The relevance of the Chinese Lotto: 25 years outsourcing of cryptanalysis

Jean-Jacques Quisquater
Université Catholique
de Louvain
Belgium

Yvo Desmedt
The University of
Texas at Dallas
USA

August 21, 2012

1. NSA NEEDS A NEW SUPERCOMPUTER!

In November 2010 China had the largest (known) supercomputer.

Evidently, NSA might not have been happy with this.

So, we might imagine the following:


ALEXANDER

NSA director Keith B. Alexander

So, may be Keith B. Alexander went to beg:

Obama’s reaction:

Obama's reaction:

$17 trillion debt!

“New” solution:

"New" solution: NSA could outsource the cryptanalysis to, e.g. China!

Quisquater-Desmedt already mentioned "obfuscation" (called covert computation) and presented a primitive solution to prevent outsiders learn the ciphertext, plaintext and key.

Where: Rump Session Crypto 1987 with title:

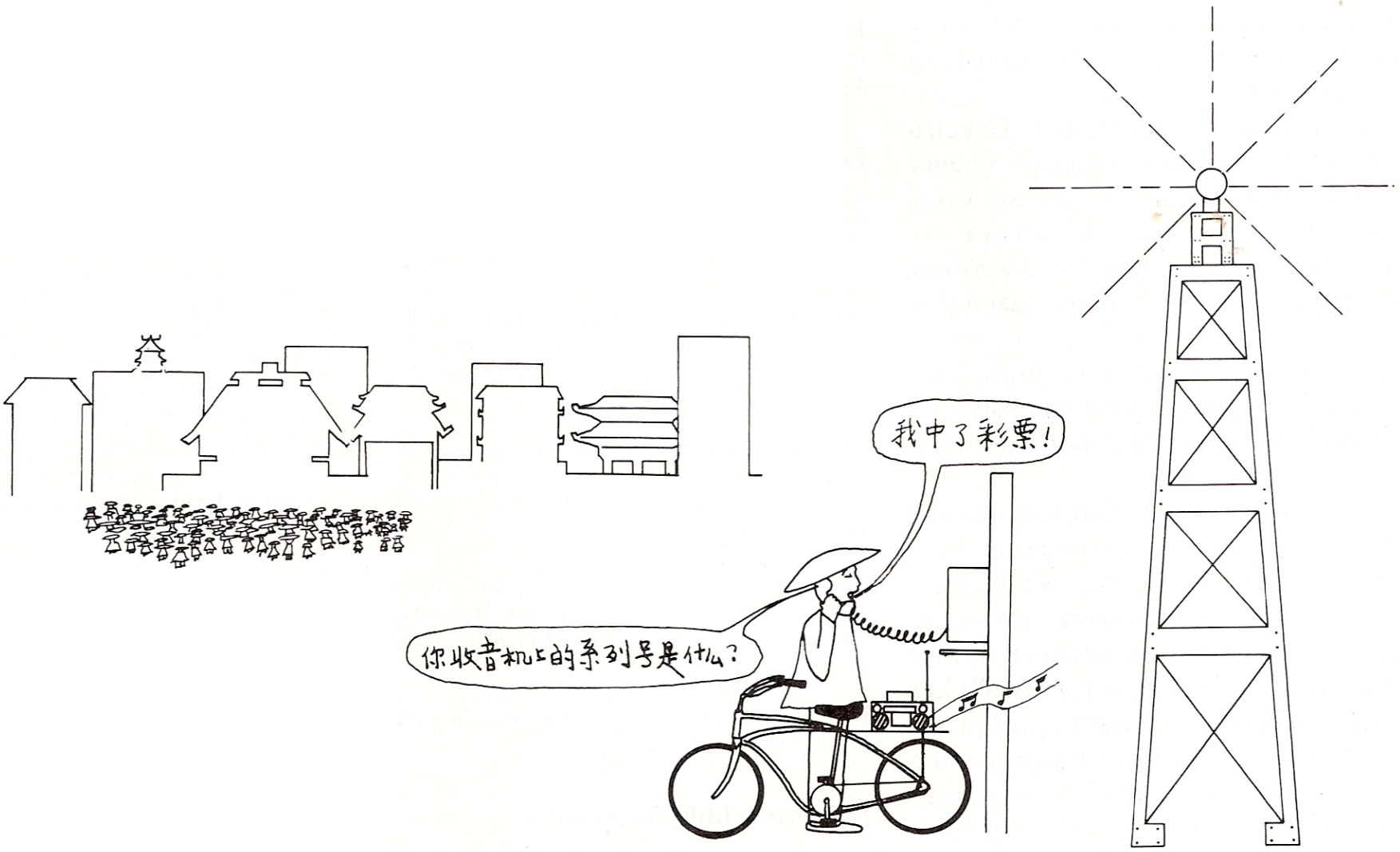
Watch for the Chinese Loto and the Chinese Dragon

Published: IEEE Computer 1991 with title:

Chinese lotto as an exhaustive code-breaking machine

Question: can obfuscation be done, or is this impossiby, using the work by Goldreich et al.?

2. APPROACH



Note: lotto did not exist in China! So, translation was not so trivial.

Today it does, so we predicted the existence of lotto in China.

http://usa.chinadaily.com.cn/china/2011-07/28/content_13003279.htm

Latest BBC Headlines

Lottery winner may hav...

21 Aug 2012 EDITIONS: CHINA | EUROPE | Search

CHINADAILY USA 中国日报

Home | China | US | World | Business | Opinion | Life | Culture | Travel | Entertainment |

China

From Chinese Media

Lottery winner may have hit $80m jackpot

Updated: 2011-07-28 11:17

By Zhang Jiawei (chinadaily.com.cn)

Comments Print Mail Large Medium Small

Twitter Facebook Myspace Yahoo! Linkedin Mixx

China's lottery may have set a new record with a man expected to win 514 million yuan ($80 million) from two tickets bought in East China's Zhejiang province on Tuesday, beating the previous record win of 359.9 million yuan, claimed by a man in Central China's Henan province in 2009.

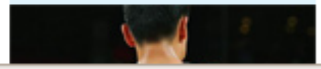
The Chutian Metropolis Daily reported Thursday two tickets sold within 34

Follow China Daily US Edition on

Specials

Turning up the heat

Traditional Chinese medicine using moxa, or mugwort herb, is once again becoming fashionable



3. WHAT ELSE DID WE PREDICT?

- Outsourcing to China!

3. WHAT ELSE DID WE PREDICT?

- Outsourcing to China!
- Serious claims:
  - our idea to distrubute exhaustive search predated Lenstra-Manasse.
  - our idea to use bio-computing predated Adleman's DNA computing.

4. CURRENT IMPACT

- On DES: irrelevant: broken.

4. CURRENT IMPACT

- On DES: irrelevant: broken.
- On AES: irrelevant: key too long

4. CURRENT IMPACT

- On DES: irrelevant: broken.
- On AES: irrelevant: key too long

So, it seems no impact!!

4. CURRENT IMPACT

- On DES: irrelevant: broken.
- On AES: irrelevant: key too long

So, it seems no impact!!

However, we found that many passwords are too short.

If using English (assume 5 bits entropy) only:

# characters	# passwords	1 PC	1 GPU	2^{60}/second
6	2^{30}	4 min.	1/4 sec.	2^{-30} sec.
7	2^{35}	2 hours	8 sec.	2^{-25} sec.
8	2^{40}	3 days	4 min.	2^{-20} sec.
9	2^{45}	3 months	2 hours	2^{-15} sec.
10	2^{50}	8 years	64 hours	2^{-10} sec.
11	2^{55}	NA	3 months	2^{-5} sec.
12	2^{60}	NA	8 years	1 sec.

Charset of 96 characters (from a keyboard):
rounded to 96 = $2^{6.5}$

# characters	Number of possibilities	1 PC (2^{22}/sec)	1 GPU (2^{32}/sec)	Rainbow table	Distributed.net boinc, botnets (2^{40}/sec)	Big one (2^{60}/sec)
6	2^{39}	32 hours	2 min.	YES	1/2 sec	2^{-21} sec
7	$2^{45.5}$	6 months	3 hours	YES	1 min.	$2^{-14.5}$ sec
8	2^{52}	NA	12 days	YES	2 hours	2^{-8} sec
9	$2^{58.5}$	NA	3 years	NA	8 days	$2^{-1.5}$ sec
10	2^{65}	NA	NA	NA	2 years	30 sec
11	$2^{71.5}$	NA	NA	NA	NA	1 hour
12	2^{78}	NA	NA	NA	NA	100 hours

Official recommendations for passwords:

For Ubuntu 7.10 (October 2007) manual for passwd:

> passwords should consist of 6 to 8 characters including one or more characters from each of the following sets: ...

in FreeBSD 8.1 (July 2010) they recommend:

> The new password should be at least six characters long (which may be overridden using the login.conf(5) "minpasswordlen" setting for a user's login class) and not purely alphabetic. Its total length must be less than `_PASSWORD_LEN` (currently 128 characters).

Finally, in "Digest Authentication" the hashed value is sent in the clear!

5. FUTURE IMPACT

In 1985 we predicted:

Quisquater and me disagree how long before this will become reality.

Quisquater favourite picture: