Distinguisher for Full Final Round of Fugue-256

Jean-Philippe Aumasson and Raphael C.-W. Phan

Fugue-256: round transform **R**

30×32 = 960-bit state

32-bit message blocks integrated through **R** transform

R makes 2 AES-like rounds on 4-word windows

Trivial distinguishers. . . (a block affects 11 state words)

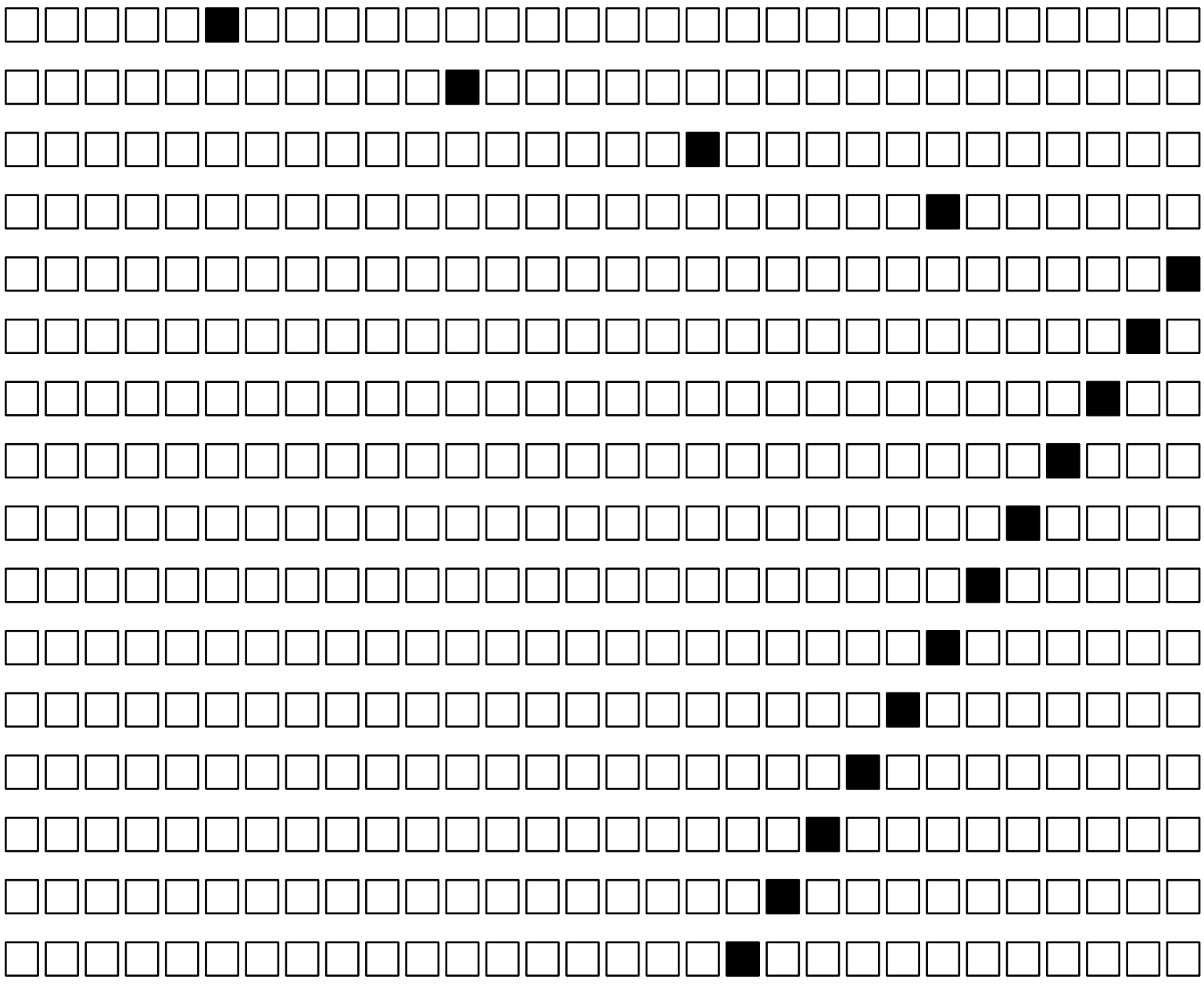
Fugue-256: finalization **G**

Message-independent permutation+truncation, 18 double-AES-like rounds

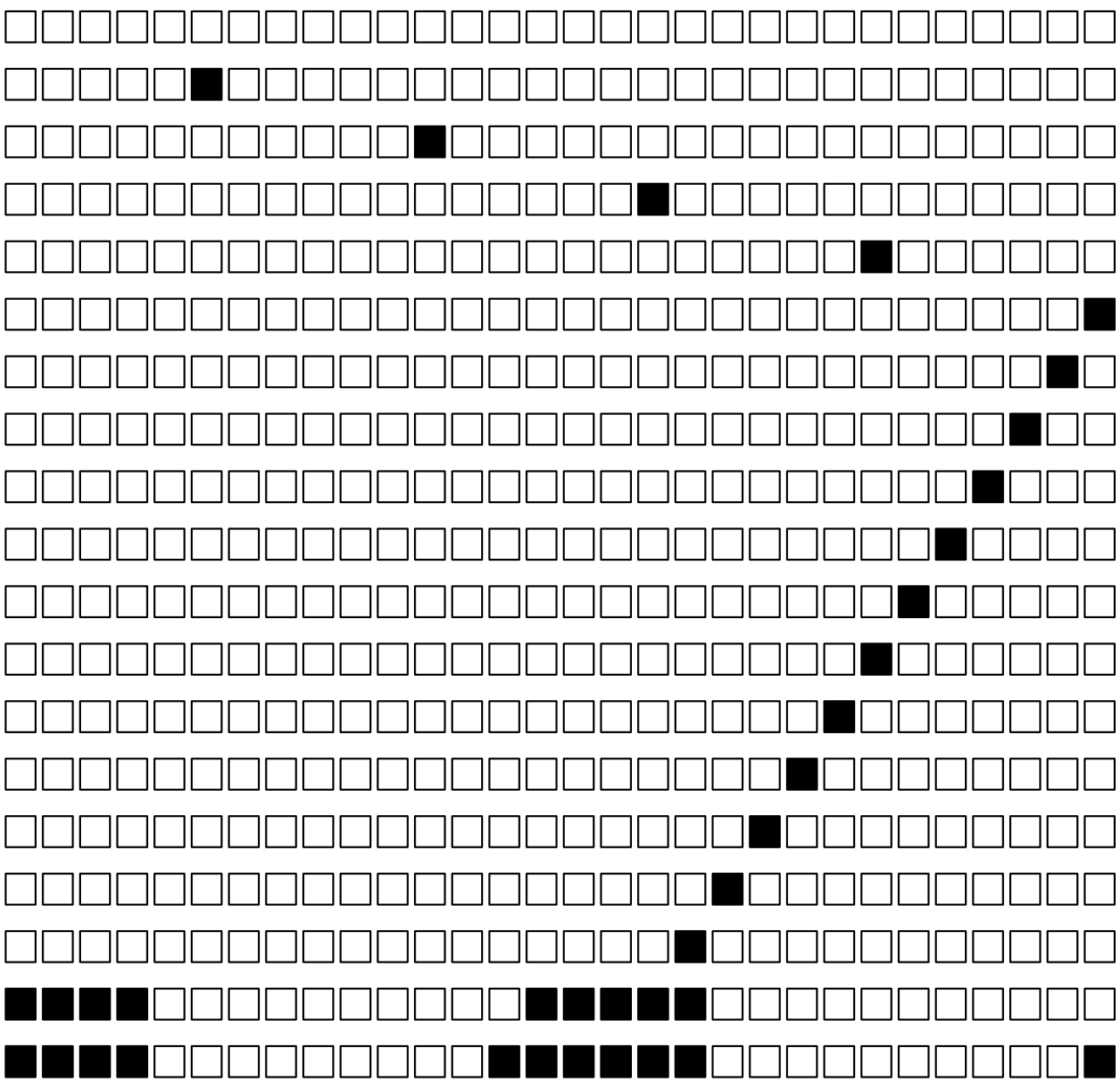
Since **R** is by definition weak, **G** should provide pseudorandomness, unpredictability, etc.

But. . .

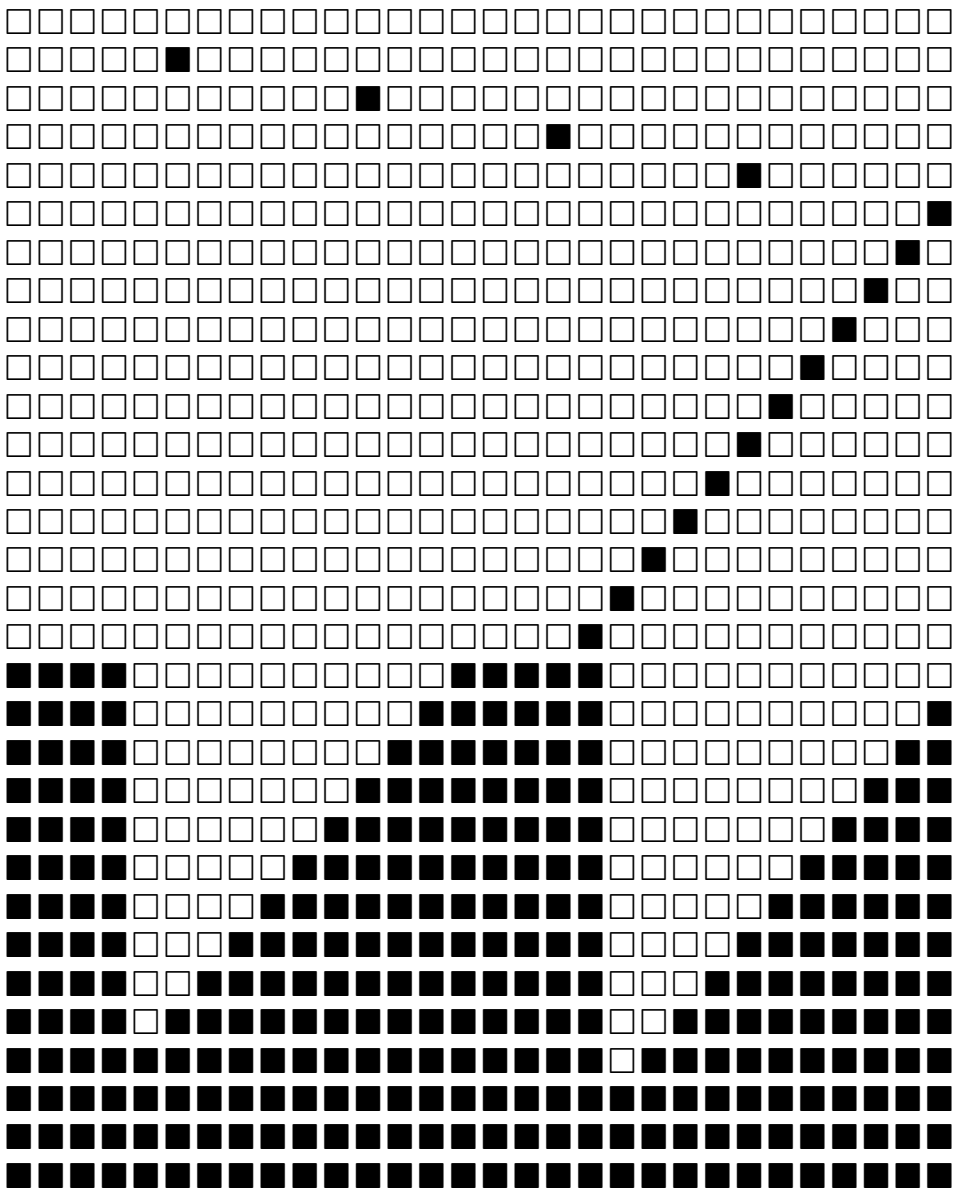
Prob.-1 characteristic for 15 rounds of **G**



Exploit it for a prob.-1 distinguisher on full 18-round **G**. . .



And even augmented-round **G** (up to 30 rounds)



Conclusions

Efficient distinguisher for **G** (and more), though not Fugue-256

Cannot make the assumption that **G** behaves ideally to show Fugue-256's RO behavior