The Coffee Block Cipher Family

A Snake Oil Candidate

Pierre Karpman

$\aleph_0$ — France

`pierre.karpman@$\aleph_0$.fr`

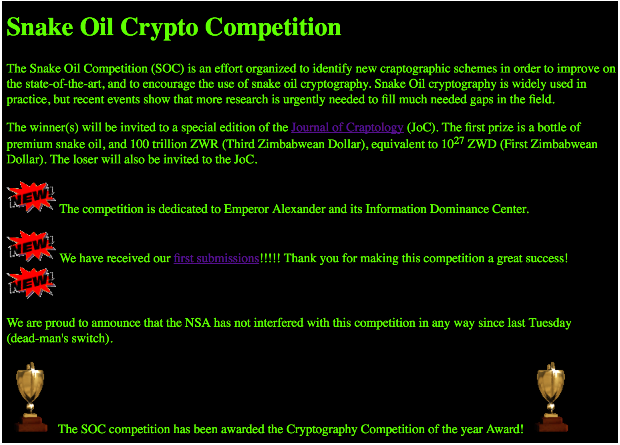
ASIACRYPT 2014 Rump Session, Kaohsiung
2014–12–09

Snake Oil competition

- Prestigious competition for new craptographic schemes

- Very serious effort, professional-looking website

Snake Oil competition



Snake Oil Crypto Competition

The Snake Oil Competition (SOC) is an effort organized to identify new craptographic schemes in order to improve on the state-of-the-art, and to encourage the use of snake oil cryptography. Snake Oil cryptography is widely used in practice, but recent events show that more research is urgently needed to fill much needed gaps in the field.

The winner(s) will be invited to a special edition of the Journal of Craptology (JoC). The first prize is a bottle of premium snake oil, and 100 trillion ZWR (Third Zimbabwean Dollar), equivalent to 10^{27} ZWD (First Zimbabwean Dollar). The loser will also be invited to the JoC.

The competition is dedicated to Emperor Alexander and its Information Dominance Center.

We have received our first submissions!!!!! Thank you for making this competition a great success!

We are proud to announce that the NSA has not interfered with this competition in any way since last Tuesday (dead-man's switch).

The SOC competition has been awarded the Cryptography Competition of the year Award!

http://snakeoil.cr.yp.to/

How traditional SPN ciphers are designed

- Alternate *substitution* and *permutation* (linear) layers
- Substitution is easy
- Permutation is hard!! Needs advanced maths (linear algebra)

Our novel (patent-pending) approach

- Do without the permutation/linear layer
- We call this SN (*substitution network*)
- ⇒ Much simpler, more efficient, very elegant!

The flexible Coffee family

1. Select S-box size
2. Select #S-boxes per block
3. Common block sizes are supported: 1, 2, 33, 89, 666

Narrow trail strategy

- At least one active S-box at every round
- Use as many rounds as S-boxes! (Or maybe more? I don't really know‽)
- Still very fast because the round function is simple

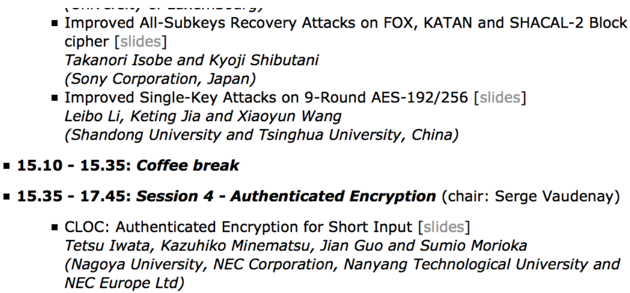
About so-called ‘Coffee break’

- Many presentations title ‘Coffee break’ at various conferences (including this one!!)
- Never included in the proceedings!
- My theory: disinformation campaign by NSA/GCHQ/DGSE
- Why? They are probably afraid that Coffee would be adopted
- Why? Because it’s so damn good!!

About so-called ‘Coffee break’

- Many presentations title ‘Coffee break’ at various conferences (including this one!!)
- Never included in the proceedings!
- My theory: disinformation campaign by NSA/GCHQ/DGSE
- Why? They are probably afraid that Coffee would be adopted
- Why? Because it’s so damn good!!

About so-called ‘Coffee break’



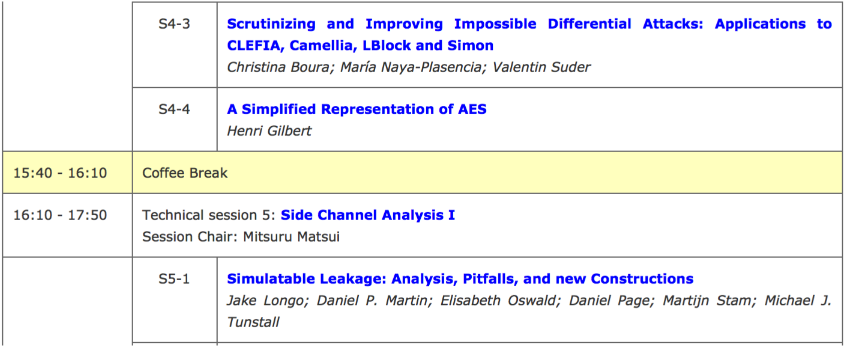
(University of Luxembourg)

- Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block cipher [slides]
  Takanori Isobe and Kyoji Shibutani
  (Sony Corporation, Japan)
- Improved Single-Key Attacks on 9-Round AES-192/256 [slides]
  Leibo Li, Keting Jia and Xiaoyun Wang
  (Shandong University and Tsinghua University, China)

- **15.10 - 15.35: *Coffee break***
- **15.35 - 17.45: *Session 4 - Authenticated Encryption*** (chair: Serge Vaudenay)
  - CLOC: Authenticated Encryption for Short Input [slides]
    Tetsu Iwata, Kazuhiko Minematsu, Jian Guo and Sumio Morioka
    (Nagoya University, NEC Corporation, Nanyang Technological University and NEC Europe Ltd)

At FSE 2014

About so-called ‘Coffee break’



	S4-3	**Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon** *Christina Boura; María Naya-Plasencia; Valentin Suder*
	S4-4	**A Simplified Representation of AES** *Henri Gilbert*
15:40 - 16:10	Coffee Break	
16:10 - 17:50	Technical session 5: **Side Channel Analysis I** Session Chair: Mitsuru Matsui	
	S5-1	**Simulatable Leakage: Analysis, Pitfalls, and new Constructions** *Jake Longo; Daniel P. Martin; Elisabeth Oswald; Daniel Page; Martijn Stam; Michael J. Tunstall*

At ASIACRYPT 2014

About so-called ‘Coffee break’

- Many presentations title ‘Coffee break’ at various conferences (including this one!!)
- Never included in the proceedings!
- My theory: disinformation campaign by NSA/GCHQ/DGSE
- Why? They are probably afraid that Coffee would be adopted
- Why? Because it’s so damn good!!

About so-called ‘Coffee break’

- Many presentations title ‘Coffee break’ at various conferences (including this one!!)
- Never included in the proceedings!
- My theory: disinformation campaign by NSA/GCHQ/DGSE
- Why? They are probably afraid that Coffee would be adopted
- Why? Because it’s so damn good!!

About so-called ‘Coffee break’

- Many presentations title ‘Coffee break’ at various conferences (including this one!!)
- Never included in the proceedings!
- My theory: disinformation campaign by NSA/GCHQ/DGSE
- Why? They are probably afraid that Coffee would be adopted
- Why? Because it’s so damn good!!

Conclusion

- More details to follow in the full version
- Positive third-party analysis welcome!
- Contact me for a quotation if you want to use Coffee (I can give you a good price in ZWR)

Conclusion

- More details to follow in the full version
- Positive third-party analysis welcome!
- Contact me for a quotation if you want to use Coffee (I can give you a good price in ZWR)

Conclusion

- More details to follow in the full version
- Positive third-party analysis welcome!
- Contact me for a quotation if you want to use Coffee (I can give you a good price in ZWR)

Thanks for you attention!