# The Inverse S-box and Two Paradoxes of Whitening

(Crypto 2004 rump session, extended version)

Nicolas T. Courtois

Crypto Research and Advanced Security,

**axalto** smart card serenity




## How White is White ?

- Much whiter than the white, that at Crypto 2003 was already so much whiter than white…


## Pure lily-white in Crypto:

Provable security
without any assumption.

Example:
A truly random permutation.





## How Black Things Can Get ?

- Pitch Black:
  Broken within a constant number of basic operations.

# Today: Whitening Paradox

The *Inv* S-box is a "cryptographic black hole":

Remains **pitch black** after astronomical amount of whitening.



axalto



# The Inverse S-box (denoted ***Inv***):

$$Inv(X) = \begin{cases} X^{-1} & \text{in } GF(2^n) \text{ if } X \neq 0 \\ 0 & \text{otherwise} \end{cases}$$



axalto

Now:

Let's try to **whiten** the blackened reputation of ***Inv***, the black sheep for some Algebraic attackers and Not Quite Linear cryptanalysts…





## Whitening Ciphers

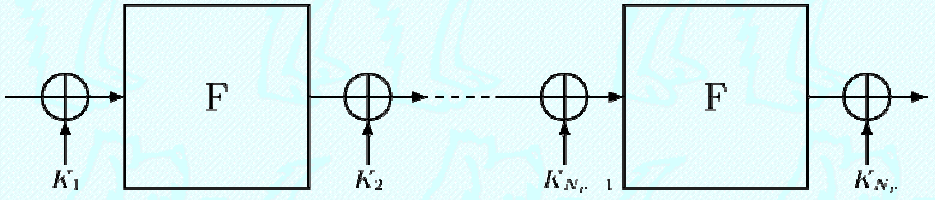


**Fig. 1.** Whitening Ciphers with identical round function $F$

E.g. Rijndael = AES, Serpent, …

# Let's Whiten Inv:

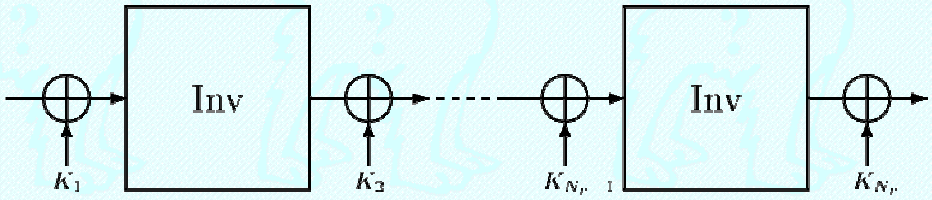


**Fig. 1.** Whitening the Inverse S-box

This F has good diffusion, high non-linearity etc… Satisfies all classical design criteria on block ciphers.



axalto



# Is it Secure ?

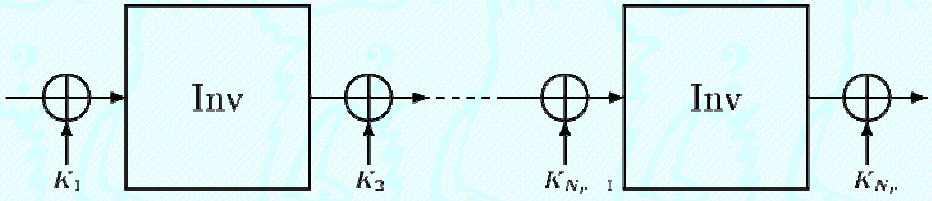


**Fig. 1.** Whitening the Inverse S-box

Theorem: [Courtois 2004, AES'4, Springer proceedings version]

This cipher is provably secure without any assumption.



axalto

# Proof:

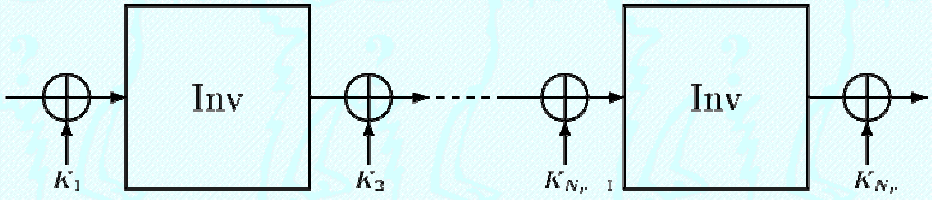


**Fig. 1.** Whitening the Inverse S-box

Theorem: [Courtois AES'4 proceedings]

Combining Inv and XOR with different round keys does generate the group of all permutations.





# Many Rounds Needed

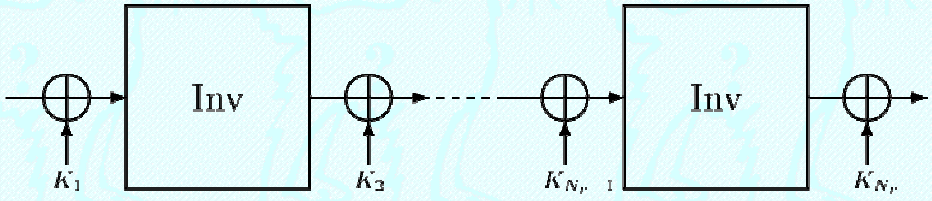


**Fig. 1.** Whitening the Inverse S-box

Information-theoretic argument:
allows the cipher to be secure after at least $\log(2^n!)/n \approx 2^n$ rounds !

My proof [AES'4 LNCS proc.]:
at most $45 \star 2^n$ rounds will do !

OK

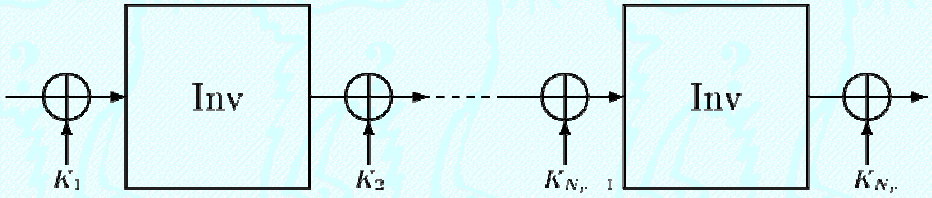


**Fig. 1.** Whitening the Inverse S-box

Let's use indeed $45 \star 2^n$ rounds.

Is it secure ?

White lie.

Remains terribly weak !





## Homographic Functions

(a.k.a. linear fractional transformations):

$$Y = \frac{\alpha X + \beta}{\gamma X + \delta}$$

They form a group under composition !

# Jakobsen-Knudsen Attack:

[FSE'97 and Journal of Cryptology 14(3) 2001].

Claim: Whatever is the number of rounds, the whole cipher is expressed as: $$Y = \frac{X + \alpha}{\beta X + \gamma}$$

False as stated, true with good probability when $N_r$ small…
Extended /Corrected result [Courtois, AES'4]:

$$Y = \frac{\alpha X + \beta}{\gamma X + \delta}$$

with probability $$\geq \left(1 - \frac{1}{2^n}\right)^{N_r} \geq \left(1 - \frac{N_r}{2^n}\right)$$



axalto



# What we get:

A cipher such that:

- High non-linearity
- Satisfies all design criteria
- The security does not grow exponentially with the number of rounds.



axalto

# Some Paradox:

On average, for $45 * 2^n$ rounds our cipher is badly broken.

$$Y = \frac{\alpha X + \beta}{\gamma X + \delta}$$

with probability $\geq \left(1 - \frac{1}{2^n}\right)^{N_r} \approx e^{-45}$

Constant-time algebraic attack:

Guess 3 correct cases and solve 3 linear equations.

(constant number of field operations, which is polynomial)





# The "Whitening Paradox"

Same cipher, same number of rounds:

- When round keys are random (average case)
  - Homographic approximation with constant prob.
  - Broken in O(1).
- For a special choice of keys (best case)
  - Provably secure without any assumption.

# "Group Size Paradox"

Related to:

What is the size of group generated by DES bla bla bla bla…..





# Subtle detail:

This function is homographic:

$$\overline{Inv}(X) = \begin{cases} X^{-1} & \text{if } X \notin \{0, \infty\} \\ 0 \mapsto \infty \\ \infty \mapsto 0 \end{cases}$$

This one (though mostly the same) isn't :

$$Inv(X) = \begin{cases} X^{-1} \text{ in } GF(2^n) & \text{if } X \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

Reason why the probability decreases with the number of rounds.

## They are Almost the Same, yet:

- Group generated by $\overline{Inv}$ and XOR with key bytes - small, few homographic transformations.
- Group generated by $Inv$ and XOR with key bytes – very very large… All permutations !





## Application to DES:

- Knowing that DES is not a group can be an illusion.
- Assume that for example DES encryption functions are equal with probability $2^{-10}$ to elements that form some group.

This would break triple DES !

# Conclusion

A good provable construction is better than an astronomical amount of random whitening, that can still leave a pitch black security hole open.



axalto