stored encrypted) are available to the attacker. To mount a brute-force attack the attacker will scan through the password space. For each password the attacker will decrypt the pseudo-random component. Since the component is pseudo-random, the results of decryption will look the same to the attacker independent of whether the correct password was selected. Therefore, no

effective Recognition Oracle recognizing the correct password from an incorrect one can be built at this stage. On the next stage the attacker will combine the pseudo-random component with the somewhat-regular component to obtain the state of the system and integrate equations of motions in the reverse time direction to obtain a candidate p-CAPTCHA image. Only the correct password will lead to the p-CAPTCHA image. However images generated by the attacker for incorrect passwords will show the level of intra-image regularities similar to the correct p-CAPTCHA. Therefore, computer-based Recognition Oracles will not be efficient.

A legitimate user in possession of the SP can decrypt the pseudo-random component and combine it with the plain text somewhat-regular component. Using the time reversibility of Hamiltonian systems, the system is evolved in the reverse time direction to regain the p-CAPTCHA and recognize the strong key SK from the image. The combined SP and SP are then used to decrypt the actual confidential data (see Fig.1).

Implementation. – In order to implement the strategy described above, we consider a two-dimensional square lattice of $N \times N$ coupled double-well oscillators depicted in Fig.2, which is described by the Hamiltonian

$$\mathcal{H} = \sum_{i,j=1}^{N} \left(\frac{1}{2} p_{ij}^2 - \frac{1}{2} u_{ij}^2 + \frac{1}{4} u_{ij}^4 + \mathcal{F}_{ij} \right) ,$$
$$\mathcal{F}_{ij} = \sum_{k=\pm 1} \frac{1}{2} \left[(u_{i+k,j} - u_{ij})^2 + (u_{i,j+k} - u_{ij})^2 \right] . \qquad (1)$$

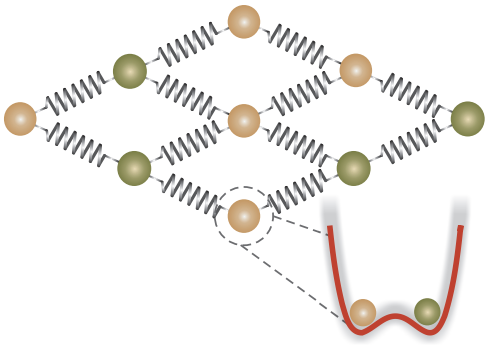

Fig. 2: The two-dimensional square lattice of coupled double-well oscillators described by Eq.(1). The springs indicate the nearest neighbour interactions. The double-well onsite potential for each oscillator includes two equilibrium positions $u_{ij} = \pm 1$.

The lattice indices i, j correspond to the two directions for the square lattice. The equations of motion read $\dot{u}_{ij} = \partial \mathcal{H} / \partial p_{ij}$, $\dot{p}_{ij} = -\partial \mathcal{H} / \partial u_{ij}$ and are invariant under time reversal. We use $N = 69$ and perform time evolution of the system using the symplectic Verlet algorithm [14]. The time step for the numeric integration is $h = 0.01$, and double precision is used.

The system (1) served as a simple model for structural phase transitions e.g. in ferroelectric materials as $BaTiO_3$ and also $SrTiO_3$ [15]. The phase transition is of the second order [16] at a certain critical value of the energy density which can be set roughly equal to the average temperature T. At high temperatures the oscillators traverse the potential barrier easily, therefore, the average polarization order parameter $M = \frac{1}{N^2} \left| \sum_{ij} \mathrm{sign}(u_{ij}) \right|$ is zero for large N. For low temperatures the energy of each oscillator is

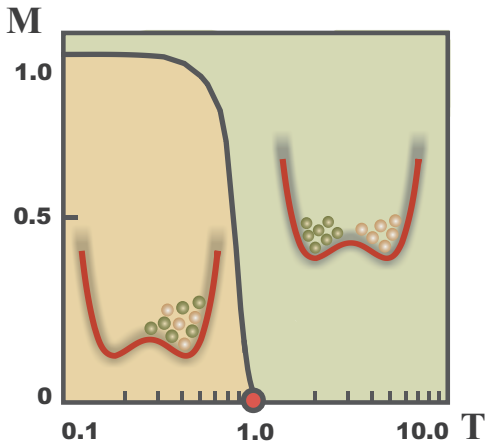

Fig. 3: Dependence of the order parameter M on the temperature T for Eq.(1). The red circle at the bottom indicates the operational point of the algorithm.

not sufficient to overcome the potential barrier, and the interaction between oscillators enforces an ordered phase with $M \neq 0$. The temperature dependence of M is shown in Fig. 3. The phase transition point is $T_c \approx 1$.

The evolution of system (1) in the vicinity of the transition point is characterized by a spatial correlation length which diverges exactly at the phase transition point. Close to the phase transition large clusters of the low temperature phase emerge and disappear spontaneously. To initialize the system, we assign random values to the momenta p_{ij} such that the kinetic energies $p_{ij}^2/2$ satisfy a Boltzmann distribution $\beta \mathrm{e}^{-\beta \mathrm{p}^2/2}$ with a temperature $T \equiv \beta^{-1} = 0.9$ (red circle in Fig.3) and coordinates $u_{ij} = 1$. We then integrate the equations of motion up to a time of the order of 200 time units (t.u.) at which all temporal correlations decay. The image of the thermalized local order parameter density distribution (the signs of the oscillator coordinates) is shown in Fig. 4.

After that we imprint the SK (here the word "CHAOS") into the system and obtain the ISK or p-CAPTCHA (see Fig. 5 and left top image "ISK/RESTORED ISK" in Fig.6).

In order to protect SK, we integrate the equations of motion further to some time τ (bottom-left image "MASKED ISK" in Fig.6).

Since the equations of motion are time reversible, we can invert the integration, and expect to regain the original

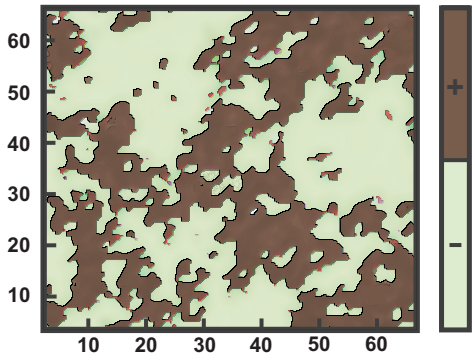

Fig. 4: The thermalized state of Eq.(1) with parameters $T = 0.9$, $N = 69$ in the color coding of coordinates after forward integration up to $\tau = 200$ t.u.

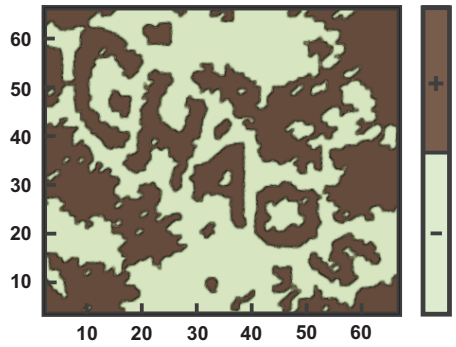

Fig. 5: *Initial* ISK (p-CAPTCHA) of Eq.(1) with parameters $T = 0.9$, $N = 69$ in color coding of coordinates. Note that the *restored* image (after forward integration to $\tau = 350$ t.u. and backward integration to the origin) yields practically the same image.

state ISK after back integration over the same time τ. This is particularly true for the Verlet discretization, which is also completely time reversible. However, the underlying dynamical system is non-integrable and, therefore, chaotic [17]. Small perturbations will grow exponentially fast as $e^{\lambda t}$ where λ is the largest Lyapunov exponent [17]. We also note that the numerical integration algorithm, while being perfectly invertible in time, generates round-off errors (for double precision, at the 15th digit after the point). These small errors will accumulate exponentially fast in time. Therefore, there exists the maximum loopback time τ_* which still allows return to ISK. For larger loopback times the image ISK is lost in the high dimensional phase space of the system after the loopback evolution is performed. We find that $\tau_* \approx 400$ t.u.

Our strategy is then to choose τ to be close to τ_*. With $\tau = 350$ t.u. we can still integrate backwards and regain the image ISK. The restored image is practically identical to the original p-CAPTCHA we started with in Fig.5.

Slightest errors in the velocities and positions of the oscillators will be amplified when integrating back, and inhibit return to ISK. Indeed, we show this by slightly detuning the coordinate of an oscillator in the final state far from the original image location (right bottom image "MASKED ISK WITH DETUNED SITE" in Fig.6): $u_{20,20} \to u_{20,20} + 0.00001$. Backward integration of the corrupted state leads to a loss of the ISK (right top image "NO ISK/RESTORING FAILED" in Fig.6). The state of the system integrated forward in time (left bottom image "MASKED ISK" in Fig.6) can be now be split into somewhat-regular and pseudo-random components. The pseudo-random component is then encrypted using SP. The somewhat-regular component is stored in plain text.

Knowledge of the password SP allows the legitimate user to decrypt the pseudo-random component and regain the correct state, which is then integrated in the reverse time direction, leading to ISK. The strong key SK together with the short password SP is now used in a combination as a secure secret token to decrypt protected data.

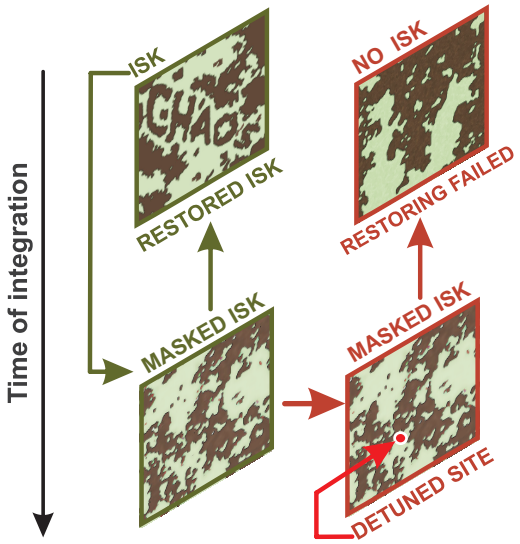

Fig. 6: The evolution of the image p-CAPTCHA into a chaotic state and its reobtaining by integrating backwards (two left images). A slight detuning of one oscillator coordinate $u_{20,20} \to u_{20,20}+0.00001$ (shown by the arrow in the bottom right image) of the chaotic state, followed by a backward integration, misses the image completely, leading to another random image of a chaotic state.

The attacker attempting a brute-force attack has to visually analyze each image obtained by time-evolution of each incorrect state corresponding to each incorrect password tried. For 10^5 SP combinations a good time estimate for this human-intensive activity will be days. Simply increasing the space of SP to 10^6 severely limits the attacker, while still maintaining a reasonably short SP.

Outlook. – To conclude, we present an approach that relates the fields of dynamical chaos, criticality, and pattern recognition to cryptography. This approach allows us to use the evolution of a chaotic Hamiltonian system near a phase transition to embed and protect a secret token that can subsequently be used for cryptographic purposes, such as encryption of confidential data. Our method can be readily and straightforwardly implemented on a wide variety of existing computer systems and devices and, to our view, provides a significant step forward in protection of confidential data as compared to the currently available methods of password-based encryption. We hope that our findings can open a promising topic for future research. Potential future directions include searching for optimal Hamiltonian and non-Hamiltonian systems to be used as a foundation for our method, optimizing the performance of the method so that it can be executed on devices with low computational power, as well as designing better image embedding and evolution algorithms to provide stronger protections against computer-based image recognition.

* * *

We thank P. Fulde and R. Khomeriki for useful discussions and a careful reading of the manuscript.

REFERENCES

[1] Sikorski R. and Peters R., *Science*, **278** (1997) 2144.
[2] Stross R., *The New York Times*, **Sept.5** (2010) .
[3] Cataliotti F. S., Burger S., Fort C., Maddaloni P., Minardi F., Trombettoni A., Smerzi A. and Inguscio M., *Science*, **293** (2001) 843.
[4] Donner T., Ritter S., Bourdel T., Oettl A., Koehl M. and Esslinger T., *Science*, **315** (2007) 1556.
[5] Stark J. and Hardy K., *Science*, **301** (2003) 1192.
[6] Zhang J., Luo X., Akkaladevi S. and Ziegelmayer J., *Eur. J. Inf. Syst.*, **18** (2009) 165.
[7] Adams A. and Sasse M. A., *Comm. ACM*, **42** (1999) 41.
[8] Hoonakker P., Bornoe N. and Carayon P., in *Proc. of the Human Factors and Ergonomics Society, 53rd Annual Meeting* 2009, p. 459.
[9] Monahan M. T., *Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary* (Pleasanton, CA: Javelin Strategy and Research) 2007.
[10] Advanced Encryption Standard, *FIPS*, **197** (2001) (available at http://csrc.nist.gov/publications/fips/).
[11] von Ahn L., Blum M. and Langford J., in *Advances in Cryptology, "EUROCRYPT-2003"*, Vol. **2656** 2003, p. 646.
[12] von Ahn L., Maurer B., McMillen C., Abraham D. and Blum M., *Science*, **321** (2008) 1465.
[13] Canetti R., Halevi S. and Steiner M., *Cryptology ePrint Archive*, **276** (2006) (available at http://eprint.iacr.org).
[14] Verlet L., *Phys. Rev.*, **159** (1967) 98.
[15] Schneider T. and Stoll S., *Phys. Rev. Lett.*, **31** (1973) 1254.
[16] Stanley H. E., *Introduction to Phase Transitions and Critical Phenomena* (Clarendon Press, Oxford) 1971.
[17] Lichtenberg A. J. and Liebermann M. A., *Regular and Stochastic Motion* (Springer, Berlin) 1982.