On the Origin of Trust: Struggle for Secure Cryptography

Anne Canteaut

On the Origin of Trust: Struggle for Secure Cryptography

Anne Canteaut

Inria, project-team SECRET, Paris, France

http://www.rocq.inria.fr/secret/Anne.Canteaut/

Attacks

In most attacks, cryptography is bypassed.

"I am not aware of any major world-class security system employing cryptography in which the hackers penetrated the system by actually going through the cryptanalysis." [Adi Shamir 2002]

Attacks

In most attacks, cryptography is bypassed.

"I am not aware of any major world-class security system employing cryptography in which the hackers penetrated the system by actually going through the cryptanalysis." [Adi Shamir 2002]

"I do not need a trophy to tell myself that I am the best."
[Zlatan Ibrahimovic 2013]

Disasters…


dna
IPL 2016
India
World
Business
Technology
Sports
Entertainment
Lifestyle
TRENDING#
Maharashtra Drought
IPL 2016
Assam Elections 2016
Home >> Sport
40
0
1
41
Champions League: Ibrahimovic misses spot kick, PSG pay the penalty against Man City
Fernandinho blasts in Manchester City's equalizer to stun the PSG supporters (Reuters)
Thu, 7 Apr 2016-10:01am , Paris , Reuters

TLS/SSL attacks

- biases in RC4 [AlFardam et al. 13]
- Logjam [Adrian et al. 15]: weak Diffie-Helman
- Sloth [Bhargavan, Leurent 16]: collisions in MD5

Attack against MIFARE

COMPUTERWORLDUK
THE VOICE OF BUSINESS TECHNOLOGY

Features Technology IT Business Careers Tut

Resources

Home › News › IT Vendors › Questions raised about Oyster card security

Questions raised about Oyster card security

Its RFID chip is cracked by researchers

Network World and Computerworld UK staff
March 7, 2008

re Smartcards with encrypted RFID chips, including London's Oyster fare card, might not be as secure as previously thought.

Can we trust cryptographers?

Rule #1

When cryptographers claim that a primitive is broken, don't use it.

Rule #1

When cryptographers claim that a primitive is broken, don't use it.

But those guys are paranoid!

Rule #1

When cryptographers claim that a primitive is broken, don't use it.

But those guys are paranoid! True.

Cryptanalysis of the full Spritz [Banik, Isobe 16]:

"We need approximatively 2^{1247} assignments to recover the internal state."

Rule #1

When cryptographers claim that a primitive is broken, don't use it.

But those guys are paranoid! True.

Cryptanalysis of the full Spritz [Banik, Isobe 16]:

"We need approximatively 2^{1247} assignments to recover the internal state."

$$2^{1247} \geq (\#\text{ atoms in the universe })^4$$

Broken?

A good primitive must behave as a function chosen at random from the set of all functions (with the same characteristics).

Broken?

A good primitive must behave as a function chosen at random from the set of all functions (with the same characteristics).

Spritz [Rivest, Schulz 15]:

Spritz generates a pseudo-random sequence from a secret state, chosen out of 2^{1730} possibilities.

Broken?

A good primitive must behave as a function chosen at random from the set of all functions (with the same characteristics).

Spritz [Rivest, Schulz 15]:

Spritz generates a pseudo-random sequence from a secret state, chosen out of 2^{1730} possibilities.

Attack: the internal state can be recovered with 2^{1247} trials

$\rightarrow$ much better than brute-force

Hash functions

$$H : \{0,1\}^\star \longrightarrow \{0,1\}^n$$

Second preimage:

Given m, find a message m' such that $H(m') = H(m)$.

Generic algorithm: Try 2^n random messages.

Hash functions

$$H : \{0,1\}^\star \longrightarrow \{0,1\}^n$$

Second preimage:

Given m, find a message m' such that $H(m') = H(m)$.

Generic algorithm: Try 2^n random messages.

Collision:

Find two messages m and m' such that $H(m) = H(m')$.

Generic algorithm: Select $2^{n/2}$ random messages.

But this is not relevant in our applications...

Finding collisions is not an issue in key-exchange protocols.

But this is not relevant in our applications...

Finding collisions is not an issue in key-exchange protocols.

Sloth attack against TLS [Bhargavan, Leurent 16]:
exploits collisions in MD5!

But these attacks are not practical...

- Attacks reveal unexpected weaknesses.

But these attacks are not practical...

- Attacks reveal unexpected weaknesses.
- Attacks always get better; they never get worse.

But these attacks are not practical...

- Attacks reveal unexpected weaknesses.
- Attacks always get better; they never get worse.

If cryptographers say that it is broken, don't use it.

What if they don't say

that it is broken?

Is there any difference between

- **AES** (NIST FIPS 197)
- **Crypto-1** (MIFARE Classic encryption)
- **Dual-EC-DRBG** (NIST SP 800-90A)

Is there any difference between

- **AES** (NIST FIPS 197)
- **Crypto-1** (MIFARE Classic encryption)
- **Dual-EC-DRBG** (NIST SP 800-90A)

AES has been standardized after an open competition (1997-2001)

Hash function competition (SHA-3)

Oct 2008	submission deadline
	$\longrightarrow$ 64 candidates received by the NIST
Dec 2008	51 candidates in the 1st round
Feb 2009	1st SHA-3 conference

Let's start the struggle!

Abacus	Neil Sholer	in round 1	2nd-preimage	
ARIRANG	Jongin Lim	in round 1		
AURORA	Masahiro Fujita	in round 1	2nd preimage	
Blender	Colin Bradbury	in round 1	collision, preimage	near-collision
Boole	Greg Rose	in round 1	collision	
Cheetah	Dmitry Khovratovich	in round 1		length-extension
CHI	Phillip Hawkes	in round 1		
CRUNCH	Jacques Patarin	in round 1		length-extension
DCH	David A. Wilson	in round 1	collision	
Dynamic SHA	Xu Zijie	in round 1	collision	length-extension

http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

Hash function competition (SHA-3)

Oct 2008	submission deadline
	$\longrightarrow$ 64 candidates received by the NIST
Dec 2008	51 candidates in the 1st round
Feb 2009	1st SHA-3 conference
July 2009	14 candidates in the 2nd round
Aug 2010	2nd SHA-3 conference
Dec 2010	5 finalists
Mar 2012	3rd SHA-3 conference
Oct 2012	winner announced (Keccak)

Prize for the best cryptanalysis

Third cryptanalysis prize

30 September 2009

We announce the third prize for the most interesting cryptanalysis of KECCAK. The results must be publicly available on an URL that is sent to keccak *-at-* noekeon *-dot-* org **before December 5, 2009** at 23:59 GMT+1 (i.e., before Sinterklaas or Saint Nicolas).

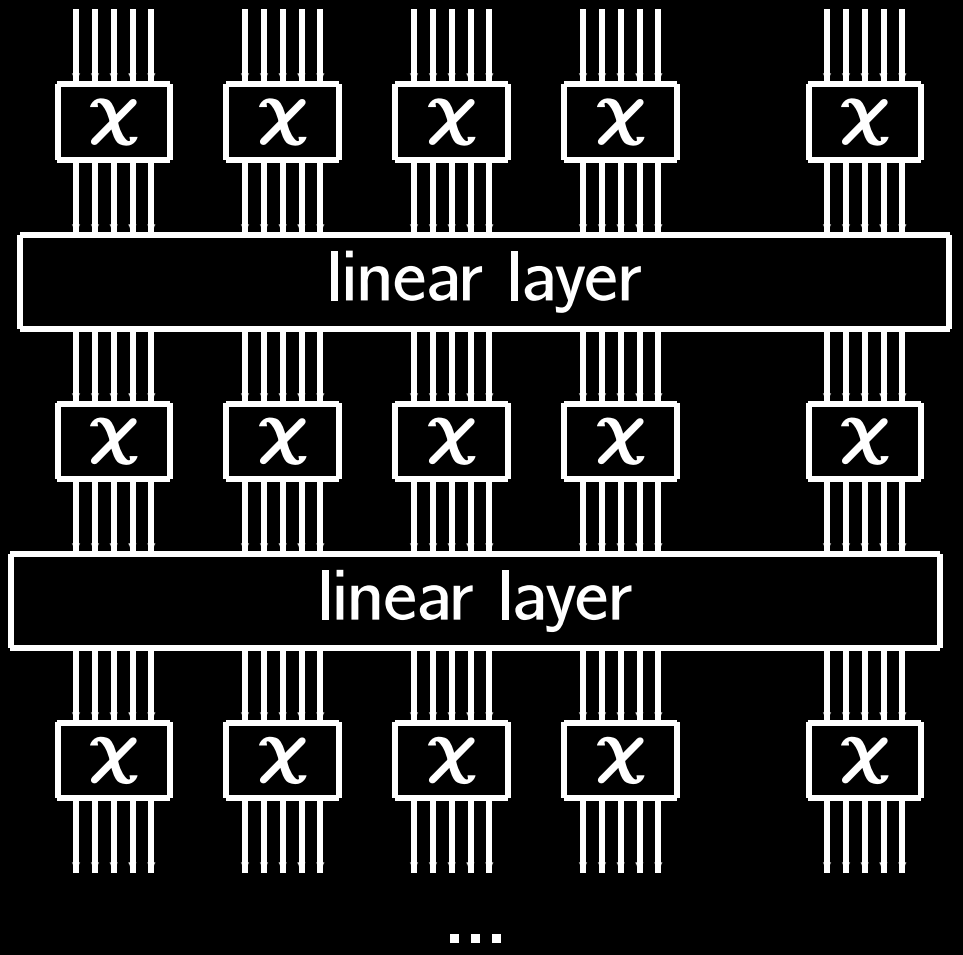
The third prize consists of beer, like the first one. This time we offer Lambic beers that according to myth can only be brewed in the surroundings of Brussels thanks to wild yeast and mysterious bacteria that would not occur anywhere else. Anyway, the prize is a case with 24 (the new number of rounds in KECCAK-*f*) bottles of Lambic-based beers from breweries such as Cantillon, Girardin, and 3 Fonteinen.

http://keccak.noekeon.org/third_party.html

Prize for the best cryptanalysis

[Boura, Canteaut 2011]: distinguisher on the inner permutation of Keccak with complexity 2^{1575} (instead of 2^{1600}).

Round-reduced versions



In Keccak, 24 rounds

How many rounds can we break?

SHA-3 (24 rounds):

collisions up to **5** rounds [Dinur, Dunkelman, Shamir 2013]

How many rounds can we break?

AES-128 (10 rounds):

5 rounds	2^{46}	Daemen, Rijmen 1998
6 rounds	2^{71}	Daemen, Rijmen 1998
6 rounds	2^{48}	Ferguson et al. 2000
7 rounds	$\simeq 2^{128}$	Gilbert, Minier 2000
7 rounds	2^{117}	Lu, Dunkelman, Keller, Kim 2008
7 rounds	2^{110}	Mala et al. 2010
7 rounds	2^{99}	Derbez, Fouque, Jean 2013

Rule #2

No public analysis, no trust

Examples:

- Crypto-1 (Mifare): proprietary design
- Simon, Speck [NSA 2015]: no design rationale

Conclusion

Public analysis is the only reliable security argument