The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

2286-12

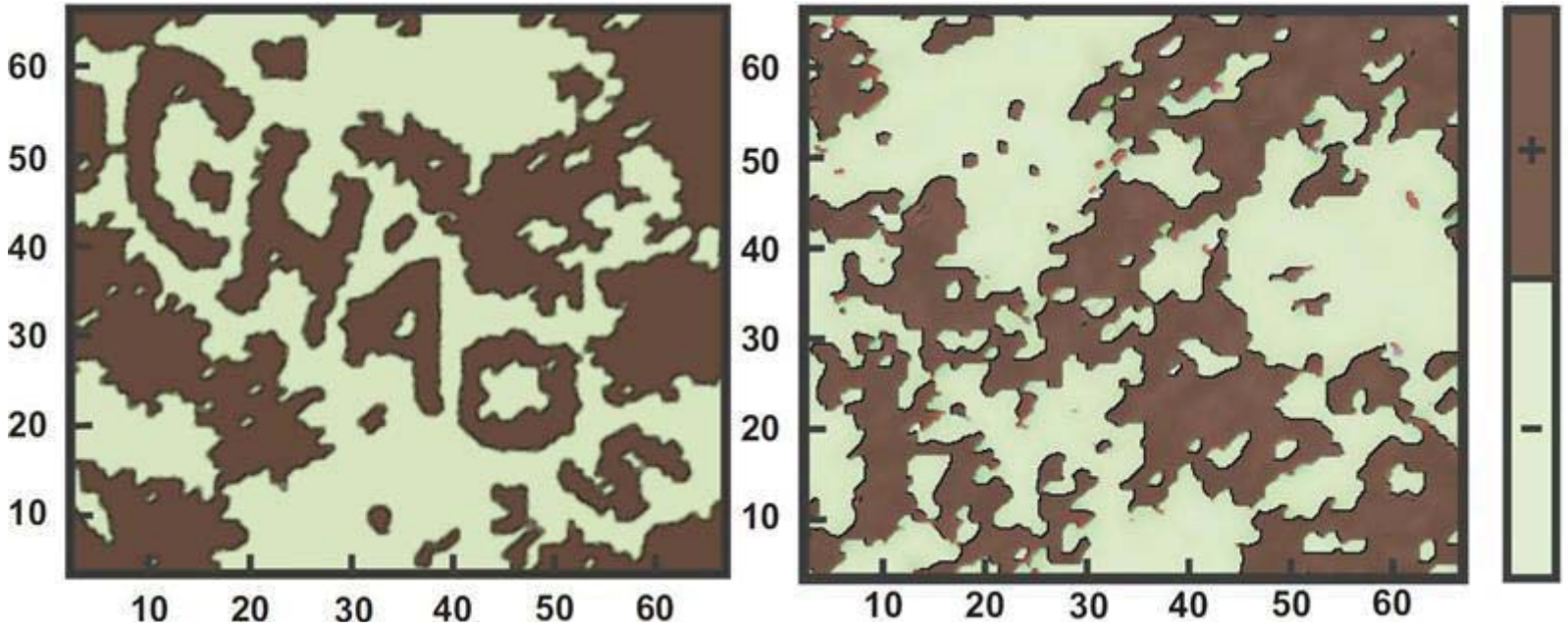
Workshop on New Materials for Renewable Energy

31 October - 11 November 201

Nonlinear Lattice Waves: Classical and Quantum
(fourth part)

Sergej Flach

Max Planck Insitute for the Physics of Complex
Systems Noethnitzer Str. 38
01187 Dresden
Germany


60
50
40
30
20
10
10 20 30 40 50 60
60
50
40
30
20
10
10 20 30 40 50 60
+
-


chpassword

Nonlinear Lattice Waves: Classical and Quantum

S. Flach, MPIPKS Dresden

mpipks

Three lectures and one tutorial:

- discrete breathers – localization in real space
- q-breathers – localization in mode space
- tutorial: quantizing discrete breathers
- the problem of weak passwords: chaos, criticality, and p-captchas

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

S. Flach, MPIPKS Dresden

work done jointly with T. Laptyeva and K. Kladko: EPL 95 (2011) 50007

- goal and basic idea
- what is the problem?
- a bit on encrypting and hacking
- and what are CAPTCHAs ?
- implementation of basic idea
- instead of conclusions: reactions from a virtual world

What means weak password?

passwords for: accounts, online services, credit/banking cards, ...

Test it:	Typical answer:
• how many passwords do you keep?	2-3...oh wait: 5-6...hm...15-20?
• how random and how long are they?	Not random, short
• are some of them equal or similar?	Sure, of course
• where do you keep or store them?	On a piece of paper, Post-it notes Files (not encrypted) ...

Diagnose: you have a problem with weak passwords

What is the problem with weak passwords?

- your data are hacked, stolen, destroyed
- companies make losses on identity fraud
  (total annual cost 2006 in US about $55 billion)

Consequence:

You are forced to memorize passwords which are:

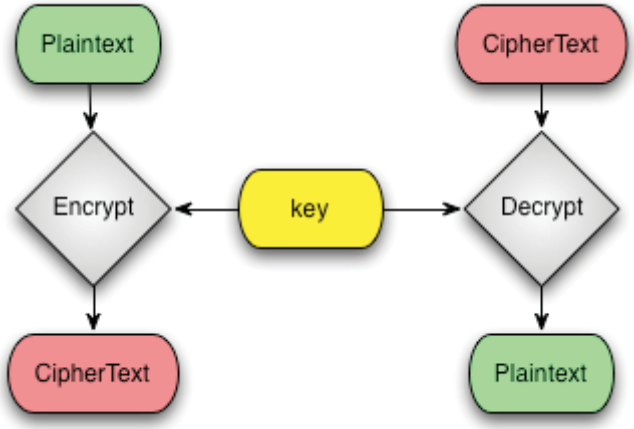
- unguessable
- all different
- never written down

These requests become unreasonable and unmanagable

A bit on data encrypting and hacking

Symmetric data encryption:

One password
Plaintext is correlated
Cipher Text is random-like

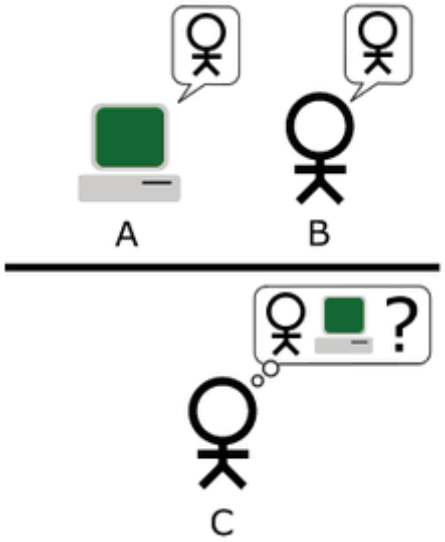


Hacking:

- **the hacker has all information except the password**
- **brute force method tries all passwords**
- **looks for correlations in decrypted candidate files**

And what are CAPTCHAs?

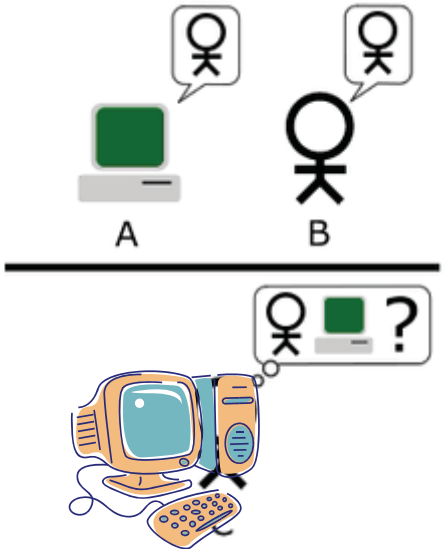
Alan  **test:**



And what are CAPTCHAs?

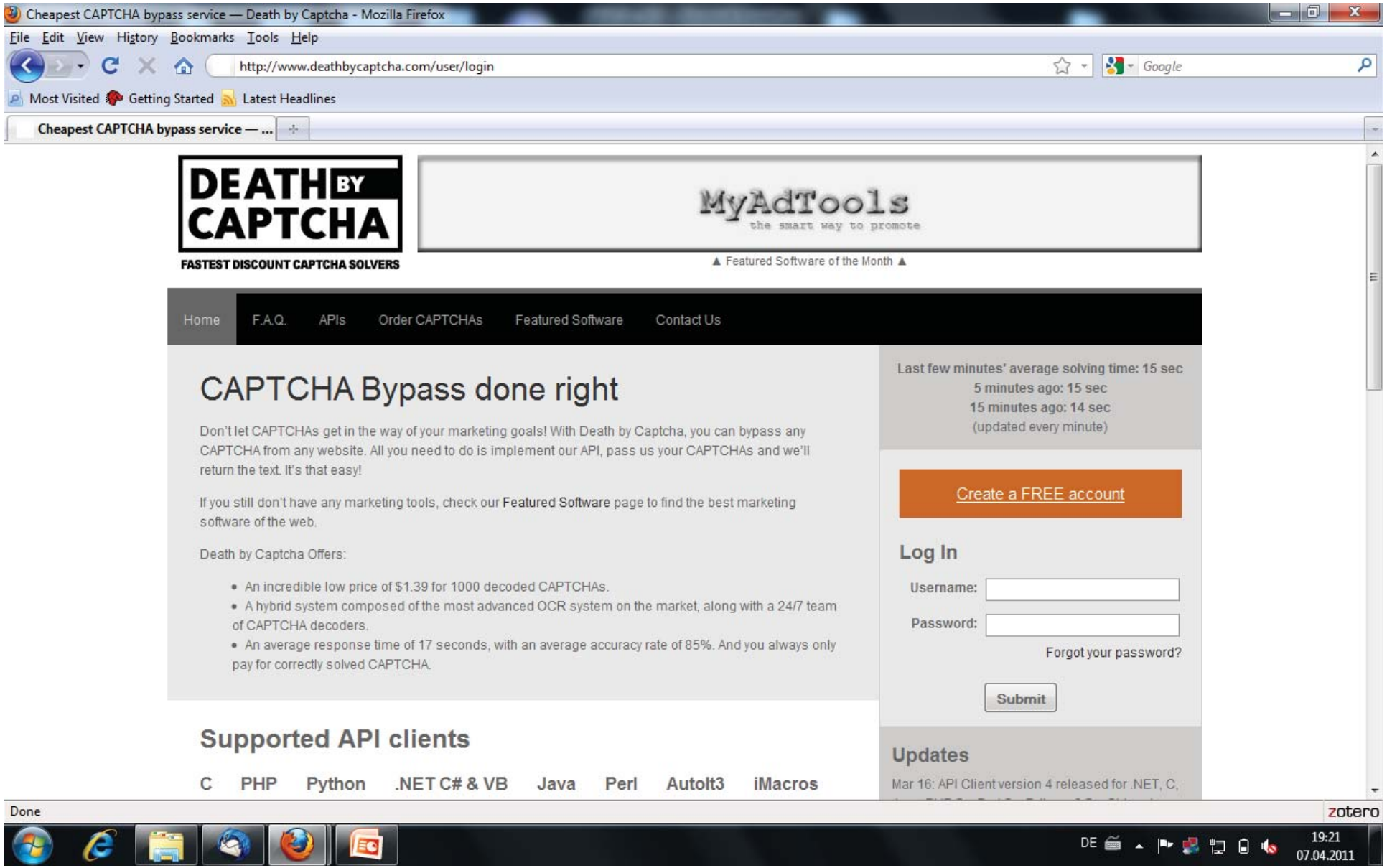
reCAPTCHA

CAPTCHA:



Completely Automated Public Turing test to tell Computers and Humans Apart

It takes about 1-10 seconds to perform a computer based CAPTCHA recognition



OUR GOAL:

develop a scheme which allows you to

- memorize a short weak password
- have protection of a long strong password
- use fact that computers are usually superior to humans, but not for image recognition!

BASIC IDEA:

- split a long strong password into two parts: Short Password SP + Strong Key SK
- memorize SP only
- encrypt SK with SP using CAPTCHA and physics of phase transitions

THE SOLUTION FROM THE PERSPECTIVE OF THE USER:

1. **Access service or program for 1st time:**

- **Choose Short Password (say 6 chars)**
- **System generates additional Strong Key (say 6 chars) inside CAPTCHA, asks to read and type in for access**
- **System encrypts CAPTCHA with Short Password using our technique**

2. **Re-access:**

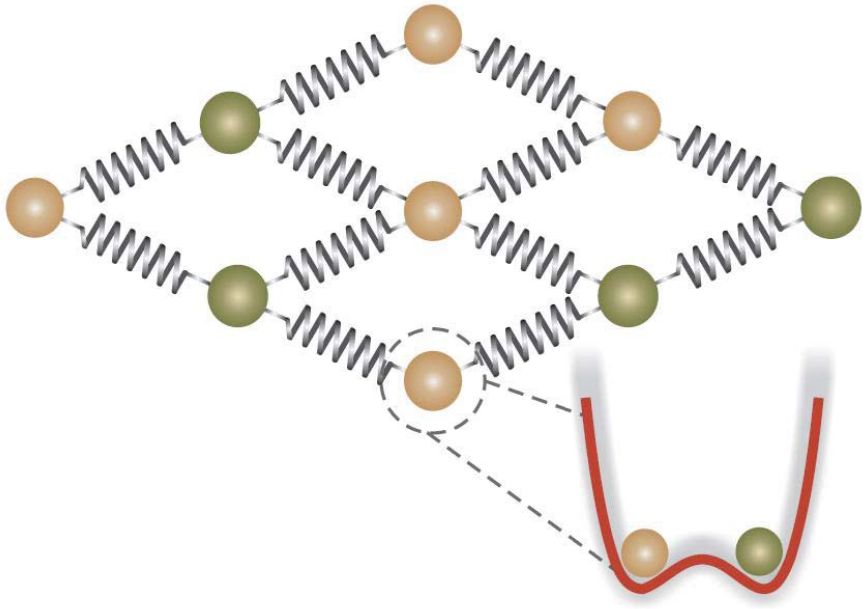
- **System asks for Short Password**
- **System decrypts CAPTCHA with Short Password using our technique**
- **System presents regenerated CAPTCHA**
- **System asks to read Strong Key and type in for access**
- **Access is granted based on a 12 chars password!**

Implementation of basic idea

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

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

square lattice N x N



Phase transition

order parameter $M = \frac{1}{N^2} \left| \sum_{ij} \mathrm{sign}(u_{ij}) \right|$

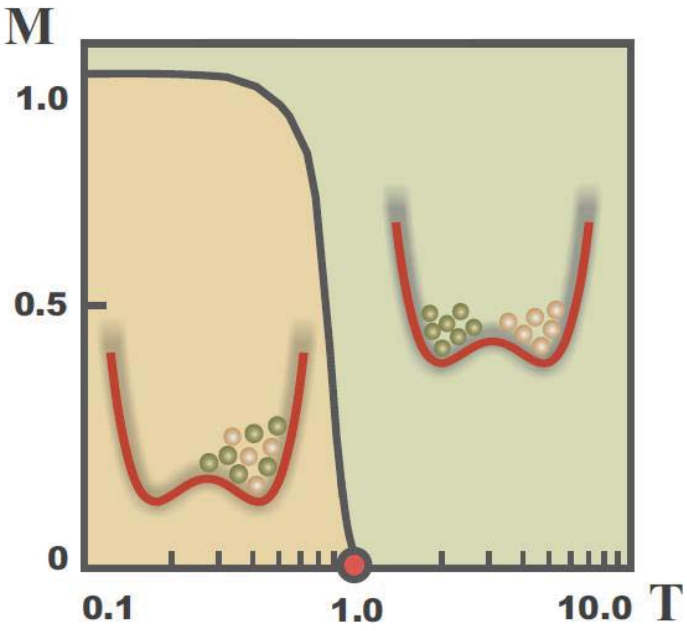
temperature: via Boltzmann distribution: $\beta \mathrm{e}^{-\beta \mathrm{p}^2/2}$ $u_{ij} = 1$

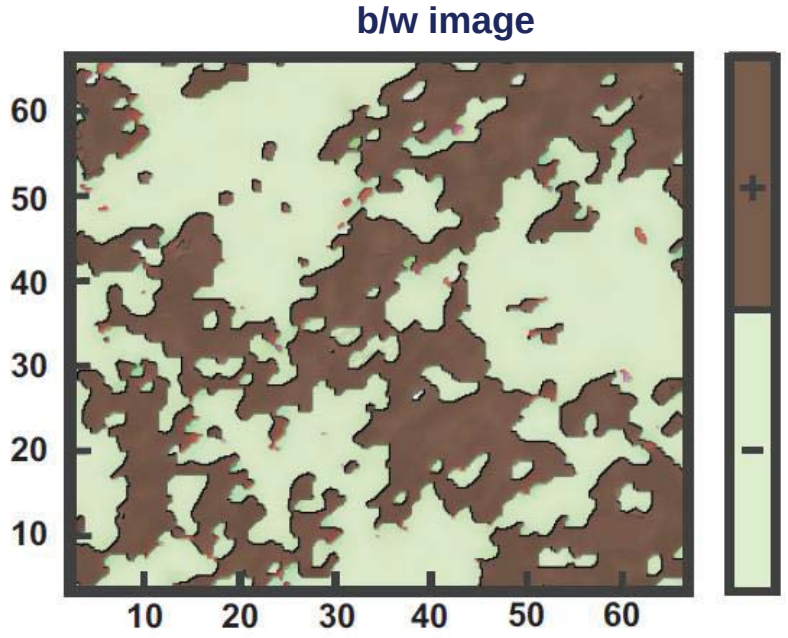
$T \equiv \beta^{-1}$

operational point: close to transition

Integrate forward in time (200 t.u.)

each dynamical state of the system can be mapped onto a b/w image





Phase transition? In 2d? Wait a second …

NN Bogolyubov

+ inequality = Mermin Wagner Hohenberg Coleman ... ?

Ising

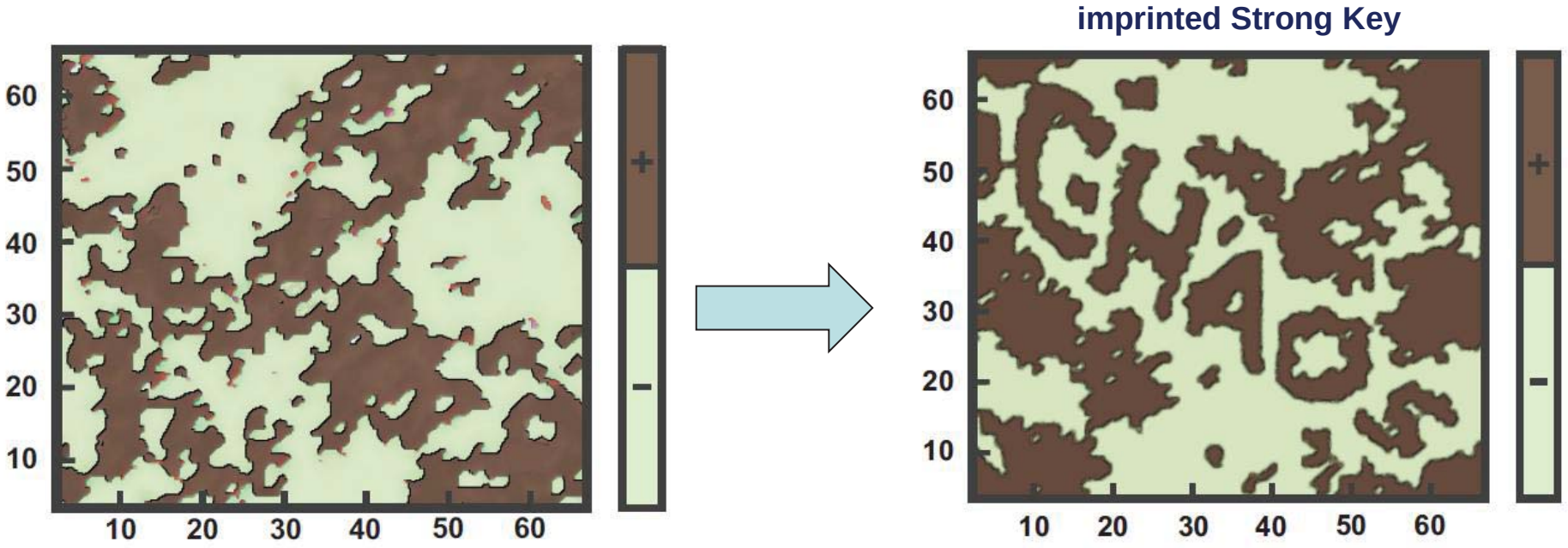
No. Model is in universality class of 2d Ising model

Onsager

It has a phase transition at finite T. Thanks to

Phase transition and imprinting of Strong Key

- the system is launched close to a phase transition
- oscillators tend to group in large domains – all left or all right
- domain walls move in time chaotically
- imprinting of Strong Key by proper change of signs of oscillators, using tools of CAPTCHA generation



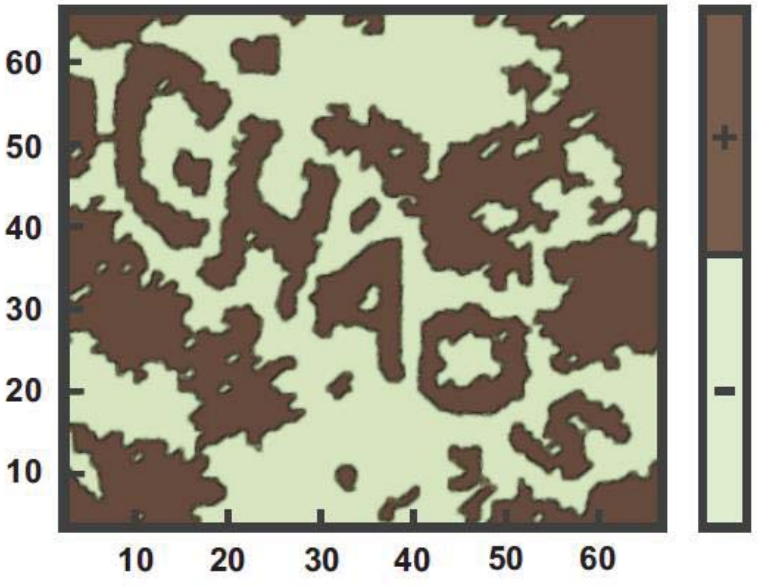
Maximum return time and chaos

- consider an initial state image at time t0=200
- define a suitable error function for blurring images
- $\tilde{RF}(t) = (1/N) \left| \sum_{ij} \mathrm{sign}_{ij}(0) \mathrm{sign}_{ij}(t) \right|$ (sorry for missing N)
- use symplectic time reversible integrator (Verlet or leap-frog)
- stop at time t=t1 and return to t0=200
- due to roundoff errors and chaos we do not return exactly
- measure blurring 1/N < RF < 1
- measure maximum t1max up to which recovering is possible: RF = 0.9
- measure largest Lyapunov coefficient: inversely proportional to t1max
- choose operational time t1 close but smaller than t1max

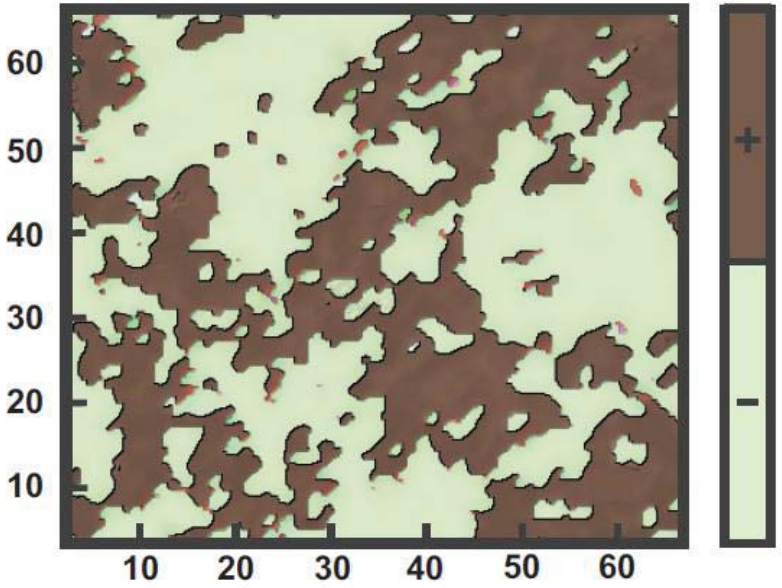
Evolve forward in time up to the edge of chaos

- Store the final state (coordinates, momenta) in two files
- F1 contains signs and all significant digits
- F2 contains the rest
- Encrypt F2 using Short Password!

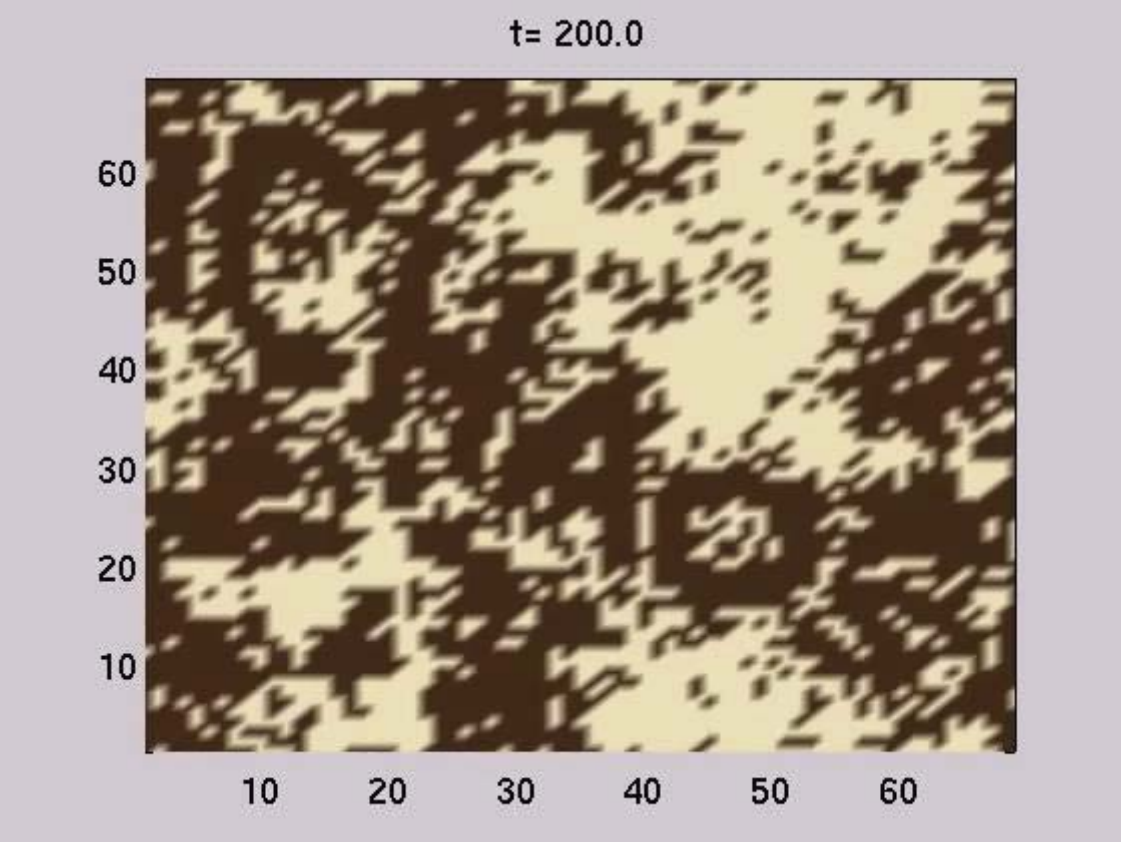
initial state with Strong Key



final state



Evolve forward in time up to the edge of chaos

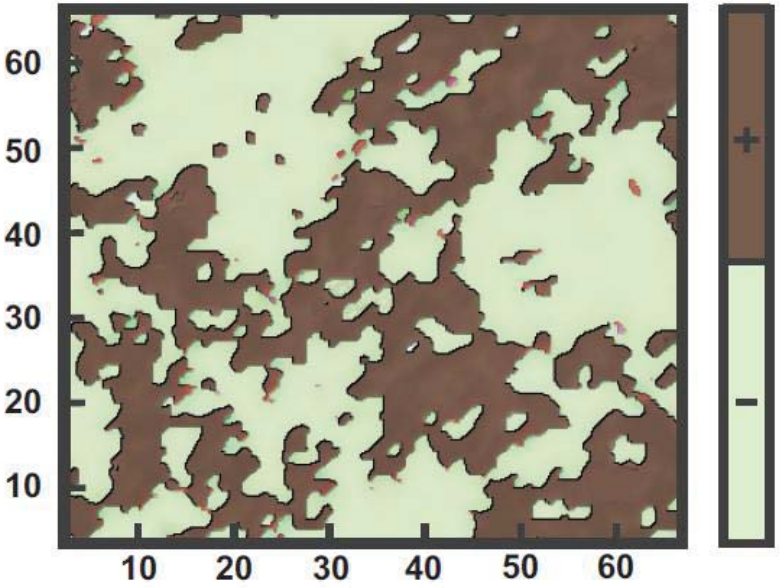


Store the final state (coordinates, momenta) in two files:
F1 contains signs and all significant digits
F2 contains the rest
Encrypt F2 using short password!

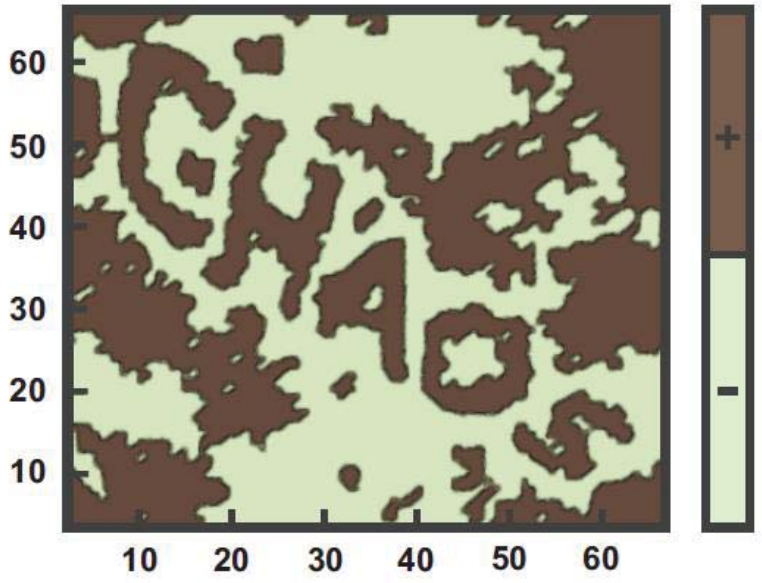
Can we return back?

- Decrypt F2 using Short Password
- Glue F1 and F2 together to obtain the correct final dynamical state
- Integrate backwards in time
- Read the Strong Key SK!

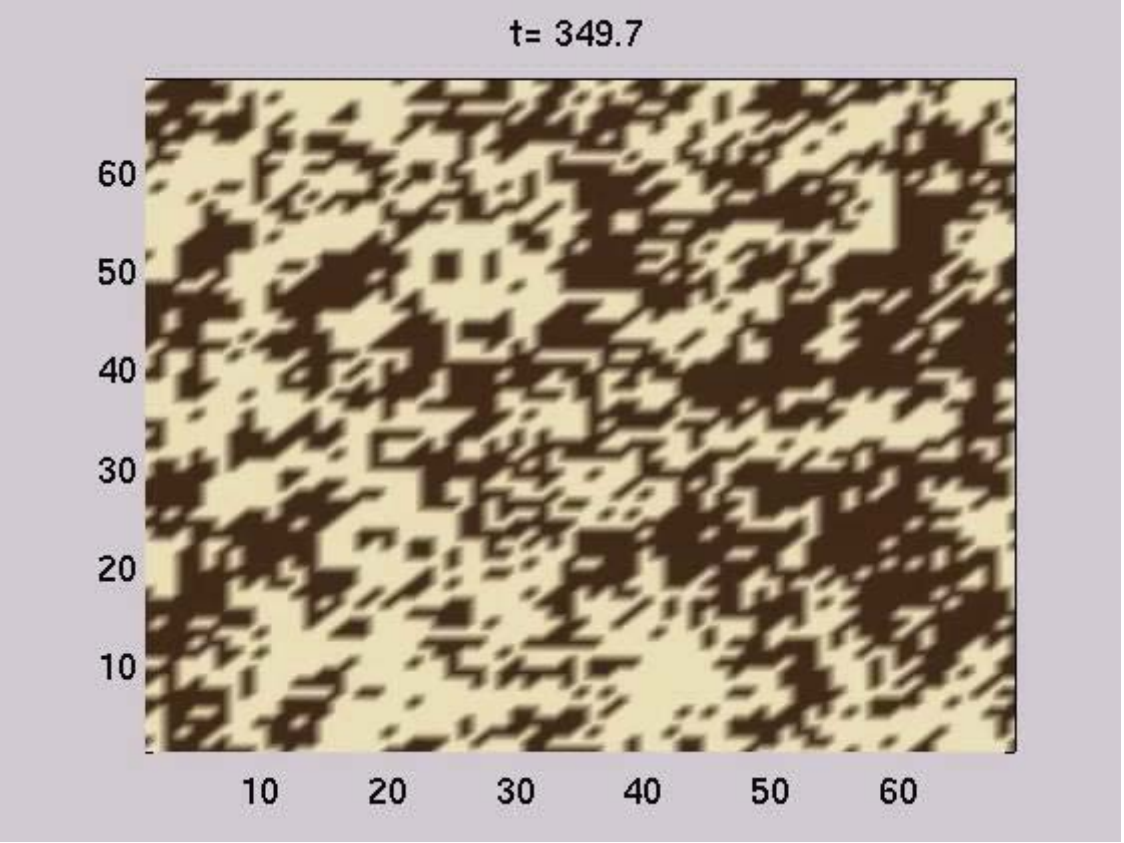
decrypted final state



restored initial state with Strong Key

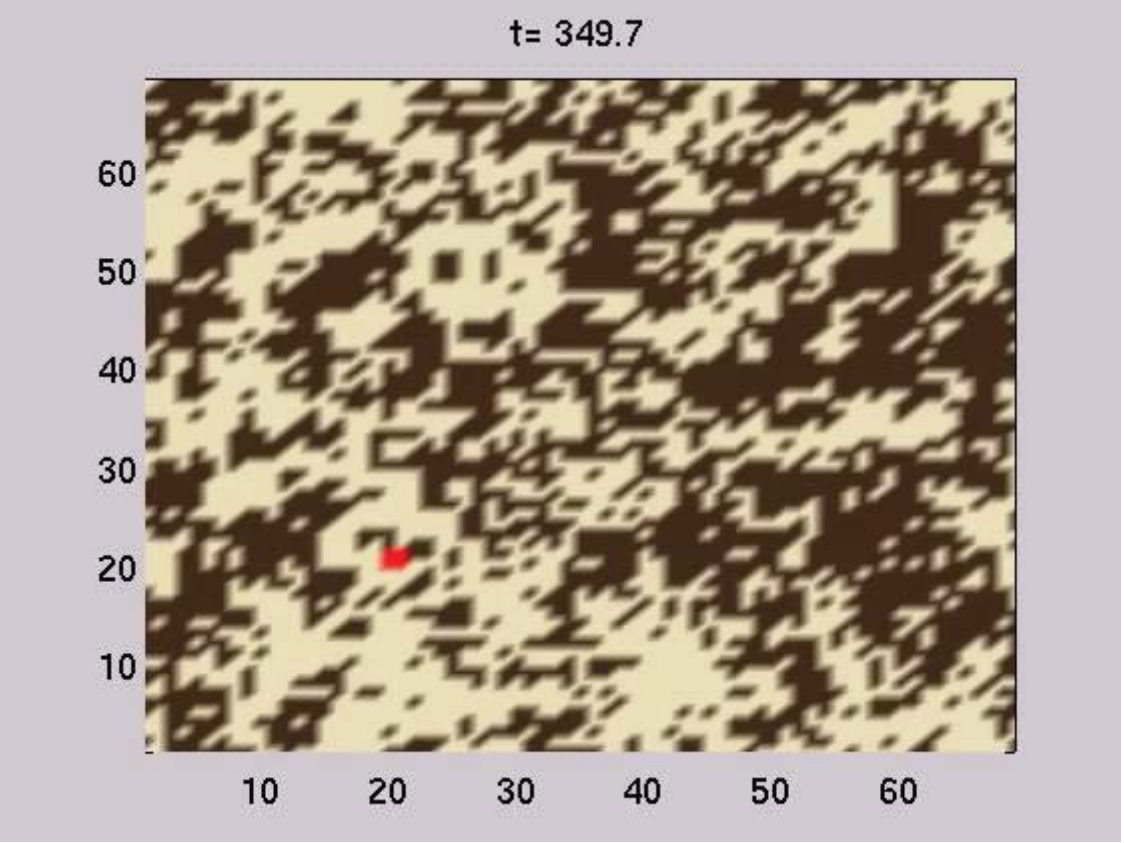


Can we return back?

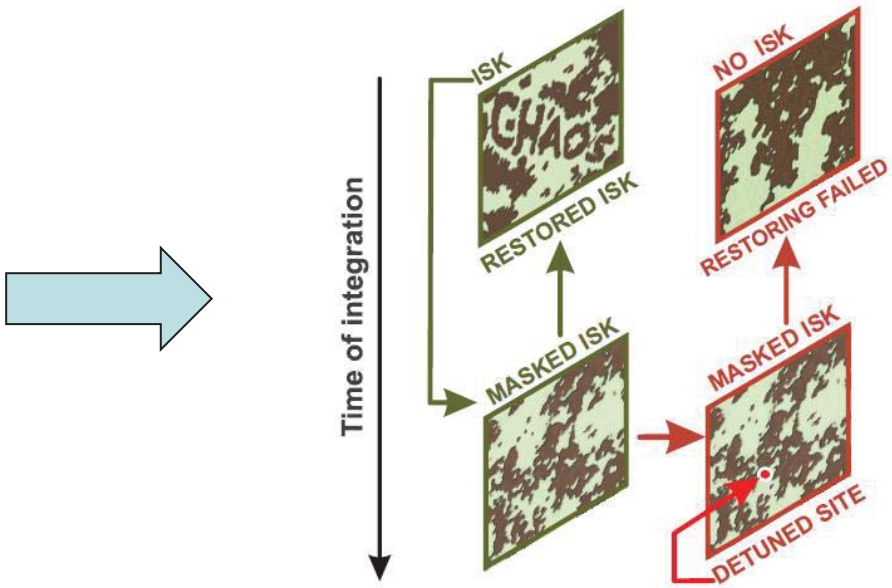


Decrypt F2 using short password
Glue F1 and F2 together to obtain the correct final dynamical state
Integrate backwards in time
Read the strong key SK!

Detune one oscillator coordinate by 0.000001



The scheme in a nutshell:



Fast hacking of Strong Key impossible:

- **via correlations – they are always large**
- **image recognition – 1-10 seconds per recognition, even with Short Passwords millions of trials**
- **Benchmarking: 5 chars Short Password is as safe as standard case with 9 chars**
- **due to dynamical chaos, slightest errors in the final state will grow back in time and spoil restoring of correct initial state**

FINISH LINE

Scheme is implemented using Java.
It can be offered both locally or remotely.

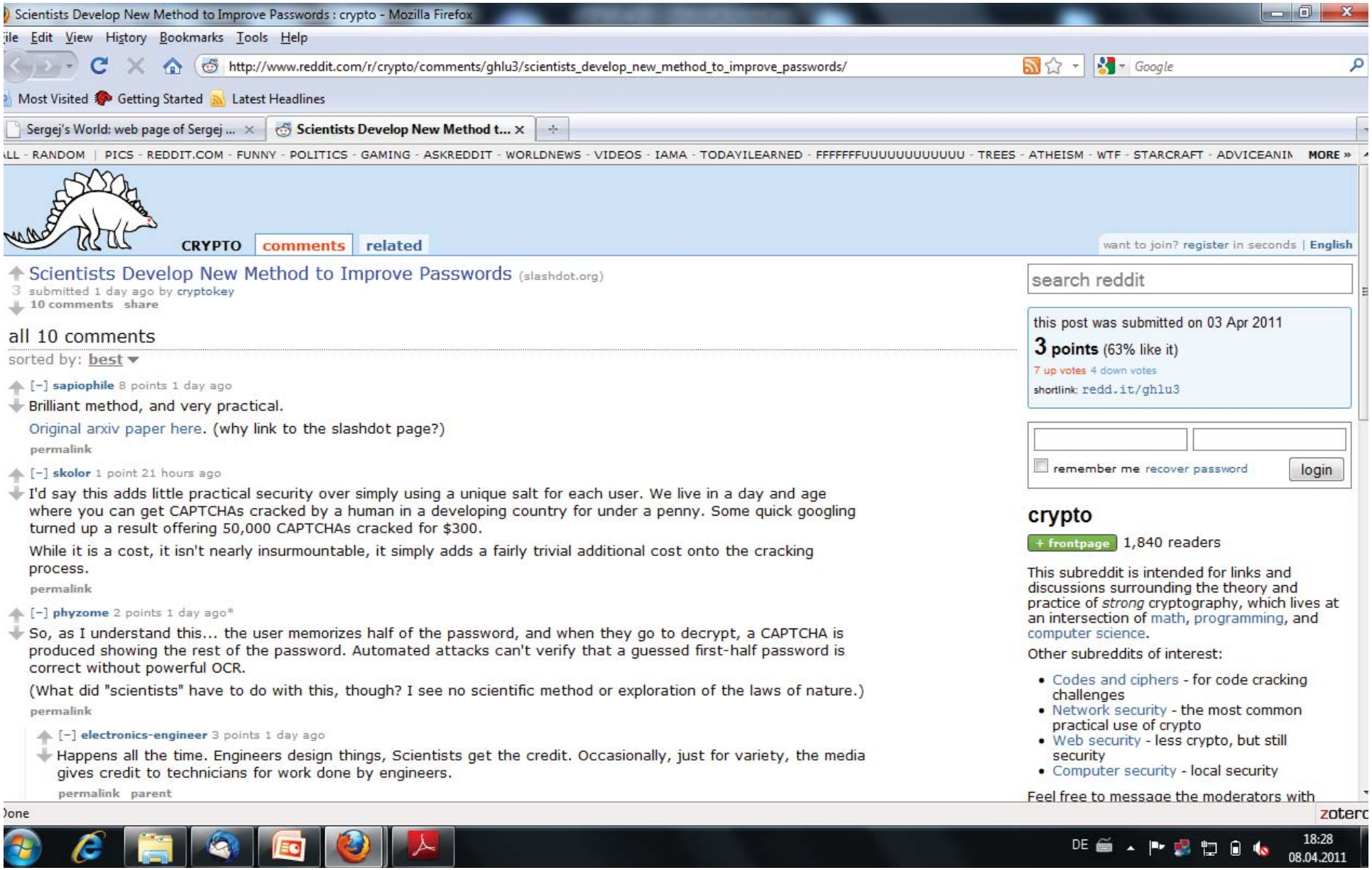
Method can be used for

- **file encryption**
- **accessing online services**
- **security apps on mobile devices**
- **any procedure which requires password identification**

Publication:
The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs
T.V. Laptyeva, S. Flach, K. Kladko, EPL 95, 50007 (2011)
http://www.pks.mpg.de/~flach/publications.DIR/2011/EPL_95_50007_2011.pdf

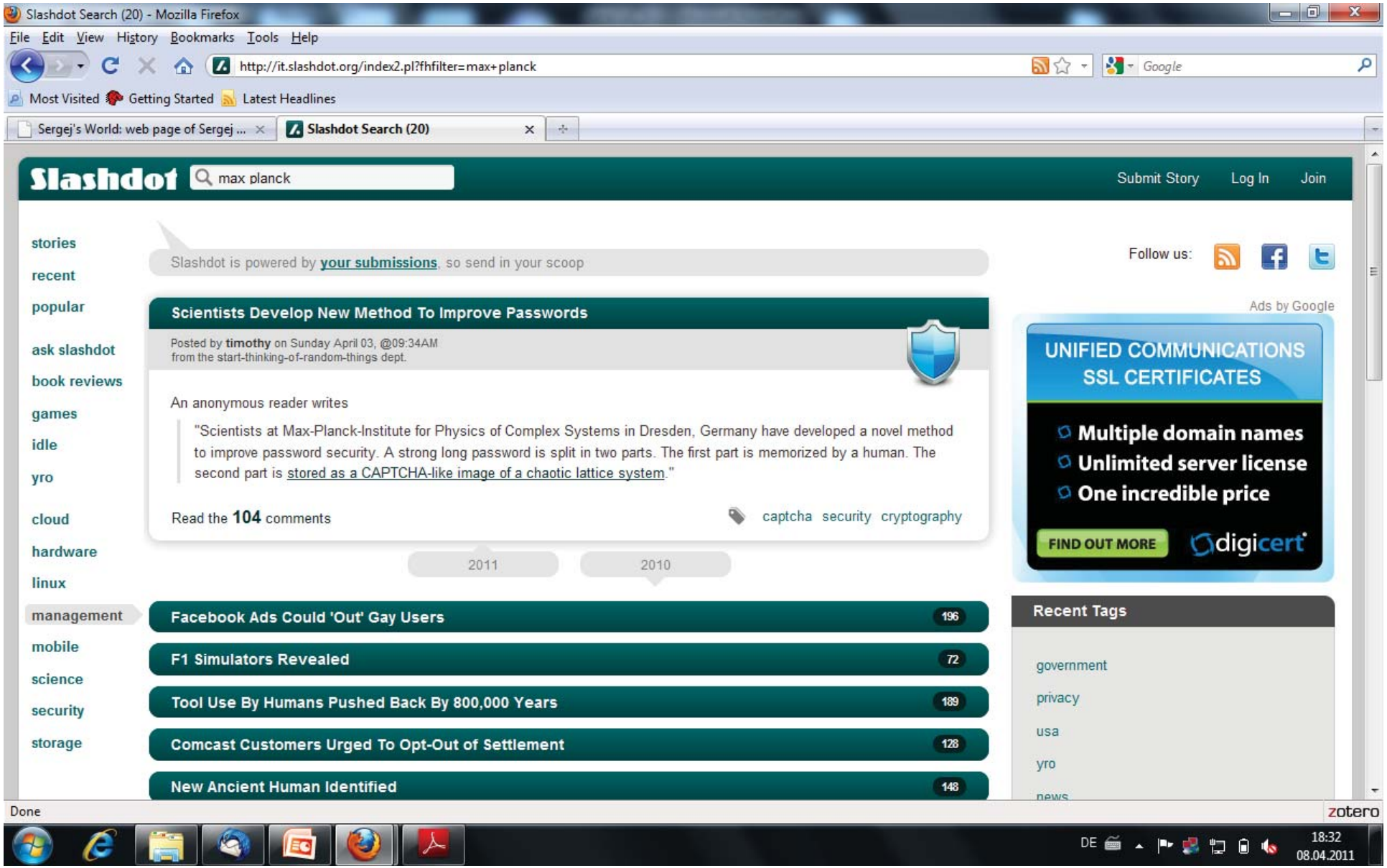
Over 230 web sites coverage, including slash dot, science daily, max planck, etc:
http://www.pks.mpg.de/~flach/html/password.html

Reactions of a virtual world



A9kGzhR

Reactions of a virtual world



Reactions of a virtual world

Max-Planck-Gesellschaft - Strong protection for weak passwords - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Sergej's World: web page of Sergej Fl... | Max-Planck-Gesellschaft - Strong pro...

http://www.mpg.de/print/2823498

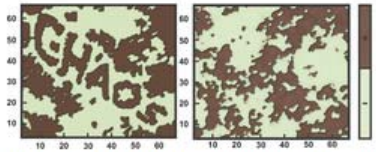
Research publication
April 19, 2011

MAX-PLANCK-GESELLSCHAFT

Strong protection for weak passwords

The combination of simple codes and Captchas, which are even more encrypted using a chaotic process, produces effective password protection

The passwords of the future could become more secure and, at the same time, simpler to use. Researchers at the Max Planck Institute for the Physics of Complex Systems in Dresden have been inspired by the physics of critical phenomena in their attempts to significantly improve password protection. The researchers split a password into two sections. With the first, easy to memorize section they encrypt a Captcha – an image that computer programs per se have difficulty in deciphering. The researchers also make it more difficult for computers, whose task it is to automatically crack passwords, to read the passwords without authorization. They use images of a simulated physical system, which they additionally make unrecognizable with a chaotic process. These p-Captchas enable the Dresden physicists to achieve a high level of password protection, even though the user need only remember a weak password.



Indecipherable for computers: The Captcha with the password is very grainy, as it is generated in a physical system close to a critical change of state (left). In a chaotic process, it is made completely unreadable. The process can be reversed with an easily remembered password, however.

© Sergej Flach / MPI for the Physics of Complex Systems

Computers sometimes use brute force. Hacking programs use so-called brute-force attacks to try out all possible character combinations to guess passwords. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) are therefore intended as an additional safeguard the input of which originates from a human being and not from a machine. They pose a task for the user which is simple enough for any human, yet very difficult for a program. Users must enter a distorted text which is displayed on the screen, for example.

zotero

DE 13:05 05.07.2011

Reactions of a virtual world

CAPTCHAs with chaos: Strong protection for weak passwords - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Sergej's World: web page of Sergej Fl... | CAPTCHAs with chaos: Strong protec...

http://www.sciencedaily.com/releases/2011/04/110420111331.htm

ScienceDaily®

Your source for the latest research news

Clarity Software
Chromatography Data System Excelent performance/price ratio www.dataapex.com
Ads by Google

News | Articles | Videos | Images | Books | Search

Health & Medicine | Mind & Brain | Plants & Animals | Earth & Climate | Space & Time | Matter & Energy | Computers & Math | Fossils & Ruins

Science News

Share Blog Cite Print Bookmark Email

CAPTCHAs With Chaos: Strong Protection for Weak Passwords

ScienceDaily (Apr. 21, 2011) — The passwords of the future could become more secure and, at the same time, simpler to use.

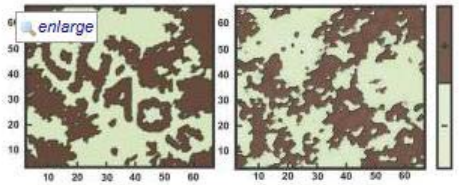
Researchers at the Max Planck Institute for the Physics of Complex Systems in Dresden have been inspired by the physics of critical phenomena in their attempts to significantly improve password protection. The researchers split a password into two sections. With the first, easy-to-memorize section they encrypt a CAPTCHA ("completely automated public Turing test to tell computers and humans apart") -- an image that computer programs per se have difficulty in deciphering. The researchers also make it more difficult for computers, whose task it is to automatically crack passwords, to read the passwords without authorization. They use images of a simulated physical system, which they additionally make unrecognizable with a chaotic process. These n CAPTCHAs

See Also:

Matter & Energy
- Physics
- Quantum Physics
- Solar Energy

Computers & Math
- Computer Science
- Artificial Intelligence
- Hacking

Reference
- Security engineering
- Computer security
- Cryptography
- Malware



Indecipherable for computers: The Captcha with the password is very grainy, as it is generated in a physical system close to a critical change of state (left). In a chaotic process, it is made completely unreadable. The process can be reversed with an easily remembered password, however. (Credit: Sergej Flach / MPI for the Physics of Complex Systems)

Ads by Google

Antivirusni program — Sophos - testirajte ga brezplačno. Zagotovite si učinkovito zaščito.
www.sophos.si

Photovoltaic Modules — Good Price Fast Delivery from Italy Range from 10 to 230Watt

Just In:
'Odd Couple' Stars: Dual Gamma-Ray Flares

Science Video News

Protect Yourself From Computer Hackers
Computer scientists observe that the people most at risk for the loss of private information and other computer problems are those who create easily.
... > *full story*

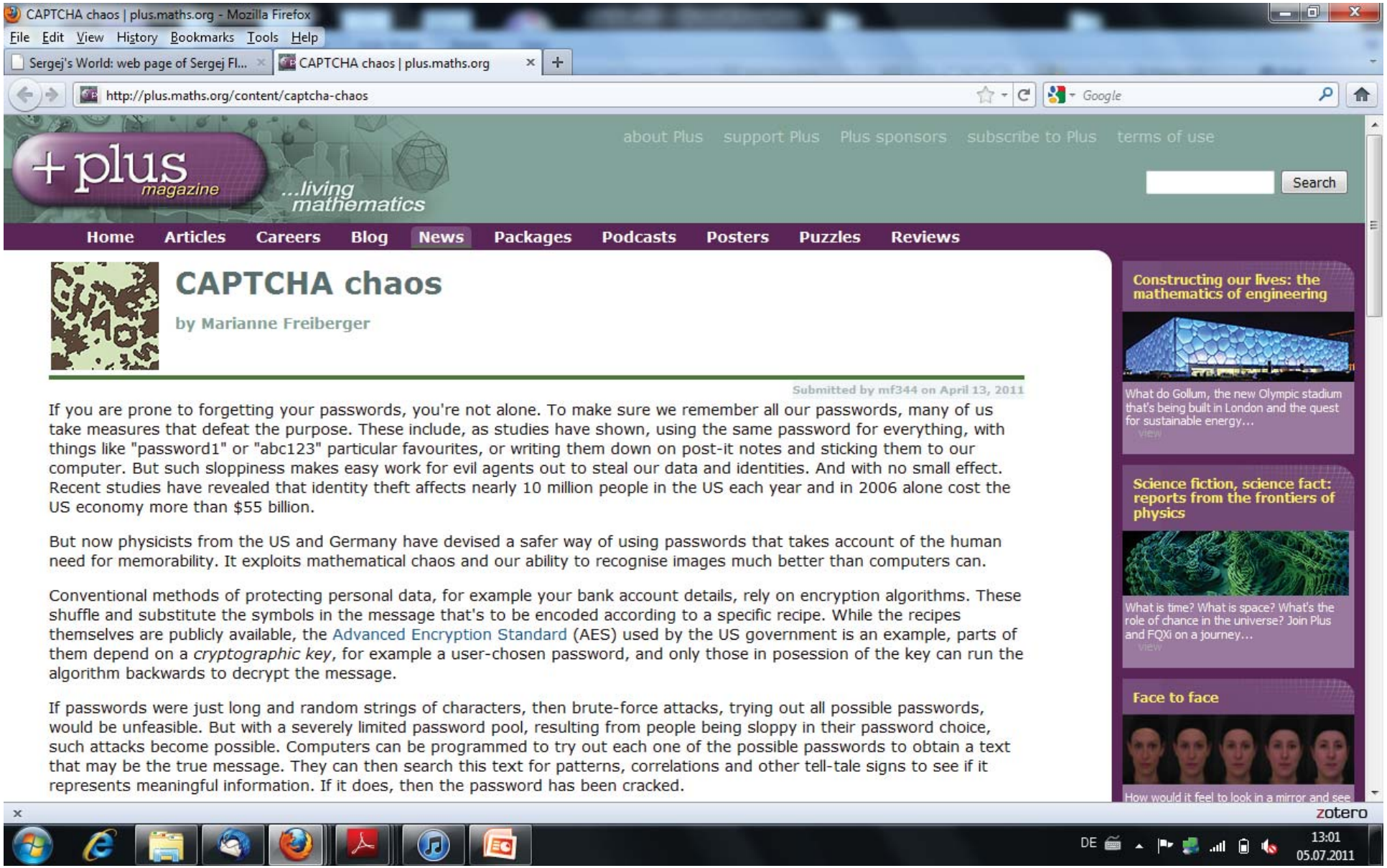
- Computer Scientists Attach Images to Passwords to Prevent Fraud
- Electrical Engineers Develop Pocket-Size Fingerprint Recognition
- Simulation Software Derives New Tricks from Math
- *more science videos*

Neural Network Software
Download NeuroSolutions and apply neural networks to your application
www.neurosolutions.com

zotero

DE 12:59 05.07.2011

Reactions of a virtual world



Reactions of a virtual world

Featured on more than 230 web sites worldwide