ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

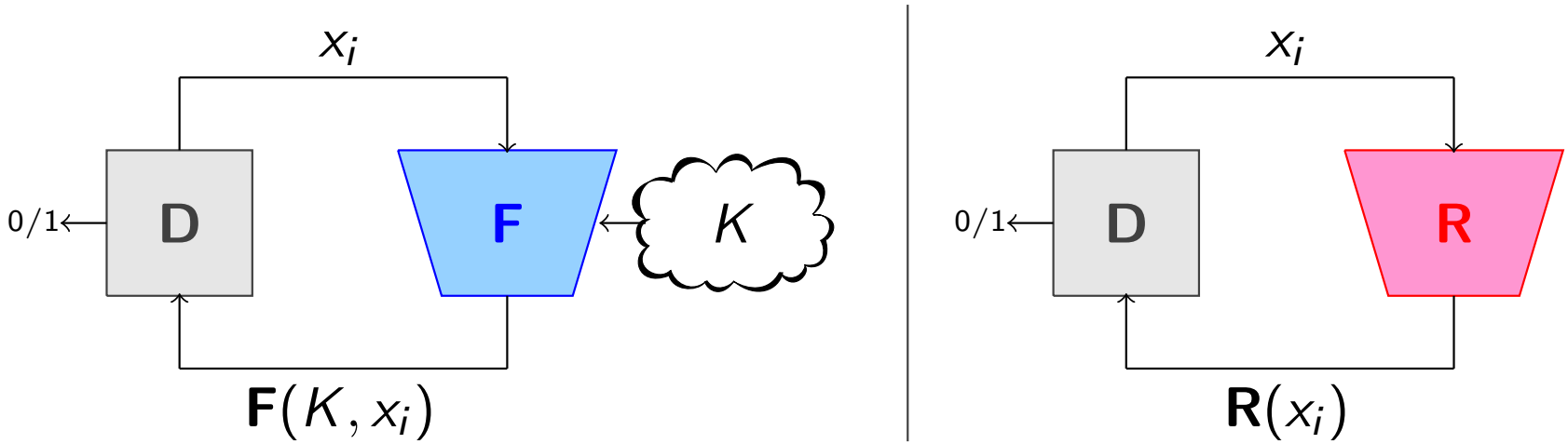
Efficient PRFs from Very Weak Assumptions

Ueli Maurer and Stefano Tessaro

Department of Computer Science
ETH Zurich

CRYPTO 2008
Rump Session

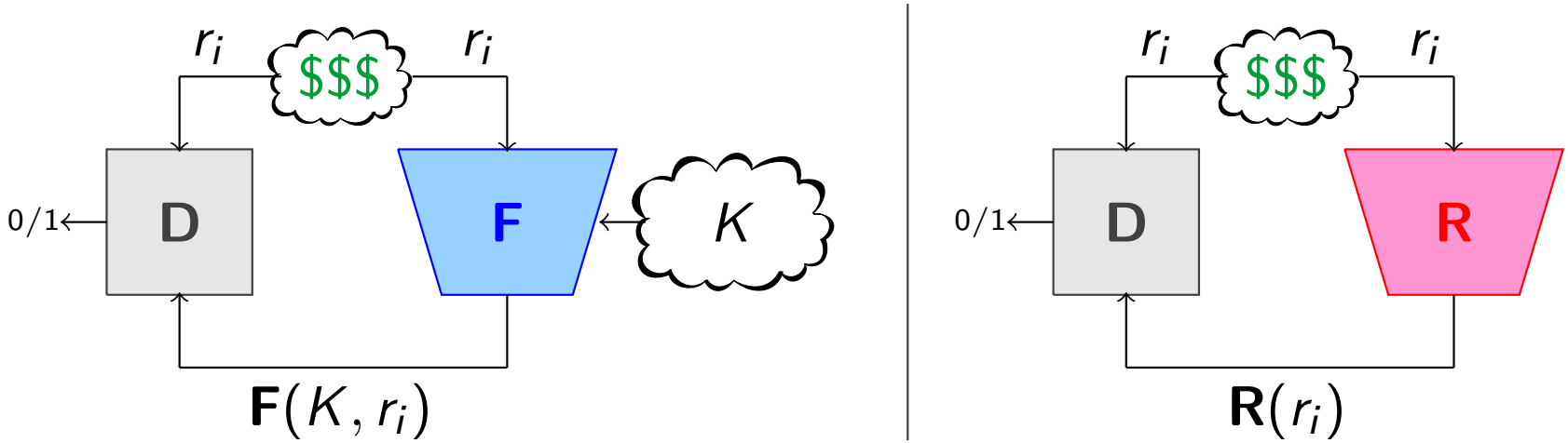
Chosen-Input Attack



$\forall$ efficient distinguishers **D**

$$|\Pr[\mathbf{D} \text{ outputs 1 left}] - \Pr[\mathbf{D} \text{ outputs 1 right}]| = \text{negligible}$$

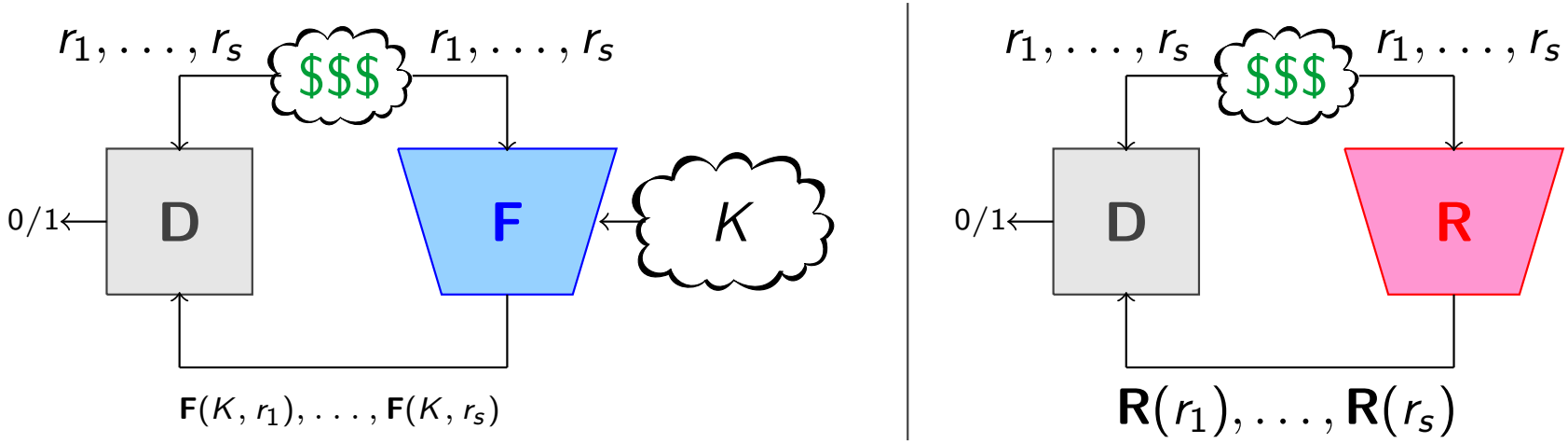
Random-Input Attack



$\forall$ efficient distinguishers **D**

$$|\Pr[\mathbf{D} \text{ outputs 1 left}] - \Pr[\mathbf{D} \text{ outputs 1 right}]| = \text{negligible}$$

s-Random-Inputs Attack

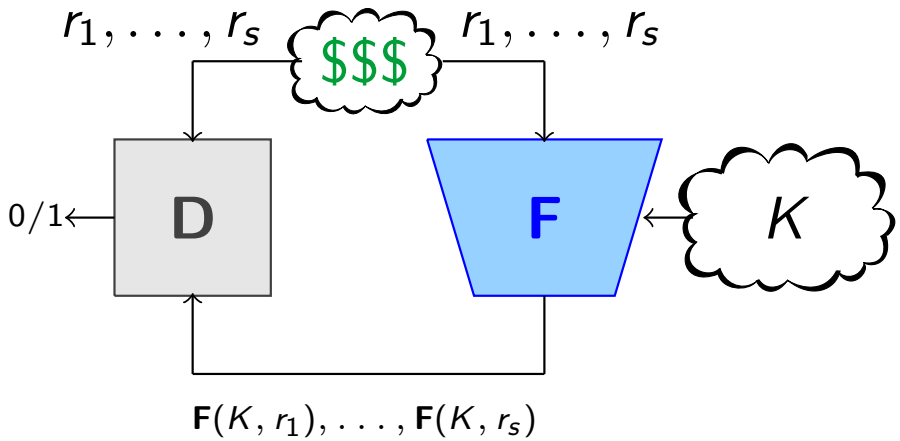


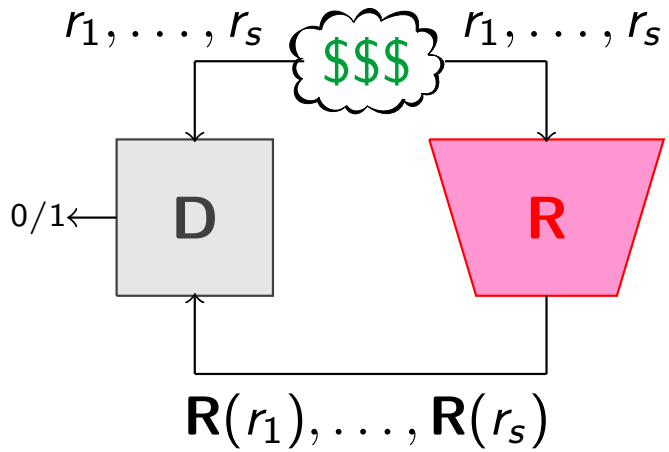
$\forall$ efficient distinguishers **D**

$$|\Pr[\mathbf{D} \text{ outputs 1 left}] - \Pr[\mathbf{D} \text{ outputs 1 right}]| = \text{negligible}$$

s-Random-Inputs Attack

This paper!



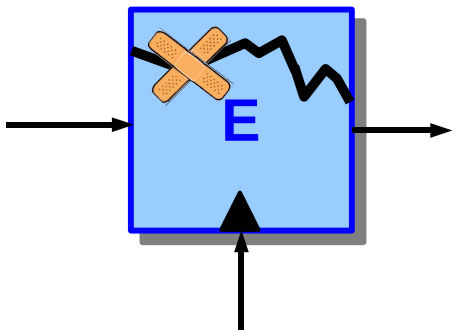


$\forall$ efficient distinguishers **D**

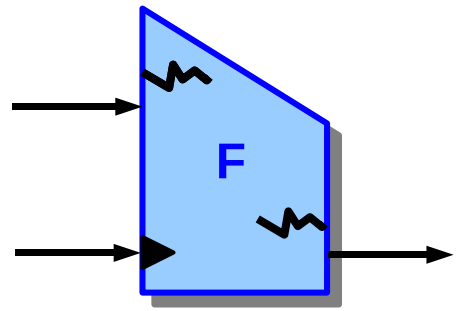
$$|\Pr[\mathbf{D} \text{ outputs 1 left}] - \Pr[\mathbf{D} \text{ outputs 1 right}]| = \text{negligible}$$

s-WPRF is a very weak assumption!

- Weak Block-Cipher



- Compression Function

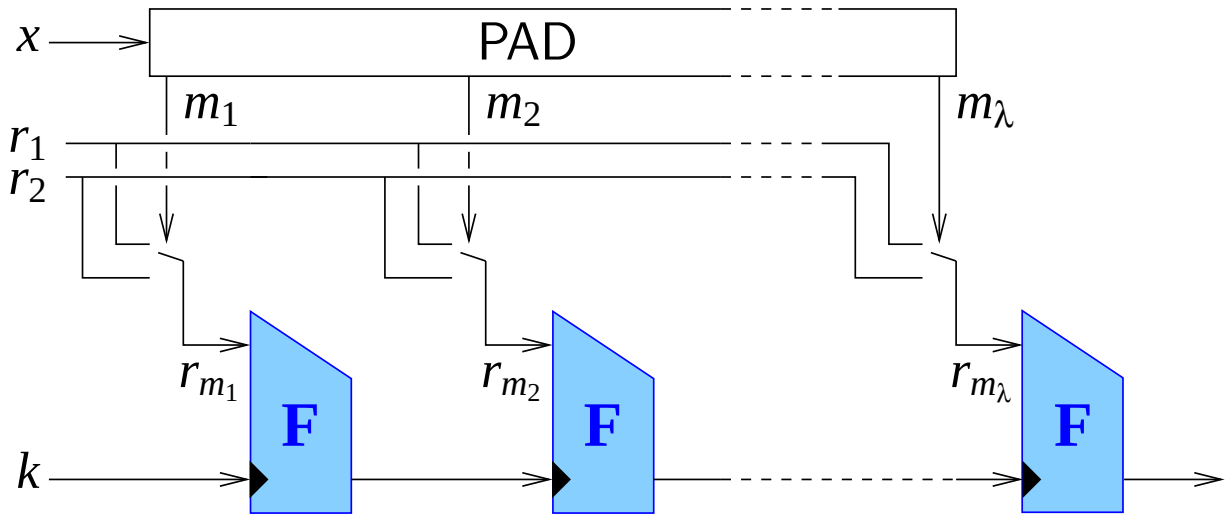


Question

Can we efficiently construct PRFs / MACs from s-WPRFs?

First Construction

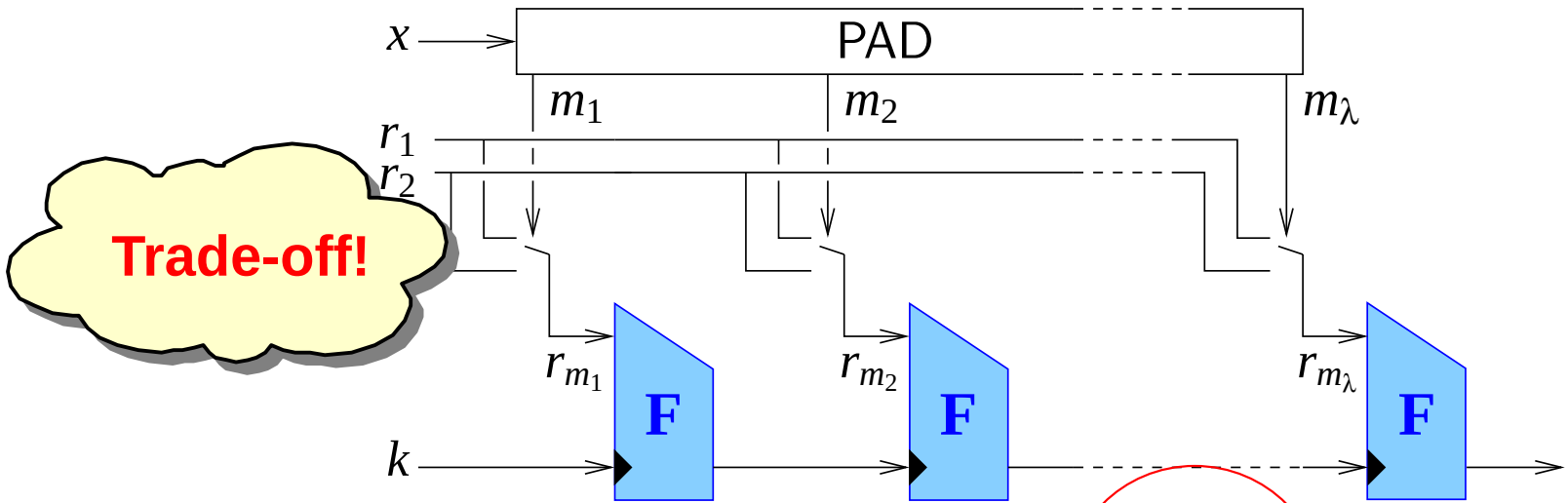
- Relies on 2-WPRF $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^\kappa$
- Key material: κ bits (private part) + $2n$ bits (public part)



- # F-calls for processing input x: $\approx |x|$

First Construction

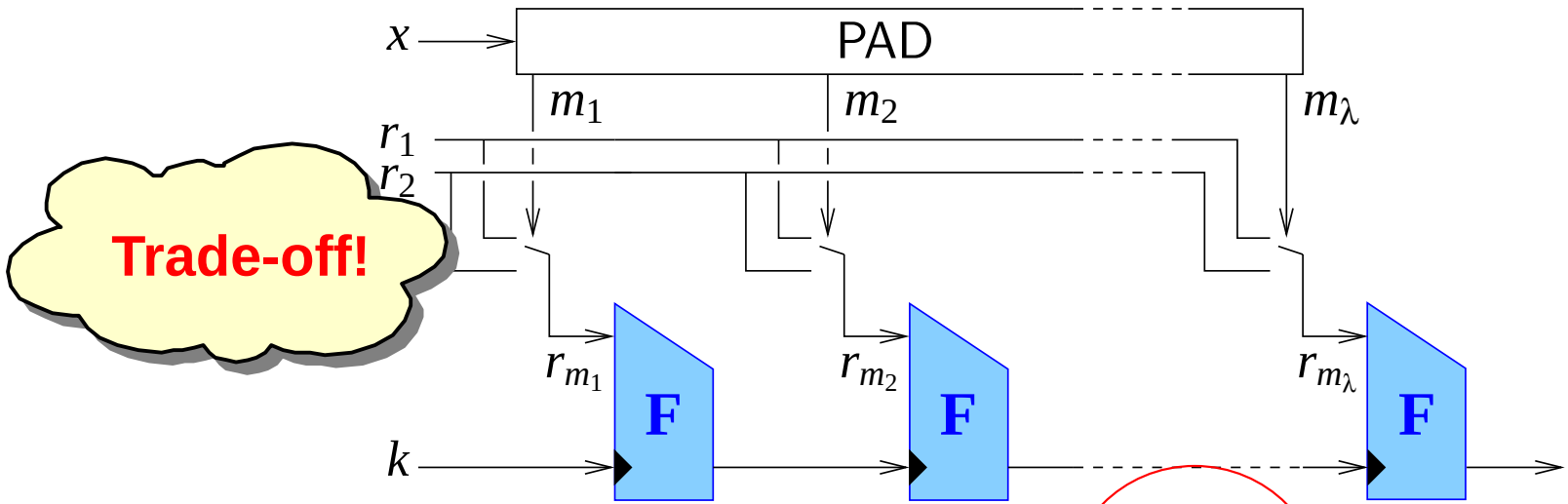
- Relies on s-WPRF $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^\kappa$
- Key material: κ bits (private part) + sn bits (public part)



- # F-calls for processing input x: $\approx |x| / \log s$

First Construction

- Relies on s-WPRF $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^\kappa$
- Key material: κ bits (private part) + sn bits (public part)



- # F-calls for processing input x: $\approx |x| / \log s$

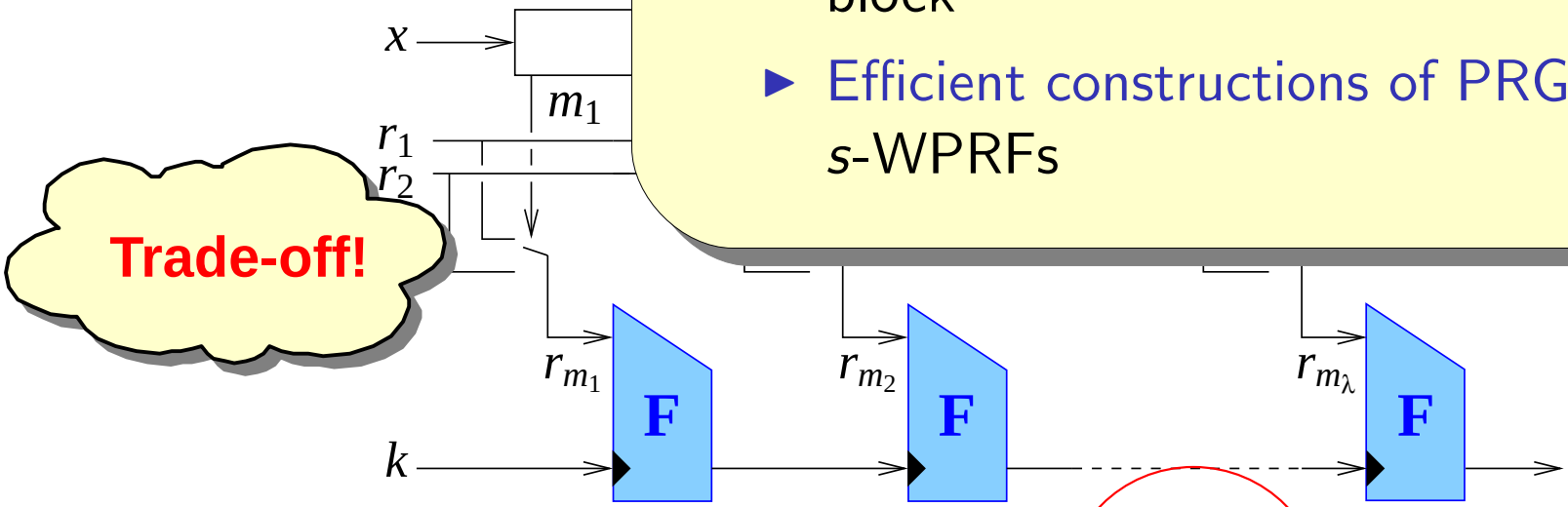
Same as best construction of PRF from WPRF

First Construction

- Relies on s-WPRF
- Key material: κ b

Corollaries:

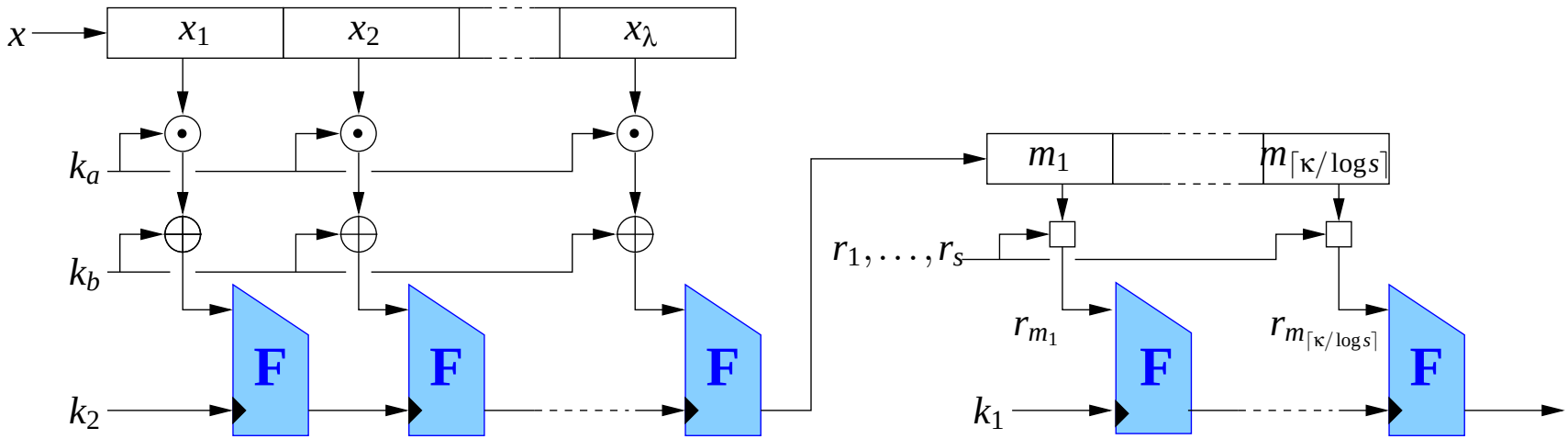
- s-WPRF-based counter-mode encryption: $1 + \frac{1}{s-1}$ calls / encrypted block
- Efficient constructions of PRGs from s-WPRFs



- # F-calls for processing input x: $\approx |x| / \log s$

Same as best construction of PRF from WPRF

Improved Construction – Long Messages

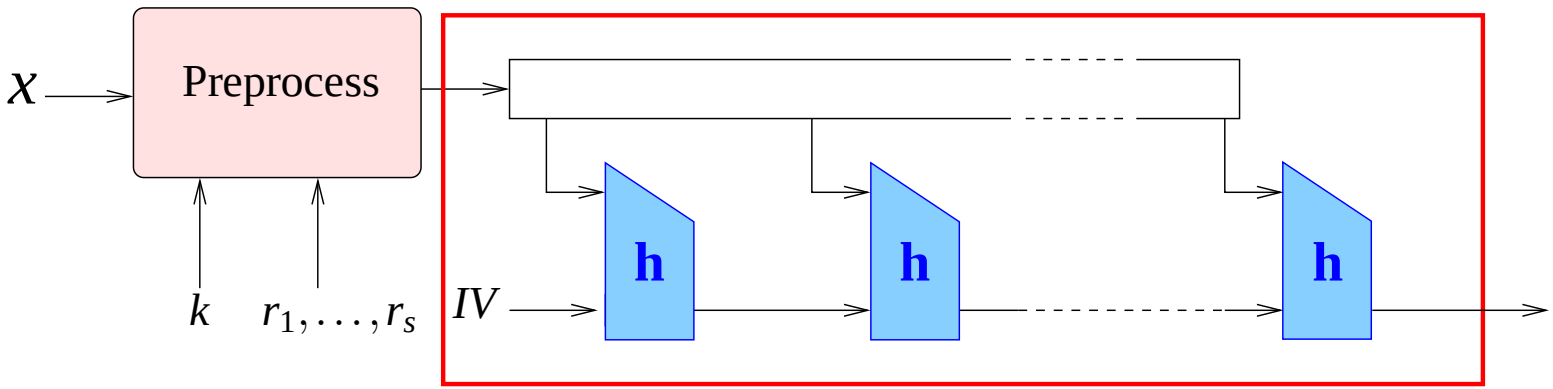


Improves # F-calls for long messages to $|x|/n + \kappa/\log s$

Hash Functions

Constructions can be obtained with black-box access to iterated hash functions (similar to HMAC) provided

- compression function **h** is s-WPRF (key = chaining value)
- compression function **h** is sufficiently regular



$\Rightarrow$ Key-based message preprocessing

Paper

Ueli Maurer and Stefano Tessaro

"Basing PRFs on Constant-Query Weak PRFs: Minimizing Assumptions in Iterated MACs"

ASIACRYPT '08