



2286-12

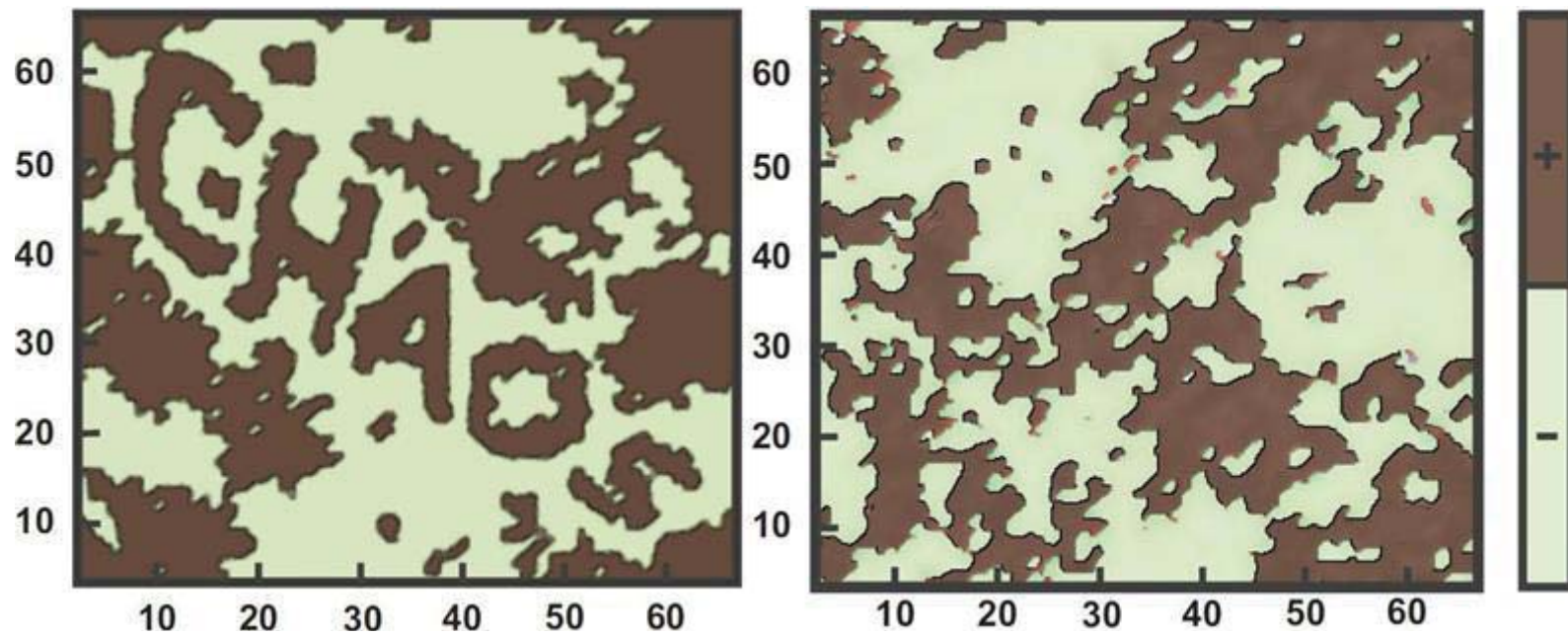
Workshop on New Materials for Renewable Energy

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*



eshdofysw784cnguikngcoh43ynhkogjpb1kfdmgoifdgmm
sd1yugfuychrh.jnhodrta5ohlfdgmuouhgicoudnhugosho
ib43giungo1sfmcohsu4ohnu iht15et...bugre1yugbik
y1qsfbug4tg5fiu1yhf16y6bgy...egtr...mc5418hc7
atu7icgirhciachr17denuc1...yibc48
zhgd8oiz8s3cuh87fzs74chf...fihoc
nri3uchgikchgykseru73ih...airc
78csyuihbguzfheyr9icgr...h48t47sdit...u13
uea623vab2xyixnuam33l...73t
xifuguiw6739dherdsik...w6f
bhgk64389b2hikcjmuhiu...ikk
v7eh7riv74xjf7icjgbcf...vor
iigy3dywd2uaayezrs37y...io
jekyhfc3o8ubrc1kjmfsi...iy9
nc798hs0cyp9jvghgnion...rio
jock7w9465fgisuyfgciae...hko
jkshgsyuisgiasgfijfeoa...4eo
iubcoac3yhrqcnhoiutyf...7e6
n90lvubaoity7iy475ytiuog...e5hyo
iusauitisyguojyuitisgt4u...anoca
cgsauigf648cnglog2489igr4e...6eiu
pauhuovnityv378ncirusdfisyavm...any34...s87
t985y89eygre9iusghyewicngfugucyenbgwtwithy...tu
3397675niurgsigyrincyefienkxgloyugtriuuuuu...4
iso587hsigf46fgtynotaygonchfwnaaginviatnot...
t28yau7acha9c89umr5uue48n9nnuuu93uukiuags

Nonlinear Lattice Waves: Classical and Quantum

S. Flach, MIPPKS Dresden



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, MIPKs Dresden



work done jointly with T. Laptjeva 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:

- how many passwords do you keep?
- how random and how long are they?
- are some of them equal or similar?
- where do you keep or store them?

Typical answer:

2-3...oh wait: 5-6...hm...15-20?

Not random, short

Sure, of course

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



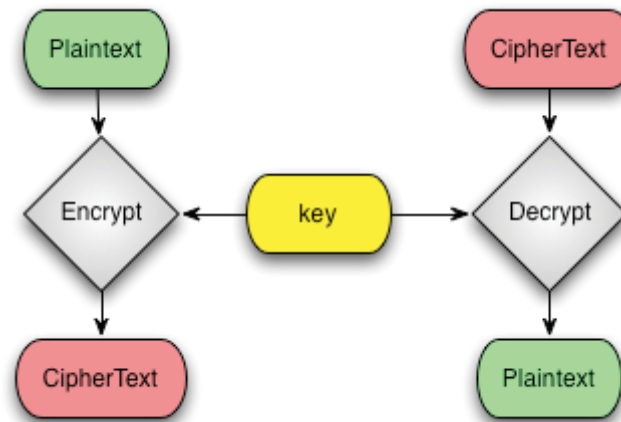
A bit on data encrypting and hacking

Symmetric data encryption:

One password

Plaintext is correlated

Cipher Text is random-like



Hacking:



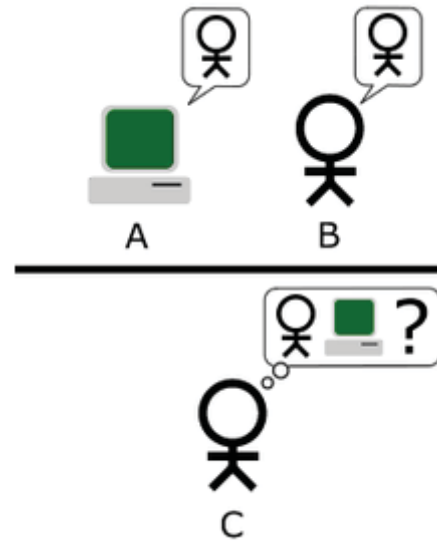
- the hacker has all information except the password
- brute force method tries all passwords
- looks for correlations in decrypted candidate files

And what are CAPTCHAs?

Alan



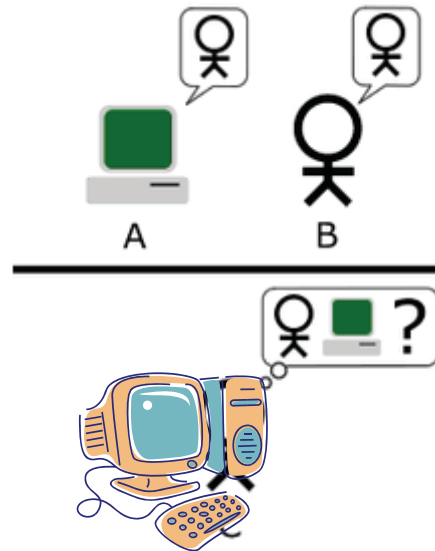
test:



And what are CAPTCHAs?



CAPTCHA:



Completely Automated Public Turing test to tell Computers and Humans Apart

Security Check

Enter both words below, separated by a space.
Can't read the words below? Try different words or an audio captcha.

Lowenbein Wardivell

Side of these? verify your account:

Text in the box: What's This?

Submit



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

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://www.deathbycaptcha.com/user/login`. The website has a dark header with the "DEATH BY CAPTCHA" logo and the tagline "FASTEST DISCOUNT CAPTCHA SOLVERS". A navigation bar includes links for Home, F.A.Q., APIs, Order CAPTCHAs, Featured Software, and Contact Us. The main content area features a section titled "CAPTCHA Bypass done right" with a description of the service and a list of offers. To the right, there is a "Log In" section with fields for Username and Password, a "Submit" button, and a link for "Forgot your password?". Above the login section, a box displays "Last few minutes' average solving time: 15 sec" and a "Create a FREE account" button. Below the main content, a "Supported API clients" section lists various programming languages and frameworks. The browser's status bar at the bottom shows the time as 19:21 on 07.04.2011, along with system icons and a Zotero extension.

Cheapest CAPTCHA bypass service — Death by Captcha - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.deathbycaptcha.com/user/login

Most Visited Getting Started Latest Headlines

Cheapest CAPTCHA bypass service — ...

DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

MyAdTools
the smart way to promote

▲ Featured Software of the Month ▲

Home F.A.Q. APIs Order CAPTCHAs Featured Software Contact Us

CAPTCHA Bypass done right

Don't let CAPTCHAs get in the way of your marketing goals! With Death by Captcha, you can bypass any CAPTCHA from any website. All you need to do is implement our API, pass us your CAPTCHAs and we'll return the text. It's that easy!

If you still don't have any marketing tools, check our [Featured Software](#) page to find the best marketing software of the web.

Death by Captcha Offers:

- An incredible low price of \$1.39 for 1000 decoded CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA decoders.
- An average response time of 17 seconds, with an average accuracy rate of 85%. And you always only pay for correctly solved CAPTCHA.

Last few minutes' average solving time: 15 sec
5 minutes ago: 15 sec
15 minutes ago: 14 sec
(updated every minute)

[Create a FREE account](#)

Log In

Username:

Password:

[Forgot your password?](#)

Supported API clients

C PHP Python .NET C# & VB Java Perl AutoIt3 iMacros

Updates

Mar 16: API Client version 4 released for .NET, C,

Done

zotero

DE 19:21 07.04.2011

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:

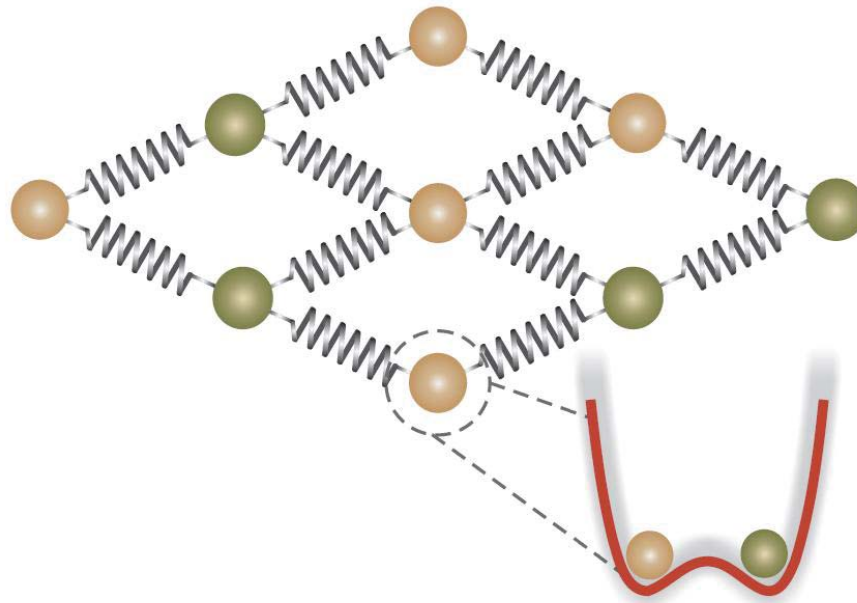
- System asks for Short Password
- System decrypts CAPTCHA with Short Password using our technique
- System presents regenerated CAPTCHA
- System asks to read Strong Key and type in for access
- Access is granted based on a 12 chars password!

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

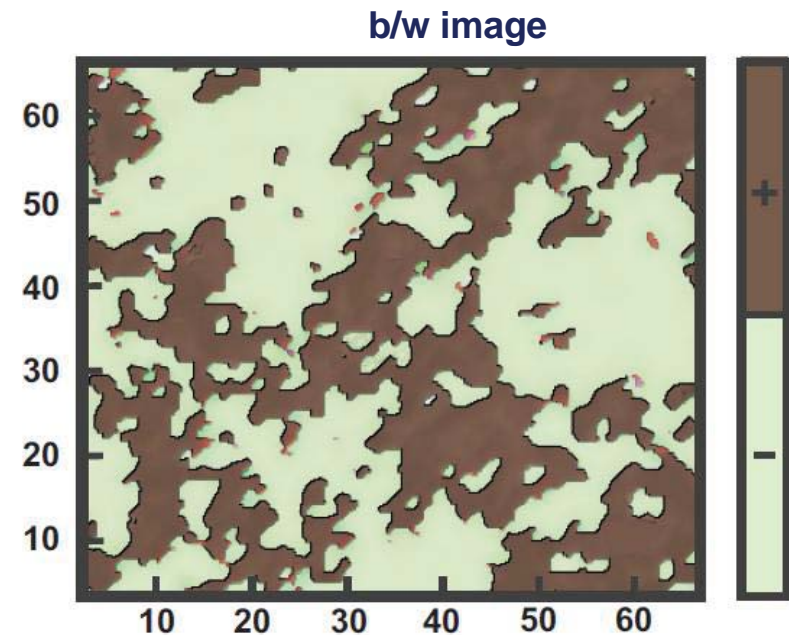
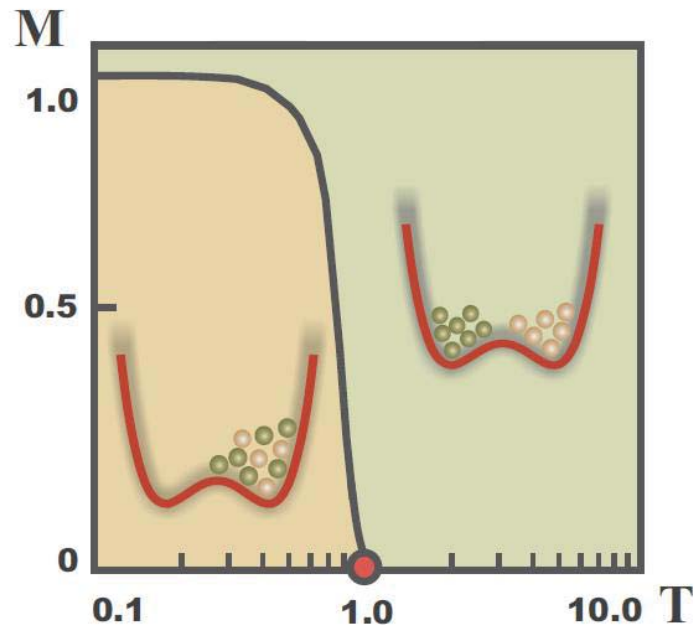
order parameter $M = \frac{1}{N^2} \left| \sum_{ij} \text{sign}(u_{ij}) \right|$

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

operational point: close to transition $T \equiv \beta^{-1}$

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 ... ?

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

Ising



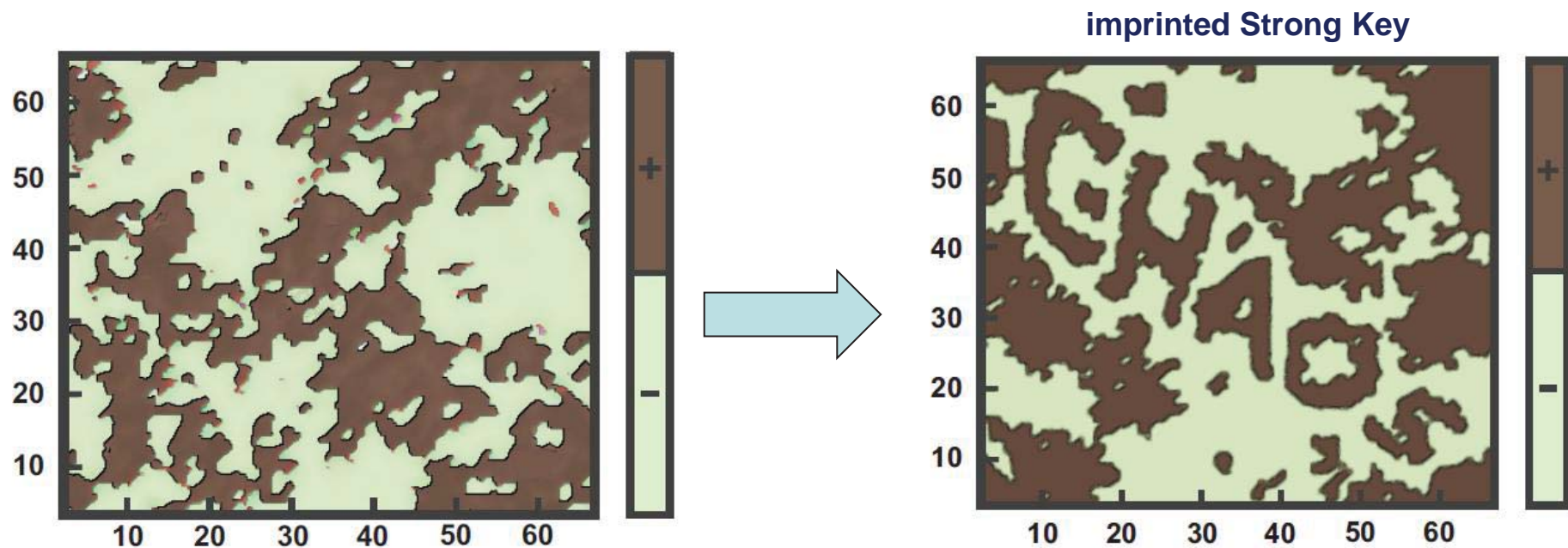
Onsager



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

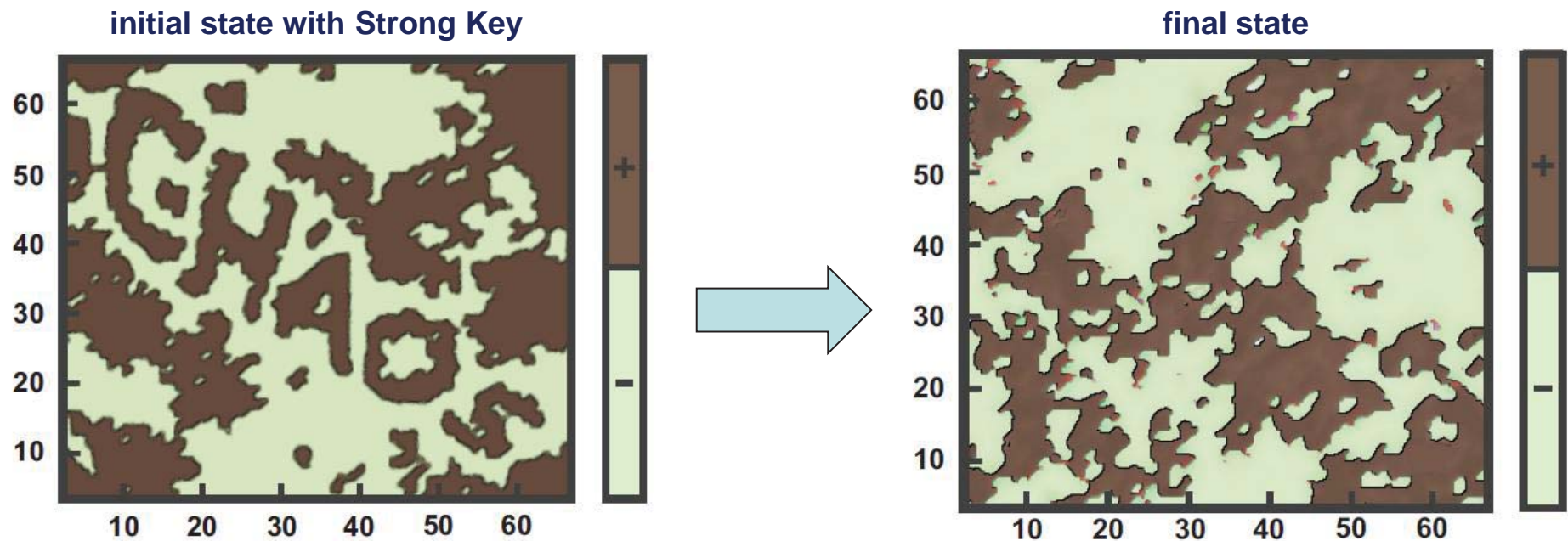


Maximum return time and chaos

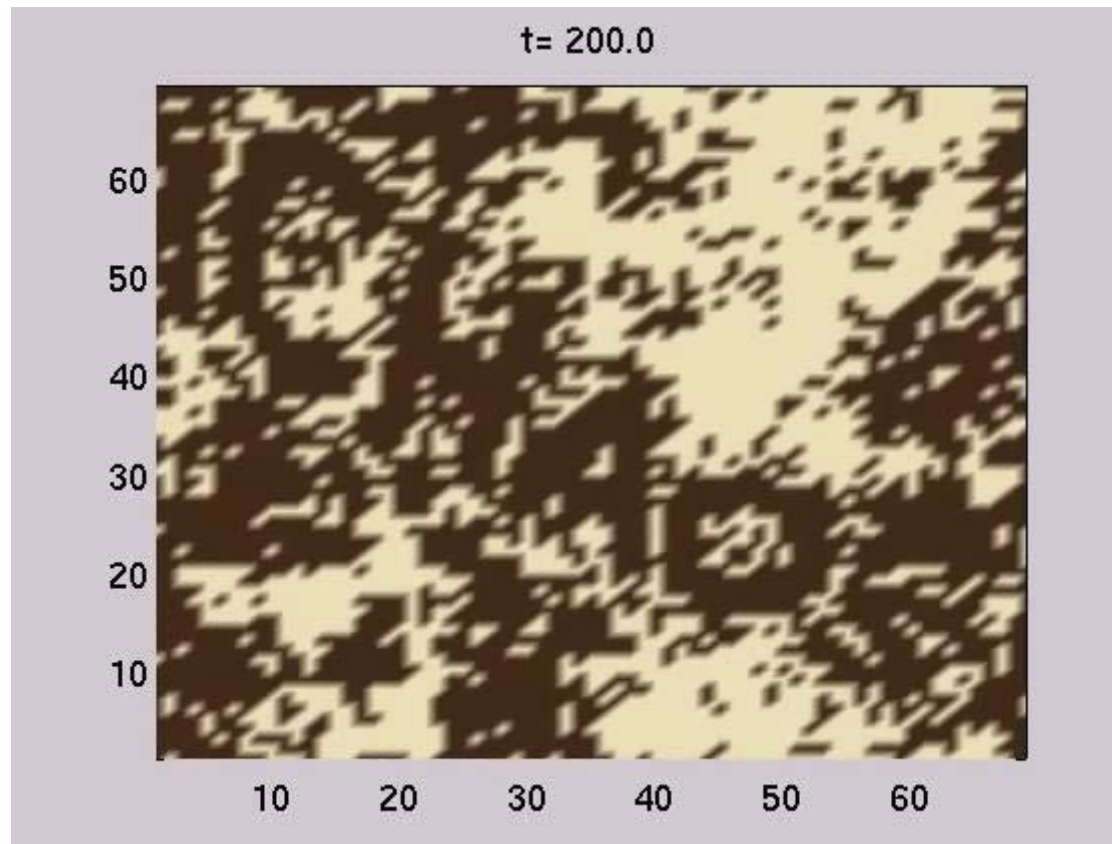
- consider an initial state image at time $t_0=200$
- define a suitable error function for blurring images
- $\tilde{RF}(t) = (1/N) \left| \sum_{ij} \text{sign}_{ij}(0) \text{sign}_{ij}(t) \right|$ (sorry for missing N)
- use symplectic time reversible integrator (Verlet or leap-frog)
- stop at time $t=t_1$ and return to $t_0=200$
- due to roundoff errors and chaos we do not return exactly
- measure blurring $1/N < RF < 1$
- measure maximum $t_{1\max}$ up to which recovering is possible: $RF = 0.9$
- measure largest Lyapunov coefficient: inversely proportional to $t_{1\max}$
- choose operational time t_1 close but smaller than $t_{1\max}$

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!



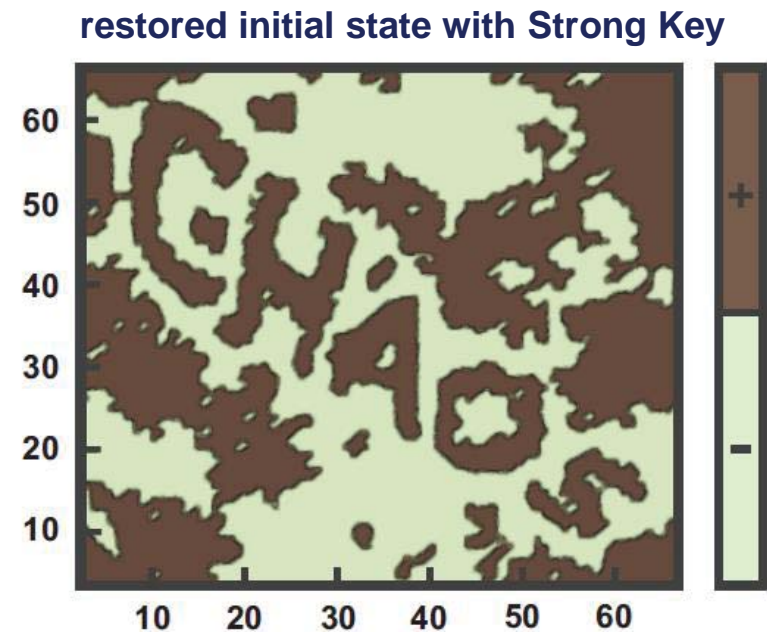
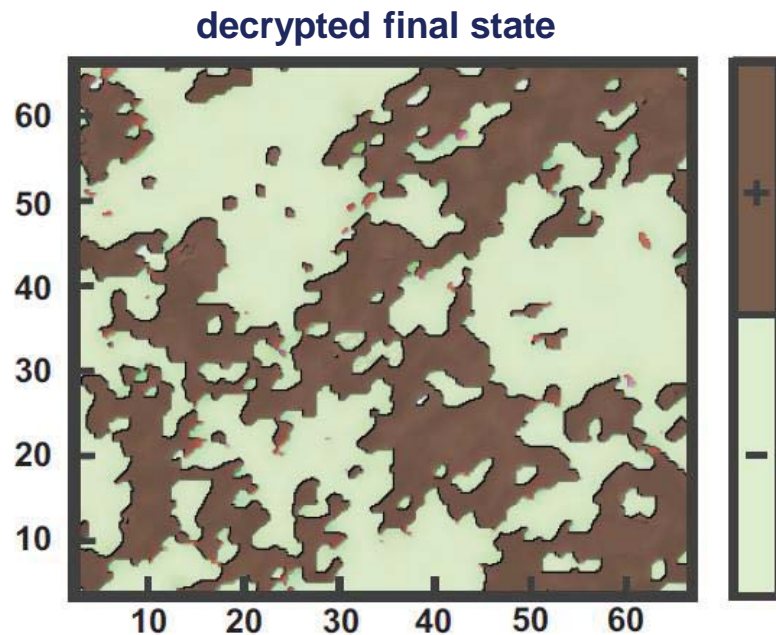
Evolve forward in time up to the edge of chaos



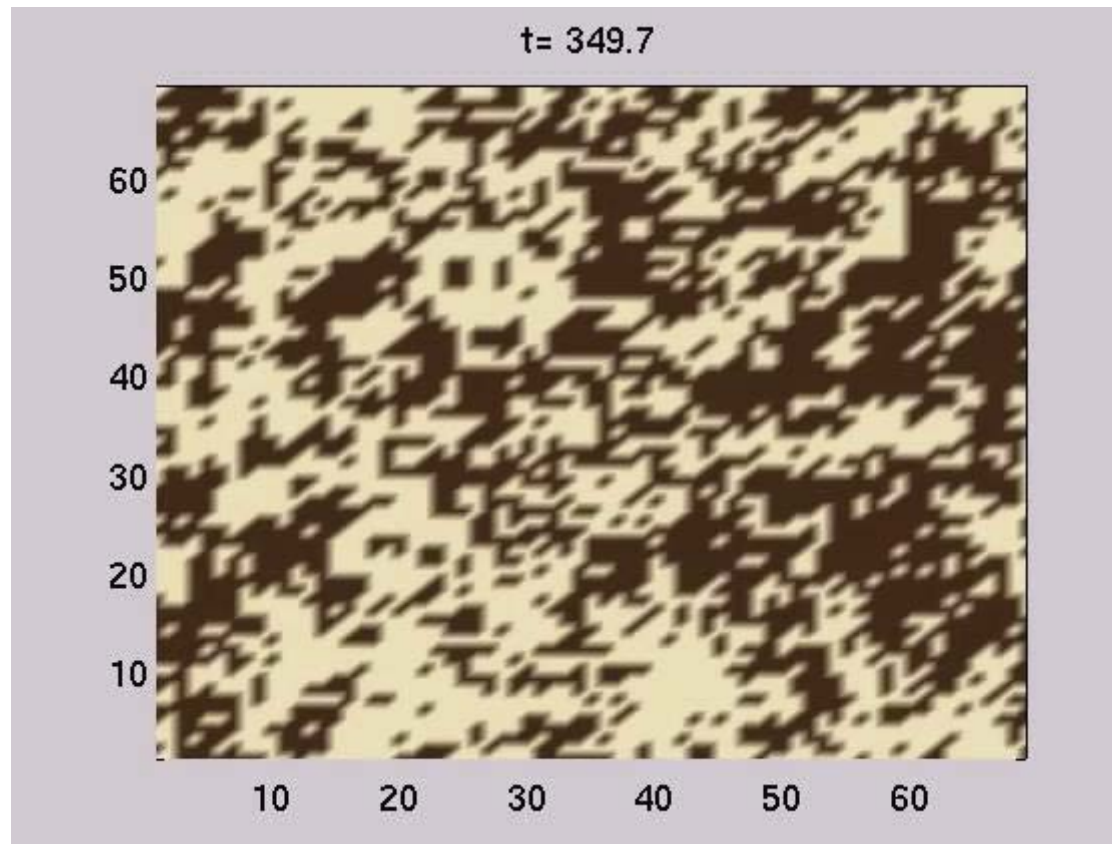
**Store the final state (coordinates, momenta) in two files:
F1 contains signs and all significant digits
F2 contains the rest
Encrypt F2 using short password!**

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!



Can we return back?



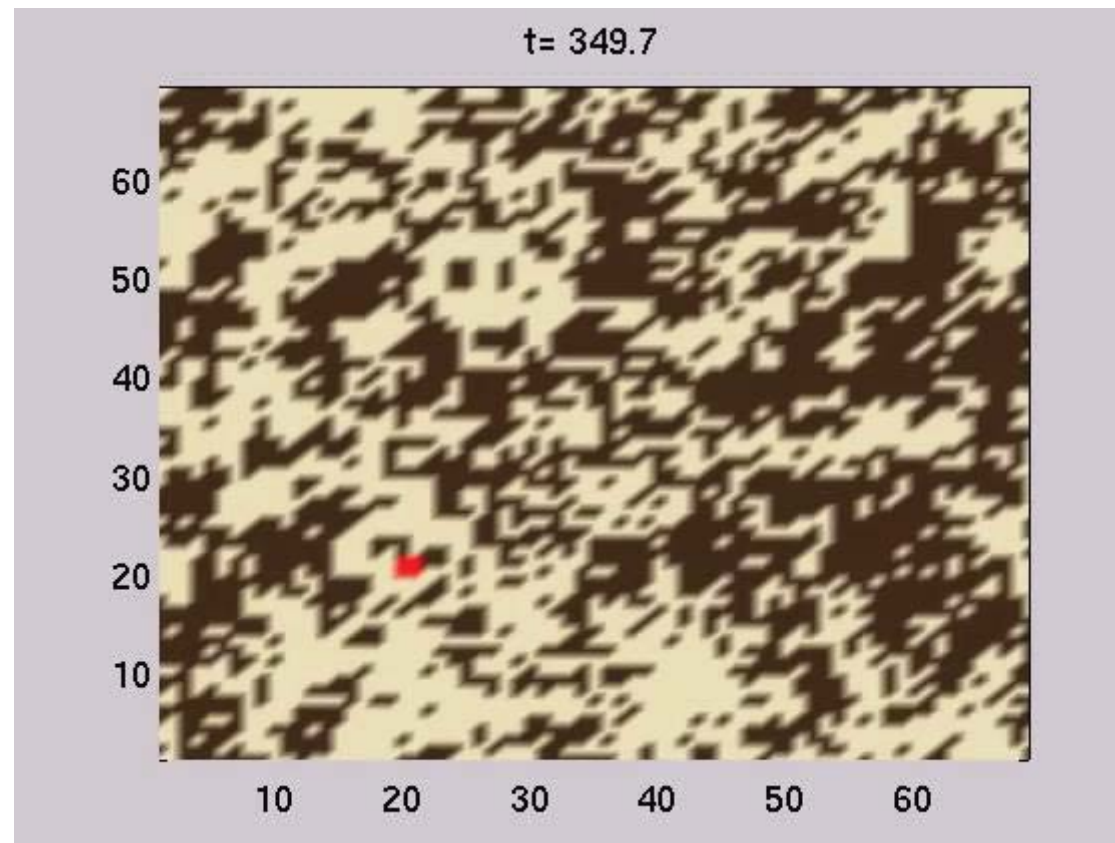
Decrypt F2 using short password

Glue F1 and F2 together to obtain the correct final dynamical state

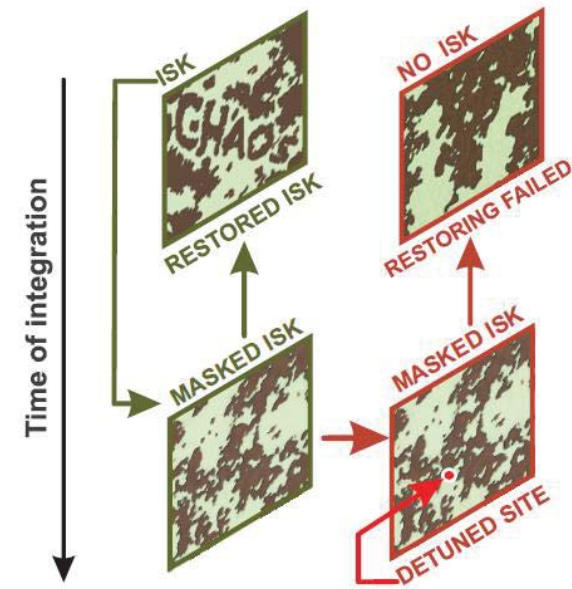
Integrate backwards in time

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. Lapyeva, 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

Scientists Develop New Method to Improve Passwords : crypto - Mozilla Firefox


File Edit View History Bookmarks Tools Help

http://www.reddit.com/r/crypto/comments/ghlu3/scientists_develop_new_method_to_improve_passwords/

Most Visited Getting Started Latest Headlines

Sergej's World: web page of Sergej ... Scientists Develop New Method to Improve Passwords

ALL - RANDOM - PICS - REDDIT.COM - FUNNY - POLITICS - GAMING - ASKREDDIT - WORLDNEWS - VIDEOS - IAMA - TODAYILEARNED - FFFFFFFUUUUUUUUUUUUUU - TREES - ATHEISM - WTF - STARCRAFT - ADVICEANIMALS - MORE »

 CRYPTO comments related

want to join? register in seconds | English

↑ Scientists Develop New Method to Improve Passwords (slashdot.org)
3 submitted 1 day ago by cryptokey
↓ 10 comments share

all 10 comments
sorted by: **best** ▼

↑ [-] sapiophile 8 points 1 day ago
↓ Brilliant method, and very practical.
Original arxiv paper here. (why link to the slashdot page?)
permalink

↑ [-] skolor 1 point 21 hours ago
↓ I'd say this adds little practical security over simply using a unique salt for each user. We live in a day and age where you can get CAPTCHAs cracked by a human in a developing country for under a penny. Some quick googling turned up a result offering 50,000 CAPTCHAs cracked for \$300.
While it is a cost, it isn't nearly insurmountable, it simply adds a fairly trivial additional cost onto the cracking process.
permalink

↑ [-] phyzome 2 points 1 day ago*
↓ So, as I understand this... the user memorizes half of the password, and when they go to decrypt, a CAPTCHA is produced showing the rest of the password. Automated attacks can't verify that a guessed first-half password is correct without powerful OCR.
(What did "scientists" have to do with this, though? I see no scientific method or exploration of the laws of nature.)
permalink

↑ [-] electronics-engineer 3 points 1 day ago
↓ Happens all the time. Engineers design things, Scientists get the credit. Occasionally, just for variety, the media gives credit to technicians for work done by engineers.
permalink parent

search reddit

this post was submitted on 03 Apr 2011
3 points (63% like it)
7 up votes 4 down votes
shortlink: redd.it/ghlu3

☐ remember me [recover password](#)

crypto
[+ frontpage](#) 1,840 readers

This subreddit is intended for links and discussions surrounding the theory and practice of *strong* cryptography, which lives at an intersection of math, programming, and computer science.

Other subreddits of interest:

- [Codes and ciphers](#) - for code cracking challenges
- [Network security](#) - the most common practical use of crypto
- [Web security](#) - less crypto, but still security
- [Computer security](#) - local security

Feel free to message the moderators with [zoterc](#)

Done

18:28 08.04.2011

Reactions of a virtual world

Slashdot Search (20) - Mozilla Firefox

File Edit View History Bookmarks Tools Help




http://it.slashdot.org/index2.pl?fhfilter=max+planck

Most Visited Getting Started Latest Headlines

Sergej's World: web page of Sergej ... Slashdot Search (20)

Slashdot max planck

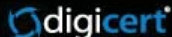
Submit Story Log In Join

Follow us:   

Ads by Google

**UNIFIED COMMUNICATIONS
SSL CERTIFICATES**

- Multiple domain names
- Unlimited server license
- One incredible price

FIND OUT MORE 


Slashdot is powered by [your submissions](#), so send in your scoop

Scientists Develop New Method To Improve Passwords

Posted by **timothy** on Sunday April 03, @09:34AM
from the start-thinking-of-random-things dept.

An anonymous reader writes

"Scientists at Max-Planck-Institute for Physics of Complex Systems in Dresden, Germany have developed a novel method to improve password security. A strong long password is split in two parts. The first part is memorized by a human. The second part is stored as a CAPTCHA-like image of a chaotic lattice system."

Read the **104** comments  [captcha](#) [security](#) [cryptography](#)

2011 2010

Facebook Ads Could 'Out' Gay Users 196

F1 Simulators Revealed 72

Tool Use By Humans Pushed Back By 800,000 Years 189

Comcast Customers Urged To Opt-Out of Settlement 128

New Ancient Human Identified 148

Recent Tags

government
privacy
usa
yro
news

Done

zotero

DE 18:32 08.04.2011

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... x +

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

MAX-PLANCK-GESELLSCHAFT

Research publication
April 19, 2011

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... x SP CAPTCHAs with chaos: Strong protec... x +

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.

See Also:

- Matter & Energy**
 - Physics
 - Quantum Physics
 - Solar Energy
- Computers & Math**
 - Computer Science
 - Artificial Intelligence
 - Hacking
- Reference**
 - Security engineering
 - Computer security
 - Cryptography
 - Malware

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-remember section they encrypt a CAPTCHA ("completely automated public Turing test to tell computers and humans apart") -- an image that computer programs perse 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 CAPTCHAs



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

CAPTCHA chaos | plus.maths.org - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Sergej's World: web page of Sergej Fl... x CAPTCHA chaos | plus.maths.org x +

http://plus.maths.org/content/captcha-chaos

about Plus support Plus Plus sponsors subscribe to Plus terms of use

+ plus magazine ...living mathematics

Home Articles Careers Blog News Packages Podcasts Posters Puzzles Reviews

CAPTCHA chaos

by Marianne Freiberger

Submitted by mf344 on April 13, 2011

If you are prone to forgetting your passwords, you're not alone. To make sure we remember all our passwords, many of us take measures that defeat the purpose. These include, as studies have shown, using the same password for everything, with things like "password1" or "abc123" particular favourites, or writing them down on post-it notes and sticking them to our computer. But such sloppiness makes easy work for evil agents out to steal our data and identities. And with no small effect. Recent studies have revealed that identity theft affects nearly 10 million people in the US each year and in 2006 alone cost the US economy more than \$55 billion.

But now physicists from the US and Germany have devised a safer way of using passwords that takes account of the human need for memorability. It exploits mathematical chaos and our ability to recognise images much better than computers can.

Conventional methods of protecting personal data, for example your bank account details, rely on encryption algorithms. These shuffle and substitute the symbols in the message that's to be encoded according to a specific recipe. While the recipes themselves are publicly available, the [Advanced Encryption Standard](#) (AES) used by the US government is an example, parts of them depend on a *cryptographic key*, for example a user-chosen password, and only those in possession of the key can run the algorithm backwards to decrypt the message.

If passwords were just long and random strings of characters, then brute-force attacks, trying out all possible passwords, would be unfeasible. But with a severely limited password pool, resulting from people being sloppy in their password choice, such attacks become possible. Computers can be programmed to try out each one of the possible passwords to obtain a text that may be the true message. They can then search this text for patterns, correlations and other tell-tale signs to see if it represents meaningful information. If it does, then the password has been cracked.

Constructing our lives: the mathematics of engineering

What do Gollum, the new Olympic stadium that's being built in London and the quest for sustainable energy...

Science fiction, science fact: reports from the frontiers of physics

What is time? What is space? What's the role of chance in the universe? Join Plus and FQXi on a journey...

Face to face

How would it feel to look in a mirror and see...

zotero

DE 13:01 05.07.2011

Reactions of a virtual world

Featured on more than 230 web sites worldwide

