

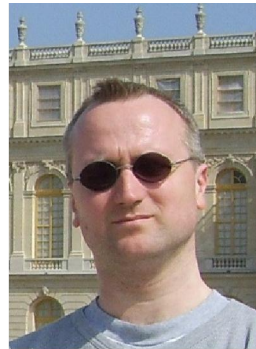
# Bitcoin Security: Cryptographic Risks

Nicolas T. Courtois University College London, UK

with special thanks to Jean-Jacques Quisquater [UCL Belgium] who taught me cryptography when I was a student but could not make it today

## Dr. Nicolas T. Courtois

1. cryptologist and codebreaker



## UNIVERSITY CIPHER CHAMPION

March 2013



2. payment and smart cards (e.g. bank cards, Oyster cards etc...)



### Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

# LinkedIn


**LinkedIn**  Account Type: Basic

[Home](#) [Profile](#) [Contacts](#) [Groups](#) [Jobs](#) [Inbox](#) **2** [Companies](#) [News](#) [More](#)

Your Groups (51) [Reorder »](#)


[+ Create a](#)



 Code Breakers

Members (712)



 IACR Cryptographers





# UCL Bitcoin Seminar

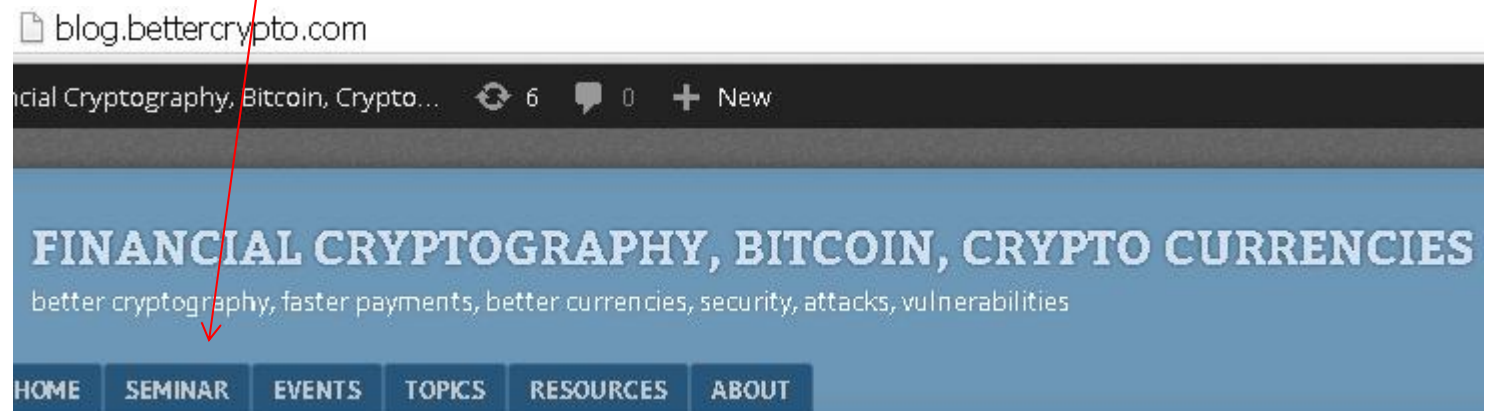
**research** seminar

=>In central London, runs EVERY WEEK!

public web page:

[blog.bettercrypto.com](http://blog.bettercrypto.com) / SEMINAR

or Google "UCL bitcoin seminar"



## New Powerful Attacks On ECDSA In Bitcoin Systems

Posted by admin on 23 October 2014, 10:57 pm

There is a wave of new powerful cryptographic attacks on bitcoin systems.





## Our Works on Bitcoin



-cf. also [blog.bettercrypto.com](http://blog.bettercrypto.com)

- Nicolas Courtois, Marek Grajek, Rahul Naik: [The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining](http://arxiv.org/abs/1310.7935), <http://arxiv.org/abs/1310.7935>
- Nicolas Courtois, Marek Grajek, Rahul Naik: [Optimizing SHA256 in Bitcoin Mining](#), CSS 2014, Springer.
- Nicolas Courtois, Lear Bahack: [On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency](http://arxiv.org/abs/1402.1718) <http://arxiv.org/abs/1402.1718>
- Nicolas Courtois: [On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies](http://arxiv.org/abs/1405.0534) <http://arxiv.org/abs/1405.0534>
- Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy: [Could Bitcoin Transactions Be 100x Faster?](#) In proceedings of SECRYPT 2014, 28-30 August 2014, Vienna, Austria.
- Nicolas T. Courtois, Pinar Emirdag and Filippo Valsorda: [Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events](http://eprint.iacr.org/2014/848), 16 Oct 2014, <http://eprint.iacr.org/2014/848>
- Poster: [http://www.nicolascourtois.com/bitcoin/POSTER\\_100x\\_Secrypt2014\\_v1.0.pdf](http://www.nicolascourtois.com/bitcoin/POSTER_100x_Secrypt2014_v1.0.pdf)

## My Whole Life:

Tried to improve  
the security baseline...

## My Whole Life:

Tried to improve  
the security baseline...

Crying Wolf!

51%, Elliptic Curve, OpenSSL...





It did NOT help,

The Wolf was allowed to operate





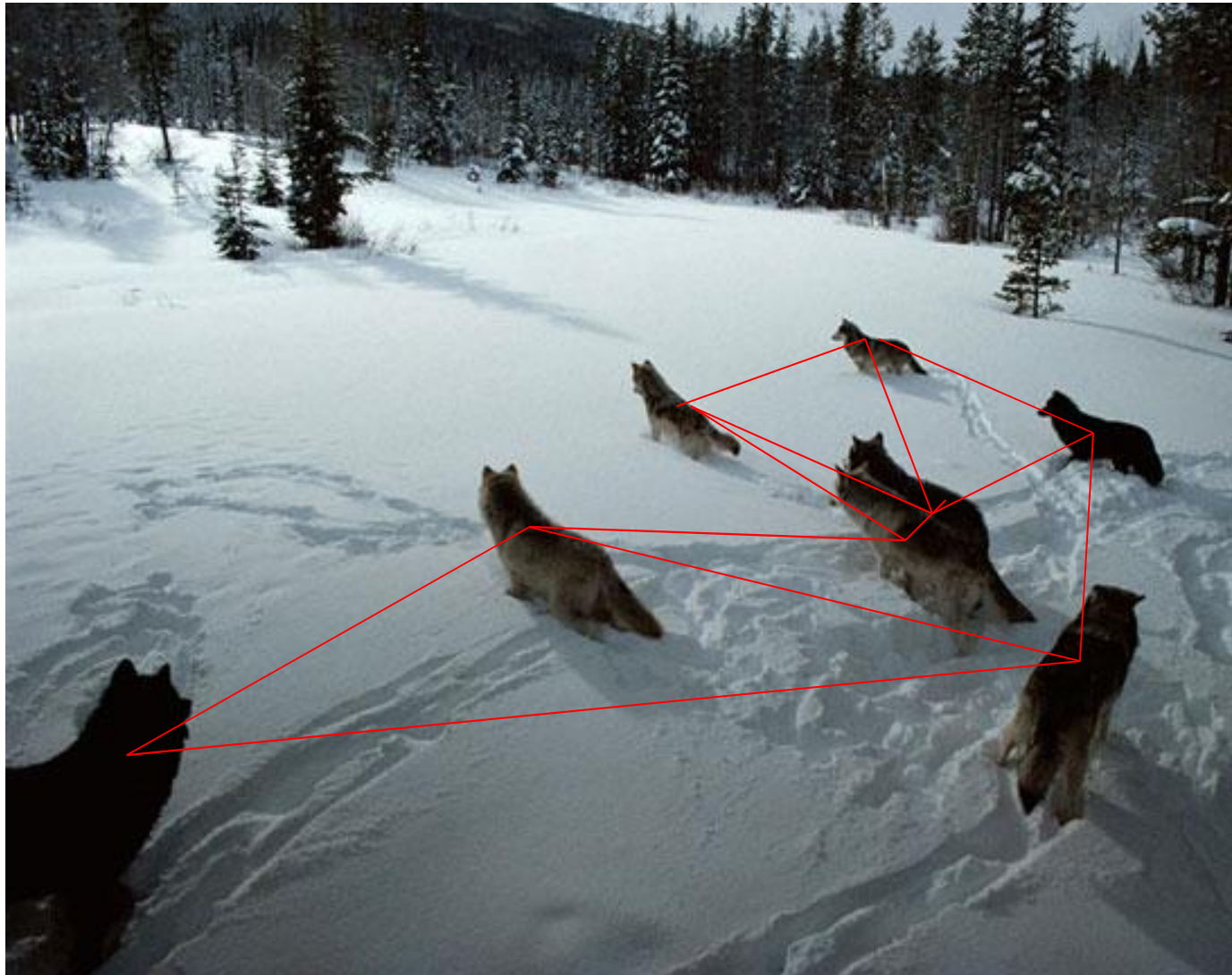
We failed to protect our DATA



We fail to protect our **MONEY**



# Solution = Decentralized P2P



## Solution = BlockChain



- Until recently, we've needed central bodies – banks, stock markets, governments, police forces – to settle vital questions.
  - Who owns this money?
  - Who controls this company?
  - Who has the right to vote in this election?
- Now we have a small piece of pure, **incorruptible** mathematics enshrined in computer code that will allow people to solve the thorniest problems without reference to “the authorities”.

<http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html>

[11 June 2014]

**The Telegraph**

## But Is Cryptography Incorruptible?

NSA 2013 Budget, excerpts:

[...] actively engages the US and foreign IT industries to **covertly influence** and/or overtly leverage their commercial products' designs.

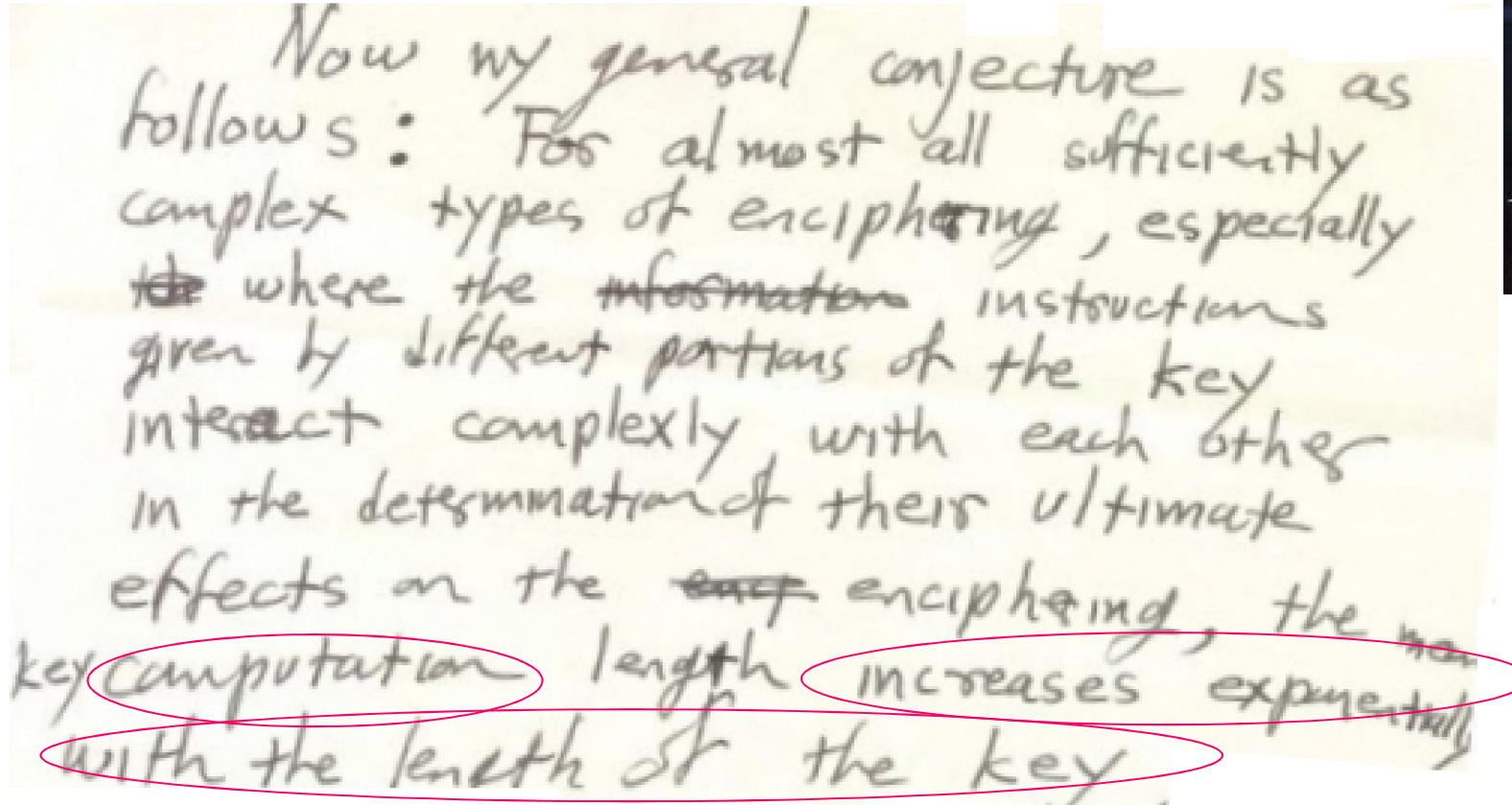


[...] **Insert vulnerabilities** into commercial encryption systems [...]

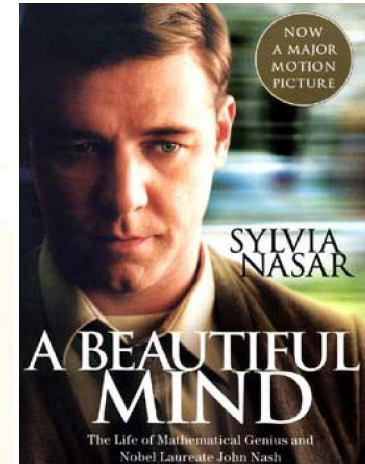
[...] Influence policies, standards and specification for commercial **public key technologies**. [...]

## John Nash - 1955

In 2012 the NSA declassified his hand-written letter:



Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially ~~the~~ where the ~~information~~ instructions given by different portions of the key interact complexly, with each other in the determination of their ultimate effects on the ~~enc~~ enciphering, the key computation length increases exponentially with the length of the key.

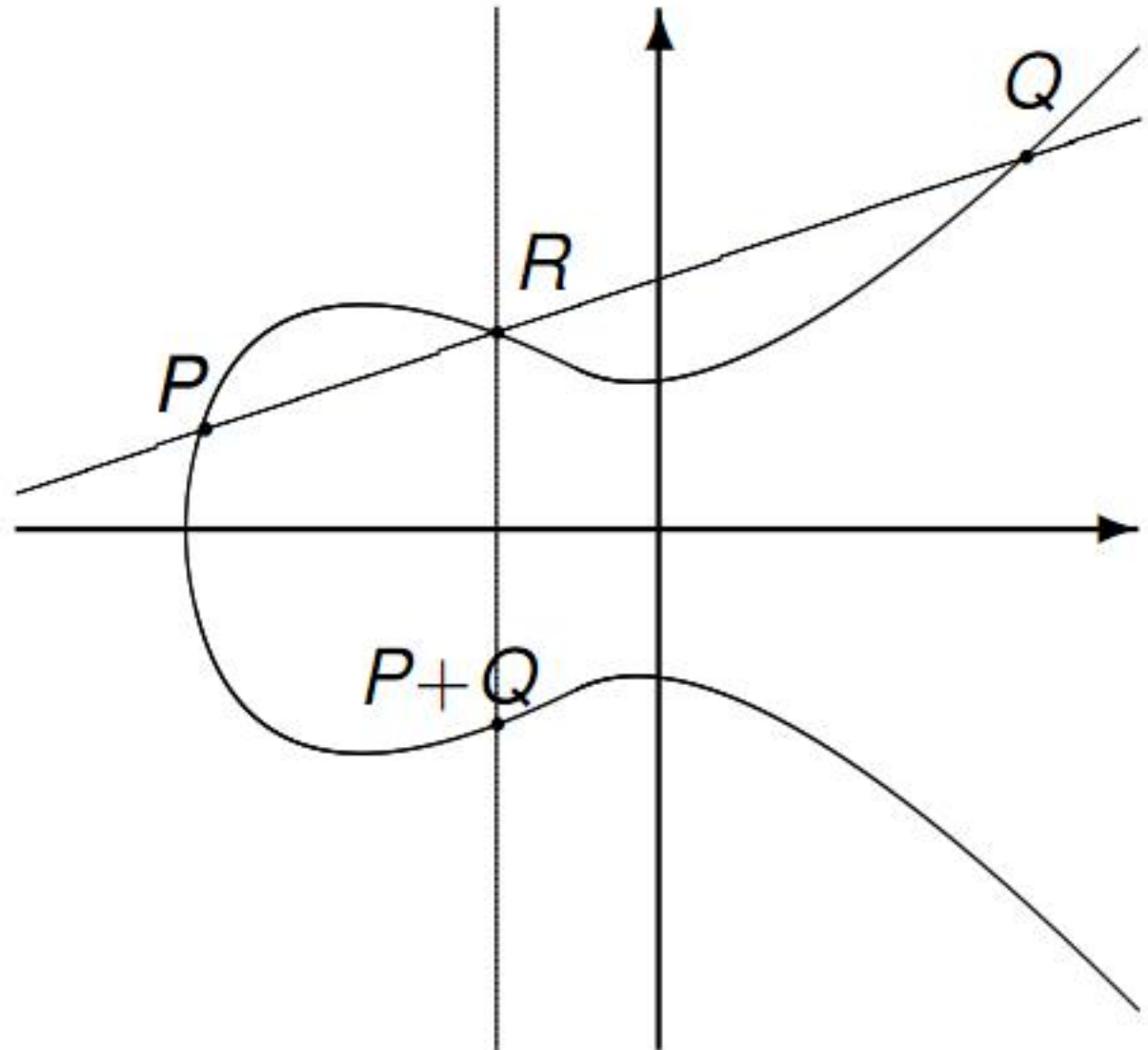
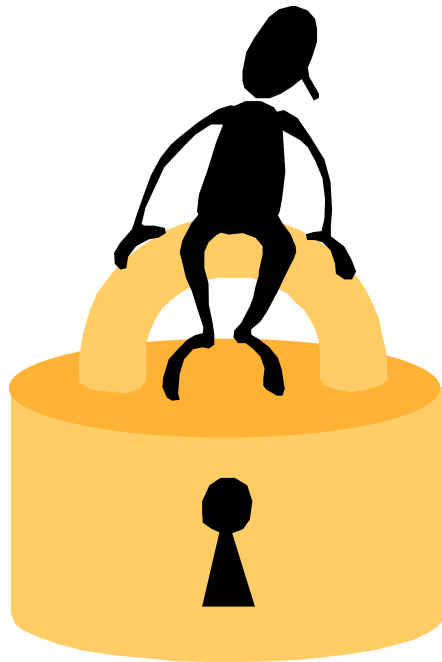


He also says that:

[...] the game of cipher breaking by skilled teams, etc., should become a thing of the past." [...]

# Elliptic Curve Crypto

“exponential  
security”





## ECC - Certicom Challenges [1997, revised 2009]

ECC2K-95	97	18322	\$ 5,000
ECC2-97	97	180448	\$ 5,000

ECCp-97	97	71982	\$ 5,000
---------	----	-------	----------

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-108	109	$1.3 \times 10^6$	\$10,000
ECC2-109	109	$2.1 \times 10^7$	\$10,000
ECC2K-130	131	$2.7 \times 10^9$	\$20,000
ECC2-131	131	$6.6 \times 10^{10}$	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-109	109	$9.0 \times 10^6$	\$10,000
ECCp-131	131	$2.3 \times 10^{10}$	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-163	163	$2.48 \times 10^{15}$	\$30,000
ECC2-163	163	$2.48 \times 10^{15}$	\$30,000
ECC2-191	191	$4.07 \times 10^{19}$	\$40,000
ECC2K-238	239	$6.83 \times 10^{26}$	\$50,000
ECC2-238	239	$6.83 \times 10^{26}$	\$50,000
ECC2K-358	359	$7.88 \times 10^{44}$	\$100,000
ECC2-353	359	$7.88 \times 10^{44}$	\$100,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-163	163	$2.3 \times 10^{15}$	\$30,000
ECCp-191	192	$4.8 \times 10^{19}$	\$40,000
ECCp-239	239	$1.4 \times 10^{27}$	\$50,000
ECCp-359	359	$3.7 \times 10^{45}$	\$100,000

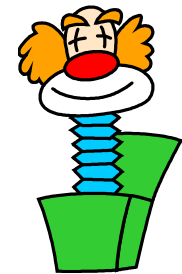
# TOTAL = 725,000 USD

## P vs. NP

- If you solve P vs. NP it: 1 M\$.
- Nobel price, Abel price in mathematics: roughly 1M\$
- Break bitcoin ECC: About 4 BILLION \$.

# How to Steal Bitcoins

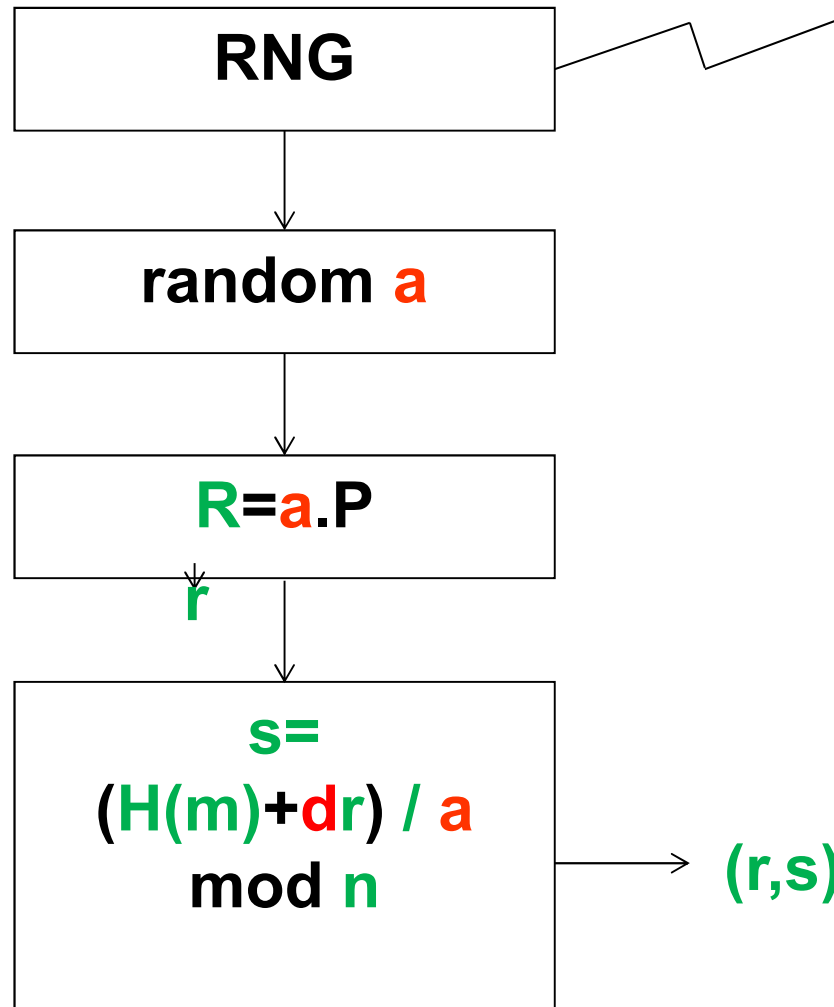
New attacks [Courtois et al. October 2014]



# ECDSA Attack – 2 Users

has already happened  
100 times in Bitcoin

random **a**: must be kept secret!



same **a** used twice  $\Rightarrow$   
detected in public  
blockchain  $\Rightarrow$

$$(s_1 a - H(m_1)) / d_1 = r = (s_2 a - H(m_2)) / d_2 \text{ mod } n$$

$\Rightarrow$

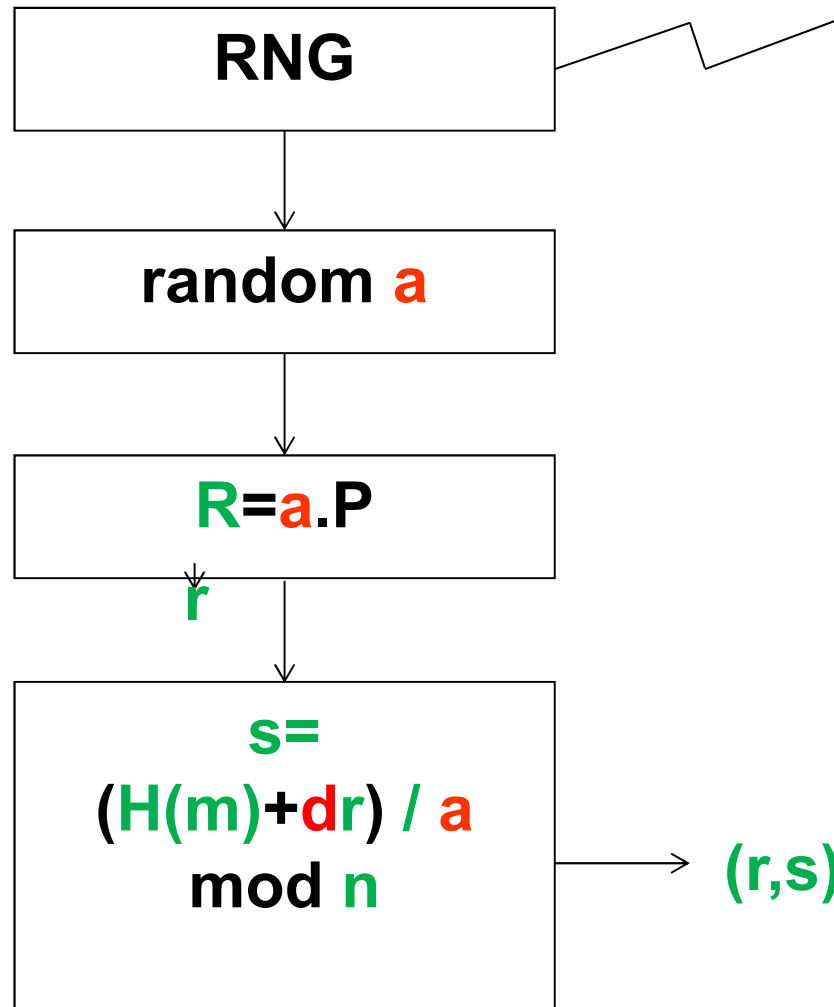
$$r(d_1 - d_2) + a(s_1 - s_2) = H(m_2) - H(m_1) \text{ mod } n$$

each person can steal the  
other person's bitcoins!

$\Rightarrow$  any of them CAN  
recompute **k** used

# Attack – Same User

random **a**: must be kept secret!



has also happened many times in Bitcoin

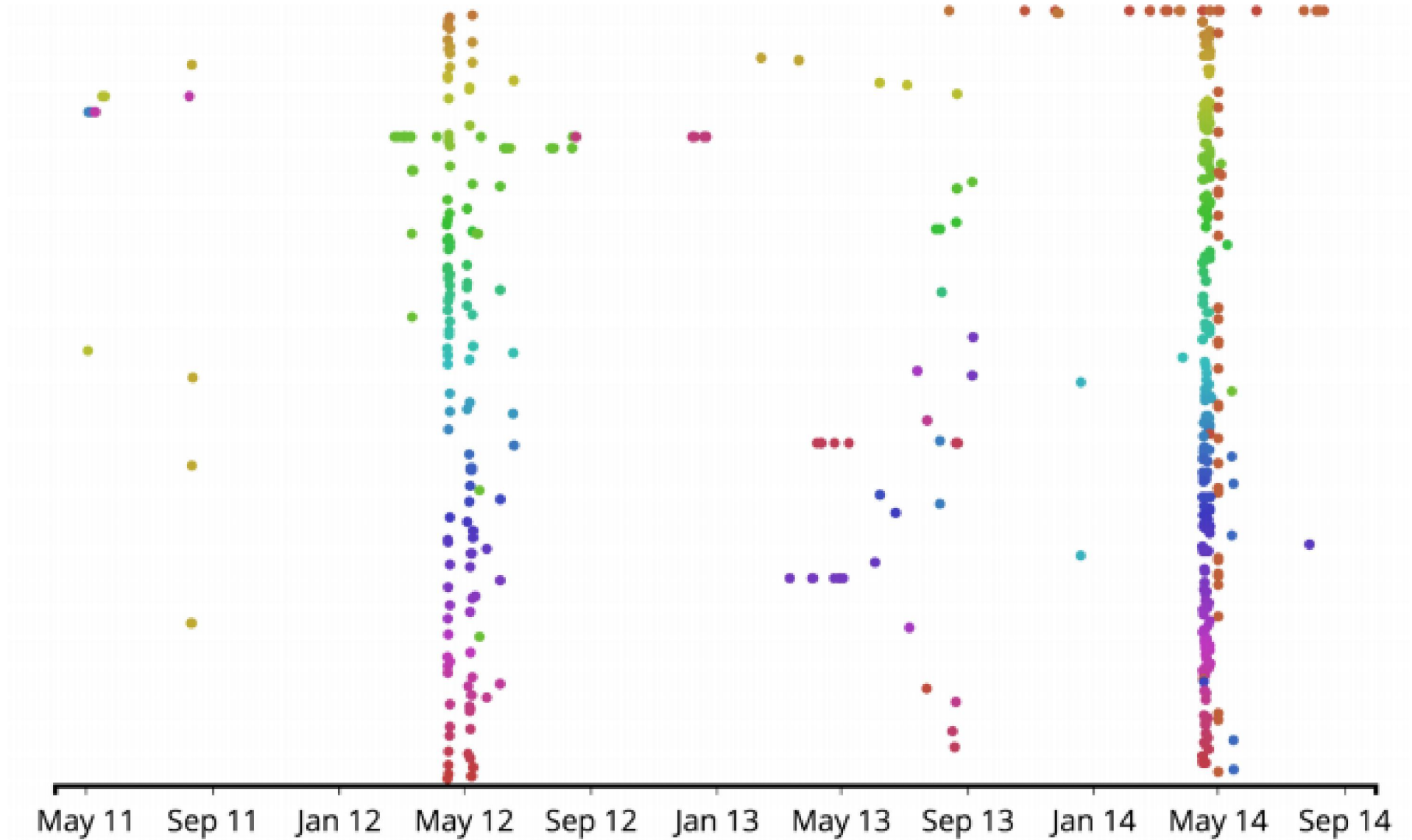
same **a** used twice by the same user ( $d_1 = d_2$ ). In this case we have:  $(s_1 a - H(m_1)) = rd = (s_2 a - H(m_2)) \mod n$   
 $\Rightarrow a = (H(m_1) - H(m_2)) / (s_1 - s_2) \mod n$  AND now  $d = (sa - H(m)) / r \mod n$

anybody can steal the bitcoins!

# Stopped in 2013?

Android bug was fixed...

## Second Major Outbreak – May 2014





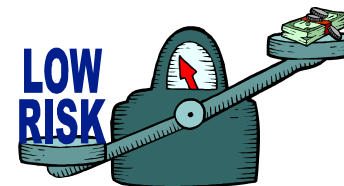
## Recent Bad Randoms

From my own scan:

0f25a7cc9e76ef38c0feadcfa5550c173d845ce36e16bde09829a  
3af57097240.

Appears 8 times in block 322925  
28 September 2014

Used by different users...



## So What?

### Previous attacks:

- Classical bad random attacks typically concern only very few bitcoin accounts, and only some very lucky holders of bitcoins can actually steal other people's bitcoins.
- Only **a few hundred accounts** in the whole history of bitcoin are affected.



# The Really Scary Attacks

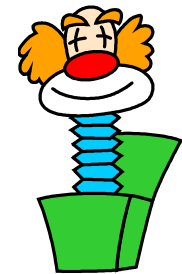
New attacks [Courtois et al. October 2014]

=> under certain conditons

ALL bitcoins in cold storage

can be stolen

=> millions of accounts potentially affected.





## New Paper:

### Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events

cf.

[eprint.iacr.org/  
2014/848/](http://eprint.iacr.org/2014/848/)

Nicolas T. Courtois<sup>1</sup>

Pinar Emirdag<sup>2</sup>

Filippo Valsorda<sup>3</sup>

<sup>1</sup> University College London, UK

<sup>2</sup> Independent market structure professional, London, UK

<sup>3</sup> CloudFlare, London, UK



**Abstract.** In this paper we study the question of key management and practical operational security in bitcoin digital currency storage systems. We study the security two most used bitcoin HD Wallet key management solutions (e.g. in BIP032 and in earlier systems). These systems have extensive audit capabilities but this property comes at a very high price. They are excessively fragile. One small security incident in a remote corner of the system and everything collapses, all private keys can be recovered and ALL bitcoins within the remit of the system can be stolen. Privilege escalation attacks on HD Wallet solutions are not new. In this paper we take it much further. We propose new more advanced **combination attacks** in which the security of keys hold in cold storage can be compromised without executing any software exploit on the cold system, but through security incidents at operation such as **bad random number or related random events**.

In our new attacks all bitcoins over whole large security domains can be stolen by people who have the auditor keys which are typically stored in hot systems connected to the Internet and can be stolen easily. Our combination attacks allow to recover private keys which none of the

## Solutions:

### Solution 1:

Deterministic signatures =  
RFC6979 by Thomas Pornin

### Solution 2:

MultiSig:

For example 2 out of 3 signatures  
are required to spend bitcoins.

BTW. Multi-Sig Concept is NOT new...

1993

**Efficient multi-signature schemes  
for cooperating entities**

Olivier Delos <sup>1</sup> and Jean-Jacques Quisquater <sup>2</sup>

# How to Un-corrupt Cryptography



## Crypto Challenges:

I always liked this idea.

Claiming (very naive) that this would:

“punish those who  
by their ignorance, incompetence  
or because of a hidden agenda,  
put everybody's security at a great risk.”

[Courtois, May 2006, Quo Vadis Cryptology 4 conference]

## ECC - Certicom Challenges [1997, revised 2009]

ECC2K-95	97	18322	\$ 5,000
ECC2-97	97	180448	\$ 5,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-108	109	$1.3 \times 10^6$	\$10,000
ECC2-109	109	$2.1 \times 10^7$	\$10,000
ECC2K-130	131	$2.7 \times 10^9$	\$20,000
ECC2-131	131	$6.6 \times 10^{10}$	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-163	163	$2.48 \times 10^{15}$	\$30,000
ECC2-163	163	$2.48 \times 10^{15}$	\$30,000
ECC2-191	191	$4.07 \times 10^{19}$	\$40,000
ECC2K-238	239	$6.83 \times 10^{26}$	\$50,000
ECC2-238	239	$6.83 \times 10^{26}$	\$50,000
ECC2K-358	359	$7.88 \times 10^{44}$	\$100,000
ECC2-353	359	$7.88 \times 10^{44}$	\$100,000

ECCp-97	97	71982	\$ 5,000
---------	----	-------	----------

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-109	109	$9.0 \times 10^6$	\$10,000
ECCp-131	131	$2.3 \times 10^{10}$	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-163	163	$2.3 \times 10^{15}$	\$30,000
ECCp-191	192	$4.8 \times 10^{19}$	\$40,000
ECCp-239	239	$1.4 \times 10^{27}$	\$50,000
ECCp-359	359	$3.7 \times 10^{45}$	\$100,000

**secp256k1**  
**NOT INCLUDED**  
 no price if you  
 break it ☹



## Timely Denial

Dan Brown, chair of SEC [Certicom, Entrust, Fujitsu, Visa International...]

**“I did not know that BitCoin is using secp256k1.  
I am surprised to see anybody use secp256k1 instead of secp256r1”,**

September 2013,

<https://bitcointalk.org/index.php?topic=289795.80>

# Comparison:

Used/recommended by:	secp256k1	secp256r1
Bitcoin, anonymous founder, no one to blame...	Y	
SEC Certicom Research	surprised!	Y
TLS, OpenSSL	ever used???	Y <b>98.3%</b> of EC
U.S. ANSI X9.63 for Financial Services	Y	Y
NSA suite B, NATO military crypto		Y
U.S. NIST		Y
IPSec		Y
OpenPGP		Y
Kerberos extension		Y
Microsoft implemented it in Vista and Longhorn		Y
EMV bank cards XDA [2013]		Y
German BSI federal gov. infosec agency, y=2015		Y
French national ANSSI agency beyond 2020		Y



## Wanna Bet?

### Bitcoin Cryptography Broken in 2015

Category: [Bitcoin](#)

By [NCourtois](#) ★★★★★

#### 📄 Description

The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers. The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them. It should be done faster than  $2^{100}$  point additions total including the time to examine the data.

#### 🕒 Decision Logic



bitcoin, cryptography, SHA256, ECDSA, ECDL, secp256k1

<https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791>

# [betmoose.com](http://betmoose.com) - Totally Anonymous Bets In BTC!

FEATURED

## Bitcoin Cryptography Broken in 2015

Category: Bitcoin

By  NCourtois ★★★★★

### Description

The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers. The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them. It should be done faster than  $2^{100}$  point additions total including the time to examine the data.



SHA256, ECDSA, ECDL, secp256k1

### Decision Logic

YES	
Volume:	₿ 0.140
# of Bets:	3
₿	
PAYOUT	ROI
₿ 0.00	0%
* assumes current weight and volumes	
Place Anonymously	

NO	
Volume:	₿ 0.189
# of Bets:	6
₿ 0.1	
PAYOUT	ROI
₿ 0.14327	43.27%
* assumes current weight and volumes	
Place Anonymously	



## Amount?

- Don't bet a ridiculous amount!
- As long as we don't have 2000 BTC in this bet, we will simply NOT yet know if bitcoin ECC is broken...

<https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791>

- Don't expect that code breakers who can make 725,000 \$ elsewhere, will even try to break bitcoin Elliptic Curve
- They would rather steal some bitcoins
  - Possible only if your public key is revealed  
=> Tip: use each Bitcoin address only once!



## Anarchy? Dark Side

- In Bitcoin many things which are BUGS are presented as FEATURES:
    - monetary policy (or the lack of one) – frequent criticism
    - problematic cryptography=
      - anonymous founder syndrome, standardized yet TOTALLY disjoint from normal industrial cryptography, NOBUS syndrome (NSA jargon)
    - decision mechanisms (the Longest Chain Rule)
      - no reason why the same mechanism decides which blocks are valid and which transactions are valid, by far too slow, too unstable, too easy to manipulate
    - 51% attacks ARE realistic feasible and ... INEXPENSIVE!
    - sudden jumps in monetary policy => genetically-programmed self-destruction of many crypto currencies
- See: Nicolas Courtois: [On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies](http://arxiv.org/abs/1405.0534) <http://arxiv.org/abs/1405.0534>



## Dangers of Open Source

- the open-source nature of the developer population provides **opportunities for frivolous or criminal behavior** that can damage the participants in the same way that investors can be misled by promises of get rich quick schemes [...]
- one of the biggest **risks** that we face as a society in the digital age [...] is the **quality of the code** that will be used to run our lives.

Cf. Vivian A. Maese: [Divining the Regulatory Future of Illegitimate Cryptocurrencies](#), In Wall Street Lawyer, Vol. 18 Issue 5, May 2014.

## Citation

Bitcoin is:

- **Wild West** of our time [Anderson-Rosenberg]

## Improve Quality/Security?

Bitcoin Has The Solution!

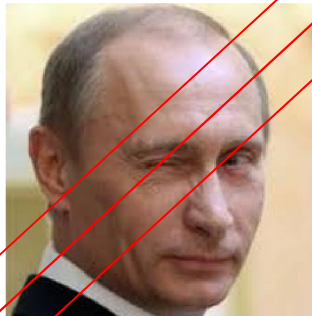


Future belongs to

**self-funded open-source communities**

⇒ can hire programmers, security experts, etc...

⇒ avoid code of dubious origin



## Crypto Challenges:

I always liked this idea.

Claiming (very naive) that this would:

“punish those who  
by their ignorance, incompetence  
or because of a hidden agenda,  
put everybody's security at a great risk.”

[Courtois, May 2006, Quo Vadis Cryptology 4 conference]

## ECC - Certicom Challenges [1997, revised 2009]

ECC2K-95	97	18322	\$ 5,000
ECC2-97	97	180448	\$ 5,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-108	109	$1.3 \times 10^6$	\$10,000
ECC2-109	109	$2.1 \times 10^7$	\$10,000
ECC2K-130	131	$2.7 \times 10^9$	\$20,000
ECC2-131	131	$6.6 \times 10^{10}$	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-163	163	$2.48 \times 10^{15}$	\$30,000
ECC2-163	163	$2.48 \times 10^{15}$	\$30,000
ECC2-191	191	$4.07 \times 10^{19}$	\$40,000
ECC2K-238	239	$6.83 \times 10^{26}$	\$50,000
ECC2-238	239	$6.83 \times 10^{26}$	\$50,000
ECC2K-358	359	$7.88 \times 10^{44}$	\$100,000
ECC2-353	359	$7.88 \times 10^{44}$	\$100,000

ECCp-97	97	71982	\$ 5,000
---------	----	-------	----------

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-109	109	$9.0 \times 10^6$	\$10,000
ECCp-131	131	$2.3 \times 10^{10}$	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-163	163	$2.3 \times 10^{15}$	\$30,000
ECCp-191	192	$4.8 \times 10^{19}$	\$40,000
ECCp-239	239	$1.4 \times 10^{27}$	\$50,000
ECCp-359	359	$3.7 \times 10^{45}$	\$100,000

## Koblitz citation:

"Once I heard a speaker from NSA complain about university researchers who are cavalier about proposing **untested cryptosystems**. He pointed out that in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed.

In academia, if you write about a cryptosystem and then a few months later find a way to break it, you've got two new papers to add to your résumé!"

Neal Koblitz,  
Notices of the American Mathematical Society,  
September 2007.

## Official Bitcoin Wiki

[https://en.bitcoin.it/wiki/Myths# Bitcoins are worthless because they're based on unproven cryptography](https://en.bitcoin.it/wiki/Myths# Bitcoins_are_worthless_because_they're_based_on_unproven_cryptography)

“SHA256 and ECDSA which are used in Bitcoin are well-known industry standard algorithms. SHA256 is endorsed and used by the US Government and is standardized (FIPS180-3 Secure Hash Standard). If you believe that these algorithms are untrustworthy then you should not trust Bitcoin, credit card transactions or any type of electronic bank transfer.”

Bitcoin has a sound basis in well understood cryptography.



## Official Bitcoin Wiki

[https://en.bitcoin.it/wiki/Myths# Bitcoins are worthless because they're based on unproven cryptography](https://en.bitcoin.it/wiki/Myths# Bitcoins_are_worthless_because_they're_based_on_unproven_cryptography)

“SHA256 and ECDSA which are used in Bitcoin are well-known industry standard algorithms. SHA256 is endorsed and used by the US Government and is standardized (FIPS180-3 Secure Hash Standard). If you believe that these algorithms are untrustworthy then you should not trust Bitcoin, credit card transactions or any type of electronic bank transfer.”

Bitcoin has a sound basis in well understood cryptography.

---

Well...actually it has major **bug** in it.

⇒ Major security scandal in the making?

⇒ Expect a lawsuit??? for

- failing to adopt the crypto/industry best practices,
- for supporting a dodgy cryptography standard,
- not giving users worried about security any choice,
- and lack of careful/pro-active/ preventive security approach etc...

Blame Satoshi ☺



## Officially Not Recommended

Dan Brown, chair of SEC [Certicom, Entrust, Fujitsu, Visa International...]

**"I am surprised to see anybody use secp256k1"**

September 2013,

<https://bitcointalk.org/index.php?topic=289795.80>

# What If? CataCrypt Conference

[Jean-Jacques Quisquater] again!

← → ↻ catacrypt.net/program.html



**cata****CRYPT**



Workshop on **cata**strophic events related to **crypt**ography and their possible solutions

## Technical Program

[Home](#)

[Committees](#)

[Call for contributions](#)

[Program \(schedule\)](#)

	<b>Venue: Grand Hyatt San Francisco, Union Square, 345 Stockton Street, downtown San Francisco: room Fillmore A - Theatre Level <a href="http://grandsanfrancisco.hyatt.com">http://grandsanfrancisco.hyatt.com</a></b> <b>October 29, 2014 (together with <a href="#">IEEE Conference on Communications and Network Security (CNS)</a>)</b>
08:15 – 08:25	Opening Remarks: <b>Jean-Jacques Quisquater</b> (UCL, Belgium)



## Wanna Bet?

### Bitcoin Cryptography Broken in 2015

Category: [Bitcoin](#)

By NCourtois ★★★★★

#### 📄 Description

The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers. The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them. It should be done faster than  $2^{100}$  point additions total including the time to examine the data.

#### 🕒 Decision Logic



bitcoin, cryptography, SHA256, ECDSA, ECDL, secp256k1

<https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791>

# [betmoose.com](http://betmoose.com) - Totally Anonymous Bets In BTC!

## FEATURED

## Bitcoin Cryptography Broken in 2015

Category: [Bitcoin](#)By  [NCourtois](#) ★★★★★

### Description

The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers. The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them. It should be done faster than  $2^{100}$  point additions total including the time to examine the data.



SHA256, ECDSA, ECDL, secp256k1

### Decision Logic

YES	
Volume:	₿ 0.140
# of Bets:	3
₿	
PAYOUT	ROI
₿ 0.00	0%
* assumes current weight and volumes	
Place Anonymously	

NO	
Volume:	₿ 0.189
# of Bets:	6
₿ 0.1	
PAYOUT	ROI
₿ 0.14327	43.27%
* assumes current weight and volumes	
Place Anonymously	

## Amount?

- Don't bet a ridiculous amount!
- As long as we don't have 2000 BTC in this bet, we will simply NOT yet know if bitcoin ECC is broken...

<https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791>

- Don't expect that code breakers who can make 725,000 \$ elsewhere, will even try to break bitcoin Elliptic Curve
- They would rather steal some bitcoins
  - Possible only if your public key is revealed  
=> Tip: use each Bitcoin address only once!



## Solutions

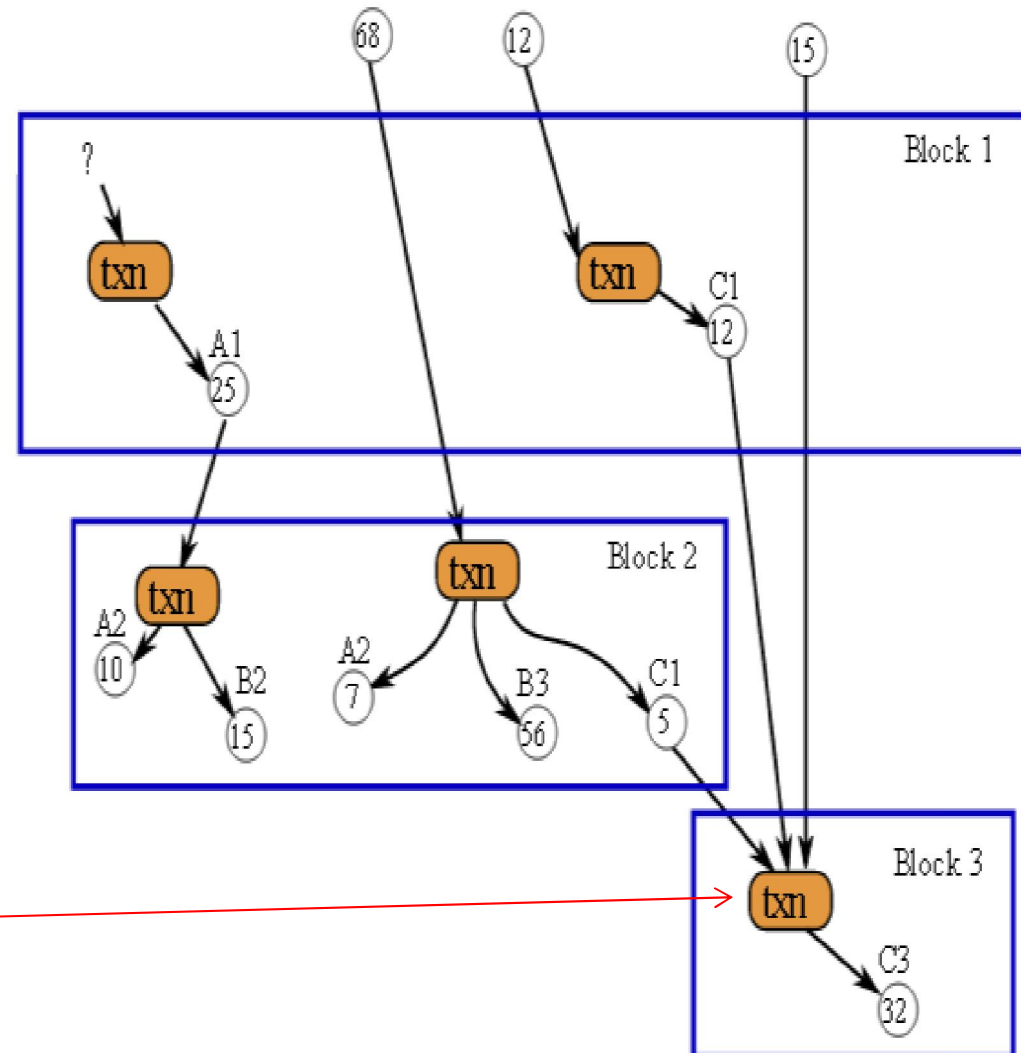
- Use each fresh bitcoin account only once!
- Satoshi did sth really brilliant:
  - Most transactions **do NOT reveal the public key**.
  - full disclosure is unbelievably stupid and simply BAD security engineering and BAD security management.
  - Example:
    - ATMs top-level public keys

51%





## Cancel A Fresh Transaction?



Cancel this?

## Can Sb. Cancel A Transaction?

Yes if he produces a longer chain with another version of the history.

Very expensive, race against the whole network (the whole planet).

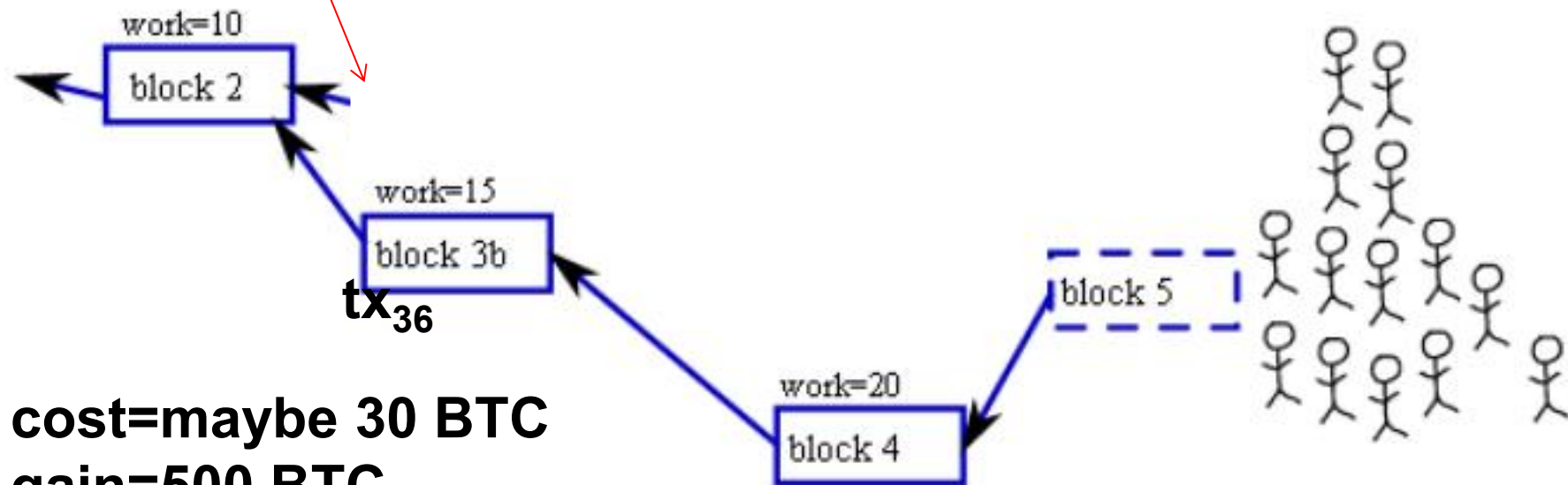
Can be easy or very difficult it depends!



## Attack:

Extend This Branch To Cancel One Transaction  $tx_{36}$

Goal: generate 4 blocks.



**cost=maybe 30 BTC**

**gain=500 BTC**

**EASY and PROFITABLE!**

**The only difficulty is the timing!!!!**

# This Attack IS FEASIBLE!

Nicolas Courtois:

On The Longest Chain Rule and Programmed Self-Destruction of Crypto  
Currencies <http://arxiv.org/abs/1405.0534>

## Easy Or Difficult?

Difficult if:

- All mining devices are privately hold by independent solo miners.

Easy if:

- Many mining devices are rented with a market which allows one instantly to buy a lot of hashing power by paying a small premium over the market price.

WORSE THAN THAT:

- A large mining pool can re-sell ALL the hash power to the attacker,  
=> this CANNOT BE DETECTED by miners,  
due to a technicality which we will discuss later  
(mining with H0, not knowing on which branch/block they mine)

# 51% - Blunders Mistakes Misunderstandings



## Is it a 51% Attack?

51 % attacks:

- computing power can be temporarily displaced.
- it is NOT a number between 0 and 100%, two different hash powers at different moments.
- almost nobody gets it right ever... including Sathoshi

## Satoshi About 51%

Amazing level of confusion already in Satoshi writings:  
in Section 6 of Satoshi paper we read that:

**WRONG: Attacker does NOT need to be powerful, hack few servers...=> 80%**

“The incentive[like 25 BTC] **may** help encourage nodes to stay honest.

If a **greedy** attacker is able to

**assemble more CPU power** than all the honest nodes,

he would have to **choose between** using it

- **to defraud people** by stealing back **his** payments,
- or using it **to generate new coins**.

**Claim: this ‘honest’ option is fiction.**

He ought to find it more profitable to play by the rules,  
such rules that favour him with more new coins than everyone else  
combined, than to undermine the system and the validity of his own  
wealth.



## Mistakes Live Forever

The Economist paper, 31 Oct 2015, page 22:

[one of the best papers on bitcoin ever seen, EXCEPT it downplays the 51% threat]:

- “Alice tries to rewrite history [...] **Short of controlling more than half the computers** - known in the jargon as 51% attack – that should not be possible.”

**WRONG:** Alice can manipulate/cheat/hack miners to work for her [MITM].

- “You cannot predict which miner will solve a puzzle so **you CANNOT predict who will get to update the blockchain** at any given time, except [...] it has to be one of hard working miners, not some random interloper”.

**WRONG:** Actually it is ALWAYS is the pool manager who updates the blockchain and DECIDES what is included in a blockchain, Miners are simple sub-workers deprived of their right to vote.