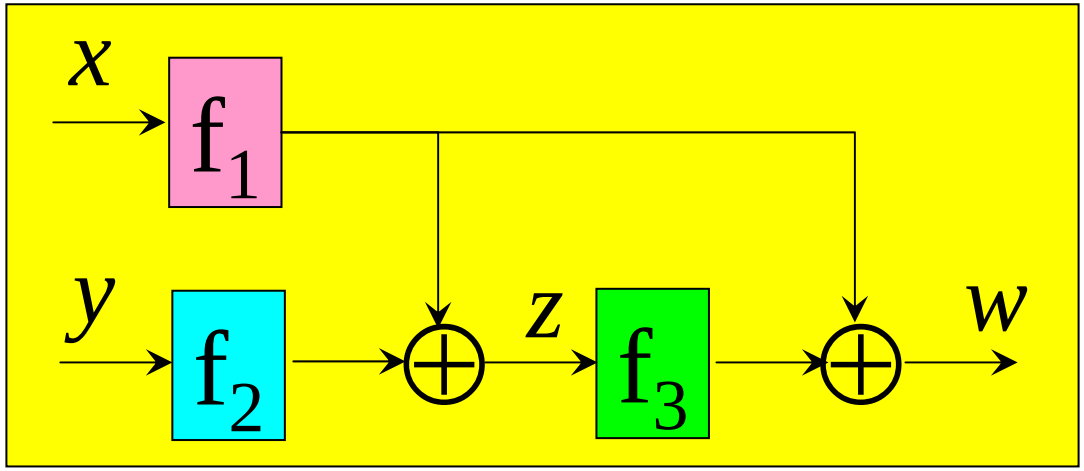


Message Authentication Codes from Unpredictable Block Ciphers

Yevgeniy Dodis (NYU)

joint work with

John Steinberger (University of British Columbia)

MACs from Block Ciphers

- Question: building efficient variable-length MAC from a block cipher f
- Easy if model f as *pseudorandom*
  - E.g., CBC-MAC, hash-then-PRF, …
- Do we need *pseudorandomness* to argue *unpredictability*?
  - Theory: No. MACs $\Leftrightarrow$ PRFs $\Leftrightarrow$ OWFs
  - Practice: ???. All "practical" approaches fail
- Question': build a (variable-length) MAC from an unpredictable block cipher?

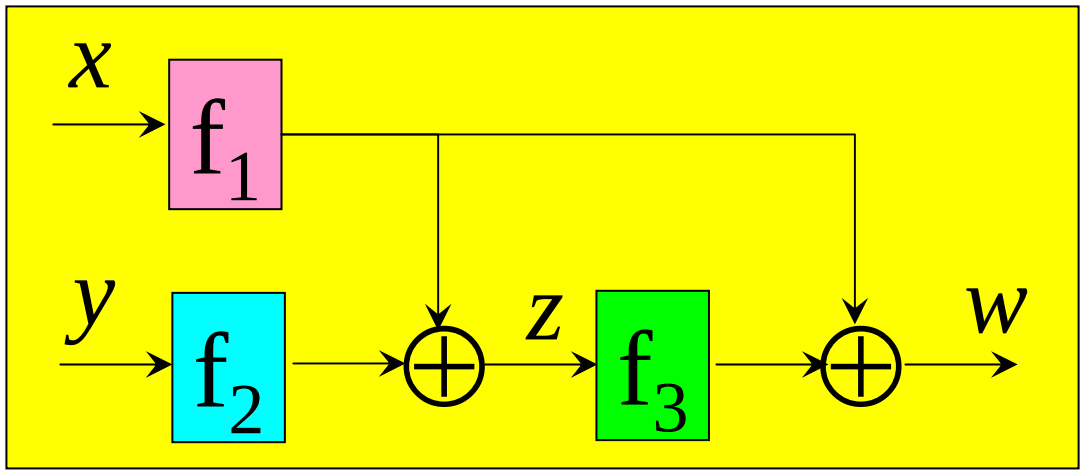
Why Bother?

- Assuming unpredictability seems safer
- Want to make minimal assumptions
- "Fallback mode":
  - if AES good PRP $\Rightarrow$ full PRF, but …
  - if its PRF security is much weaker than its MAC security $\Rightarrow$ still get excellent MAC
- All prior solutions insecure/impractical
  - CBC, HMAC, hash-then-PRF, CRHF, Feistel, …
- Surprisingly non-trivial technical question

Our Solution

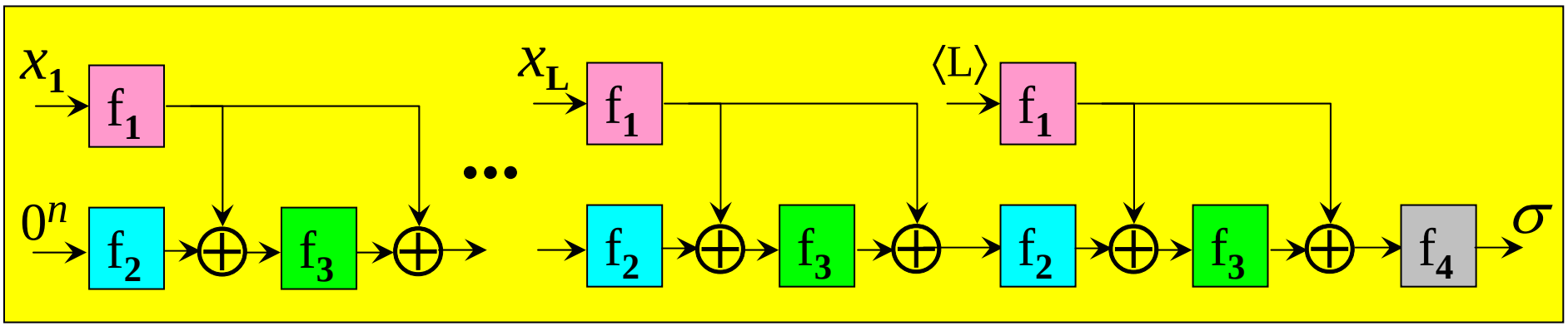
- Use Shrimpton-Stam compression function

$F(x, y)$:



$= w$

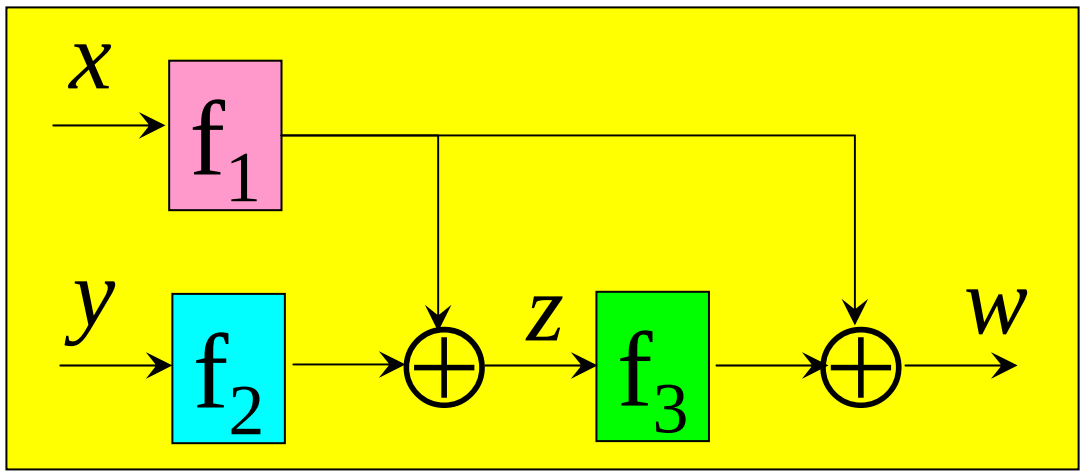
- Gives the following rate-3, 4-key VIL-MAC



Our Solution

- Use Shrimpton-Stam compression function

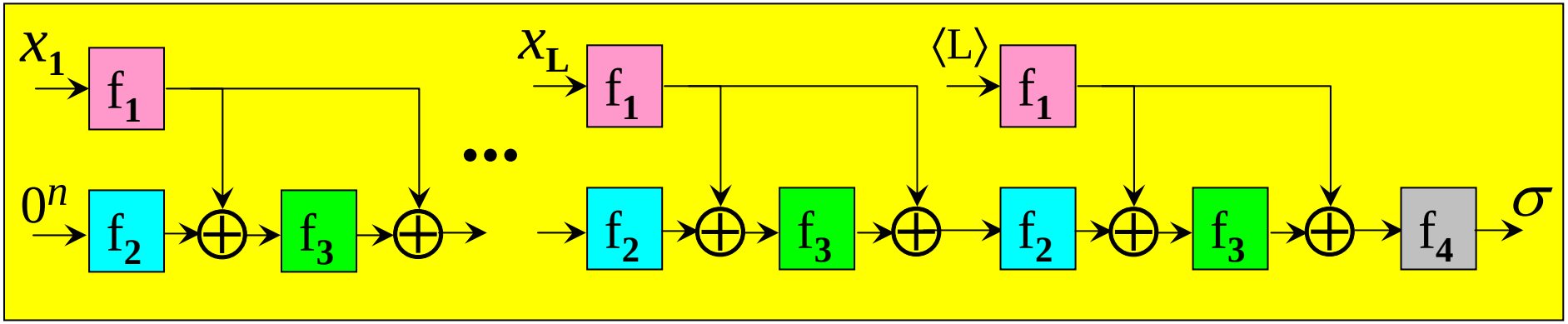
$F(x, y)$:



$= w$

- <u>Main theorem</u>: if block ciphers f_1, f_2, f_3 are (q, ε)-unpredictable, then $F(x, y)$ above is $(q, O(\varepsilon\, q^2 (\log q)^2))$-weakly collision-resistant
  - (nearly) matches "birthday" security
  - implies final VIL-MAC with same security

PRF Preservation



- **Theorem**: If f_1, f_2, f_3, f_4 are (q, ε)-PRFs $\Rightarrow$ get (q', ε')-VIL-PRF with birthday security:

$$q' \sim q,\ \varepsilon' \sim 4\varepsilon + O(q^2/2^n)$$

- Unlike CBC and related modes, still secure PRF in "leaky block-cipher" model:

$$q' \sim q,\ \varepsilon' \sim 4\varepsilon + O(q^2 (\log q)^2 / 2^n)$$

Summary

- First practical MAC from a block cipher which is only assumed to be a short MAC
  - Rate 3, birthday security, PRF-preserving
- Nice interplay between theory & practice
- Question: Should this replace CBC-MAC?
  - How big is the "real" gap between unpredictability and pseudorandomness for actual block ciphers used (e.g., AES)?