Double-Length Hash Functions with Birthday PRO Security in the Ideal Cipher Model

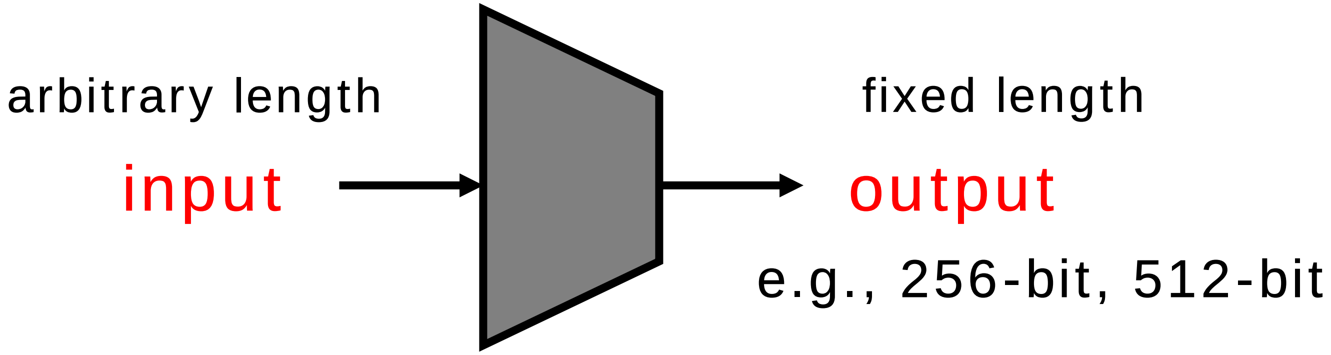
Yusuke Naito

Mitsubishi Electric Corporation

This talk was presented at SAC 2011

Hash Function

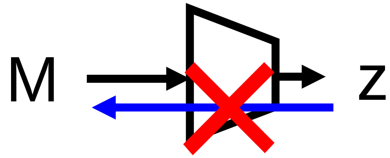
- Hash function: $\{0,1\}^* \rightarrow \{0,1\}^n$.



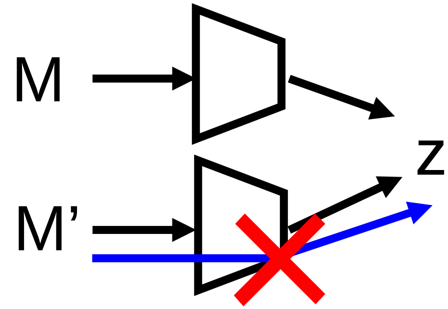
- Hash functions are used as
  - Random Oracle instantiation
  - HMAC
  - Pseudorandom Function
  - ...

Hash Security

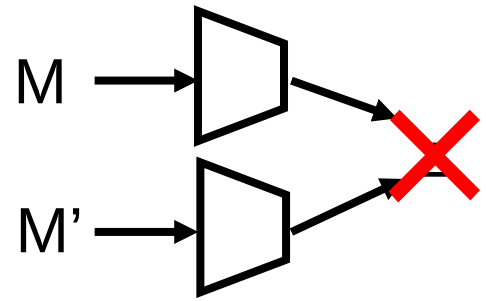
- **Preimage Resistance**
  given z, hard to find M s.t. z=H(M)



- **Second Preimage Resistance**
  given M, hard to find M'
  s.t. H(M)=H(M') and M≠M'



- **Collision Resistance**
  hard to find M, M'
  s.t. H(M)=H(M') and M≠M'

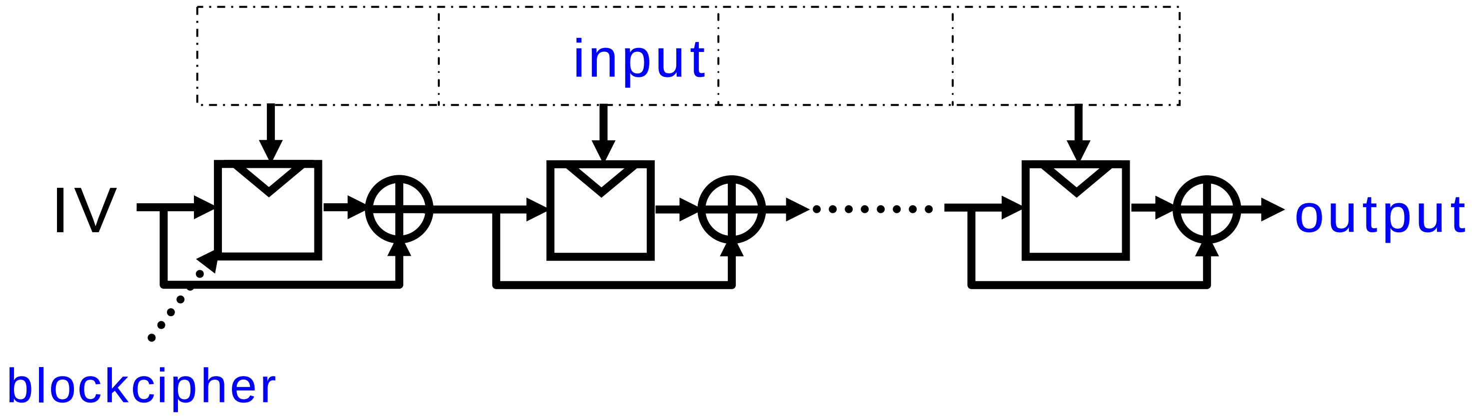


- **Pseudorandom Oracle (indiff. from RO):** Our Goal
  Stronger property than CR, SPR and PR

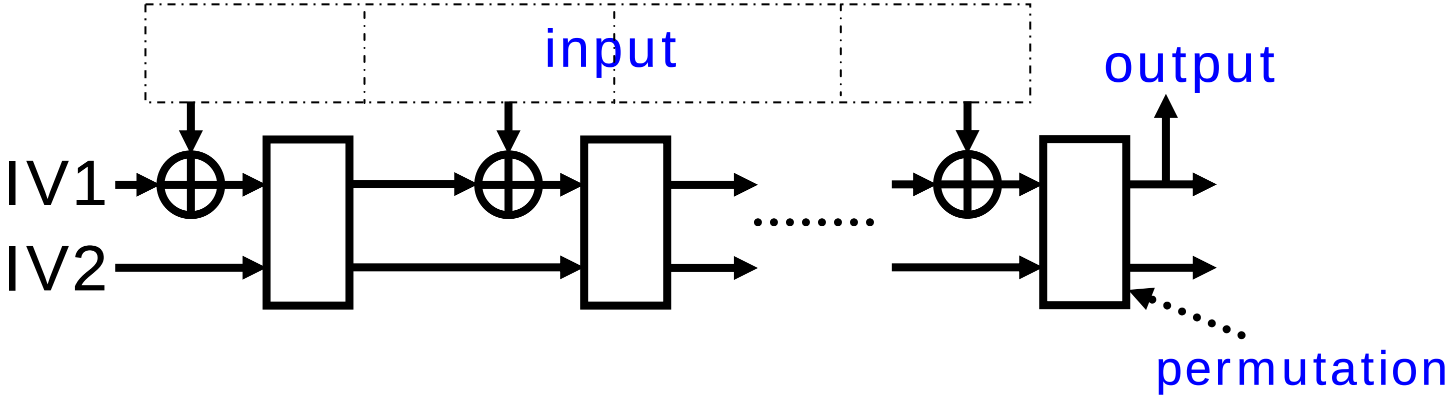
Hash Function Design

Blockcipher-based hash and Permutation-based hash

Davies-Meyer Merkle-Damgard



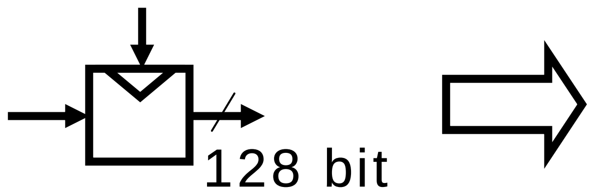
Sponge



Blockcipher-based Double-Length Hash Function (DLHF)

- DLHF is constructed from an existing blockcipher (e.g., AES)
- The output length of blockciphers is too short.

e.g., AES (output length: 128 bit)



A collision of 128 bit hash is found with 2^{64} complexity

- DLHFs are designed so that the output length is twice of that of the blockcipher.

e.g., AES-based hash: the output length is 256 bit

Blockcipher-based Double-Length Hash Function (DLHF)

- Hirose's scheme, Tandem-DM, Abreast-DM, MJH, MDC-2, ...

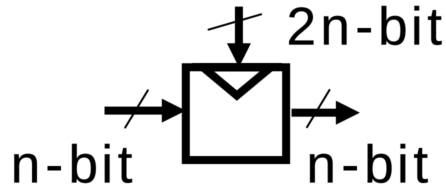
- DLHFs are useful on size restricted devices (e.g., RFID, IC card) when implementing both a hash function and a blockcipher.
  - one has only to implement the blockcipher.

- DLHFs are designed from a single blockcipher.

- The security is proven in the ideal cipher model.

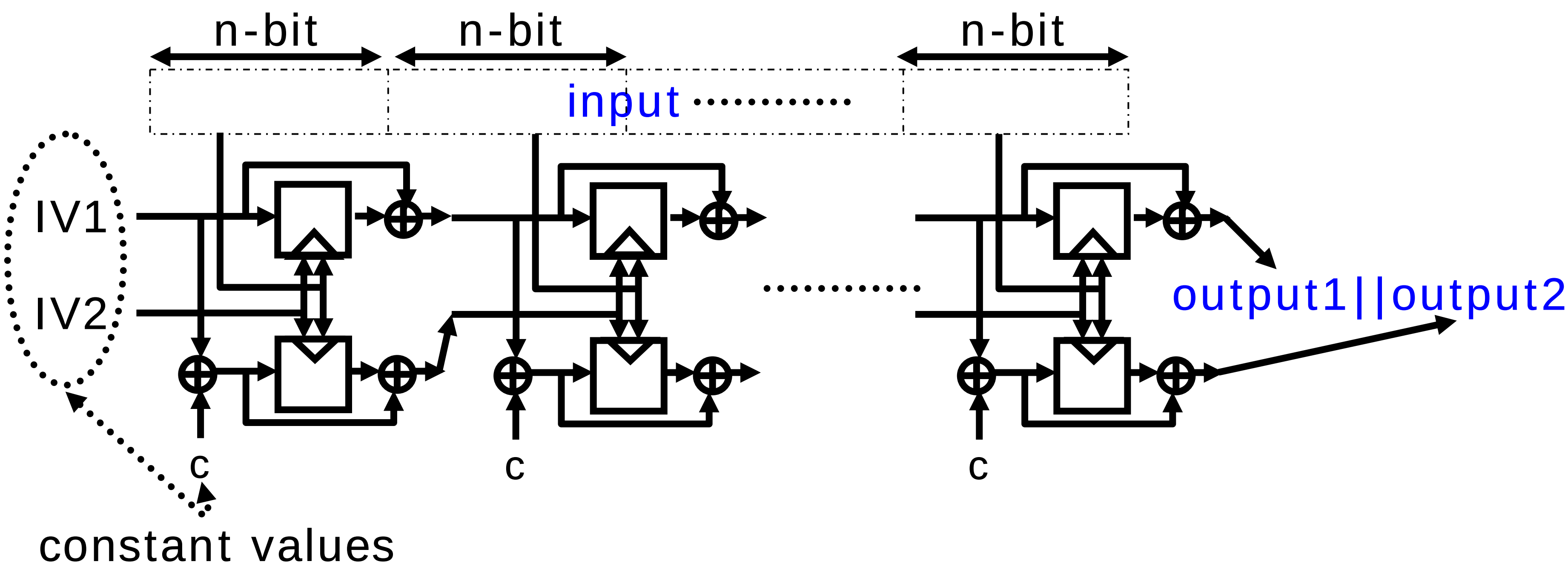
Example: Hirose's Hash

- Constructed from a single blockcipher.



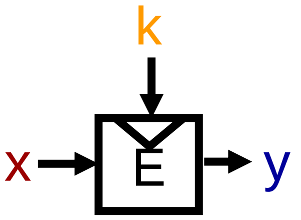
e.g., AES-256

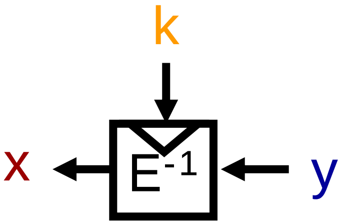
- The Davies-Meyer mode is used twice in one block.



Ideal Cipher Model

- An adversary (or distinguisher) can access to
  - (ideal) encryption oracle E
    - query: plain text x, key k
    - response: cipher text y
  - (ideal) decryption oracle E^{-1}
    - query: cipher text y, key k
    - response: plain text x

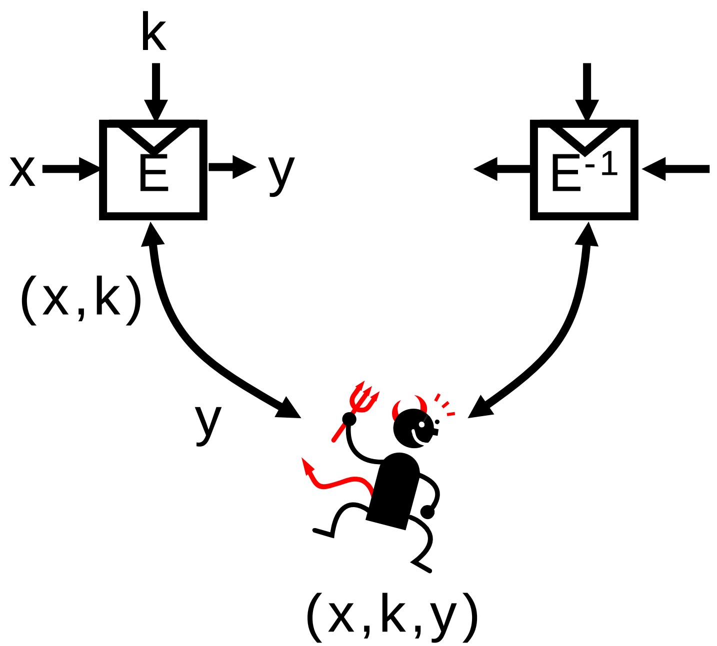




Ideal Cipher Model

forward procedure

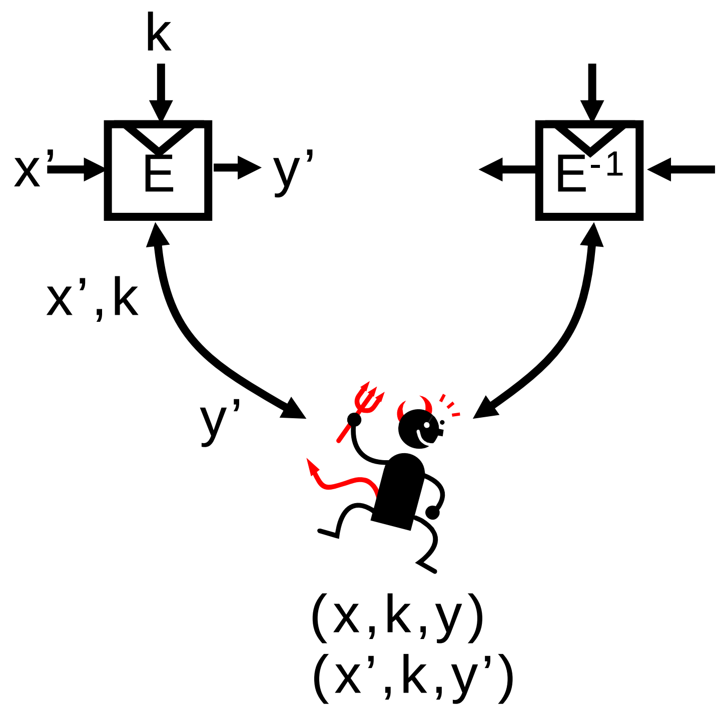
on query (x,k)
  $y \leftarrow_R \{0,1\}^n$
  Ret y



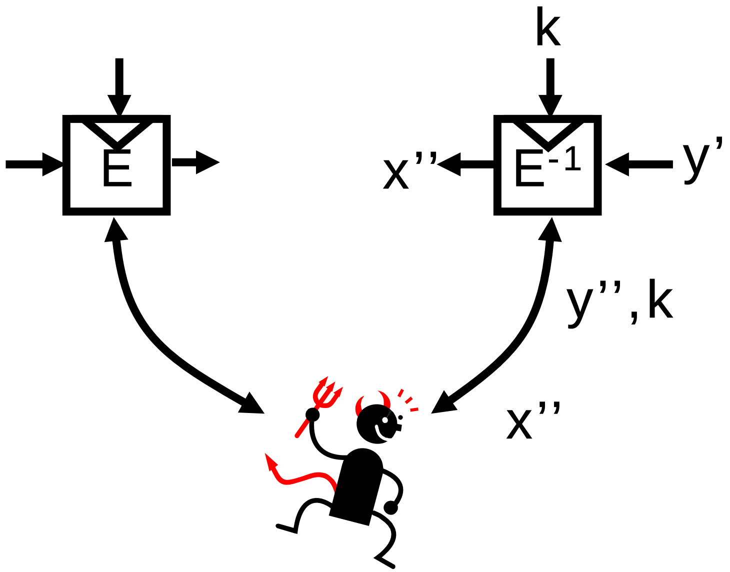
Ideal Cipher Model

forward procedure

on query (x,k)
  $y' \leftarrow_R \{0,1\}^n \setminus \{y\}$
  Ret y'



Ideal Cipher Model



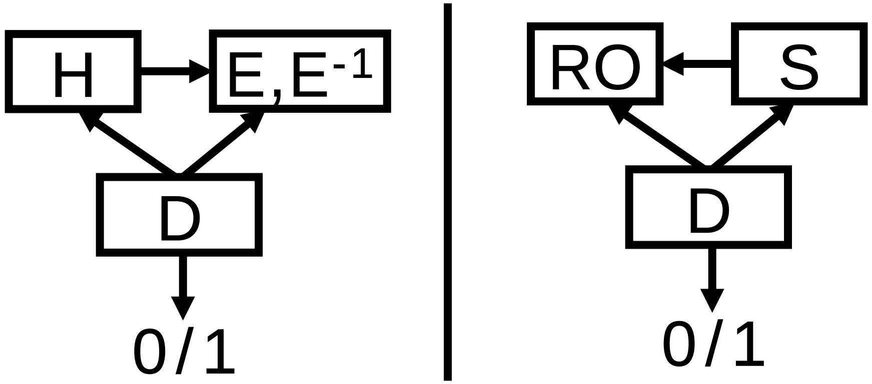
inverse procedure

on query (y'',k)
$x'' \leftarrow_R \{0,1\}^n \setminus \{x,x'\}$
Ret x''

(x,k,y)
(x',k,y')
(x'',k,y'')

Pseudorandom Oracle (PRO) or Indifferentiable from RO

H^E is PRO if ∃S s.t. ∀D: |Pr[D⇒1 (left)]-Pr[D⇒1 (right)]| ≦ ε
(ε is a negl. function for the security parameter)



- (Left) D can make queries to H, E and E^{-1}.
- (Right) D can make queries to RO and S.
- S simulates E,E^{-1} by using RO.

- PRO is the important security property
  - the security of many cryptosystems is preserved when RO is replaced with H^E (e.g., IND-CCA security, EUF-CMA security and many others)

Birthday Pseudorandom Oracle Security

- The PRO advantage |Pr[D⇒1 (left)]-Pr[D⇒1 (right)]| is bounded by the birthday bound.
  e.g.,
  When $H^E:\{0,1\}^*\text{->}\{0,1\}^{2n}$ and D can make q queries, the birthday bound is $O(q^2/2^{2n})$.

⇨ The query complexity to be differentiable from RO with probability of 1/2 is $O(2^n)$.

Previous Security Results
(Ideal Cipher Model)

	Collision Resistance	Pseudorandom Oracle (PRO)
Dedicated Hash	○	○ birthday security beyond birthday security
Double-Length Hash (from a single practical size blockcipher)	○	△ not achieve birthday security

Previous Results of Blockcipher-based DLHF

There is no double-length hash function constructed from a single practical size blockcipher and achieving birthday PRO-security

	Security		blockcipher		
	PRO	Collision Resistance	key size	output size	hash size
Hirose Tandem-DM Abreast-DM …	×	○	2n	n	2n
prefix-free Merkle-Damgård using PBGV	△ $O(2^{n/2})$	○	2n	n	2n

↑ The size is supported by AES-256

Our Result v.s. Previous Results

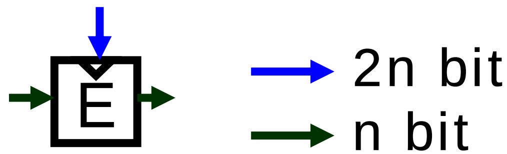
Our double-length hash functions can be constructed from a single practical size blockcipher and achieves the birthday PRO security!

	Security		blockcipher		
	PRO	Collision Resistance	key size	output size	hash size
Our Shemes	$O(2^n)$	○	2n	n	2n
Hirose Tandem-DM Abreast-DM ...	×	○	2n	n	2n
prefix-free Merkle-Damgård using PBGV	△ $O(2^{n/2})$	○	2n	n	2n

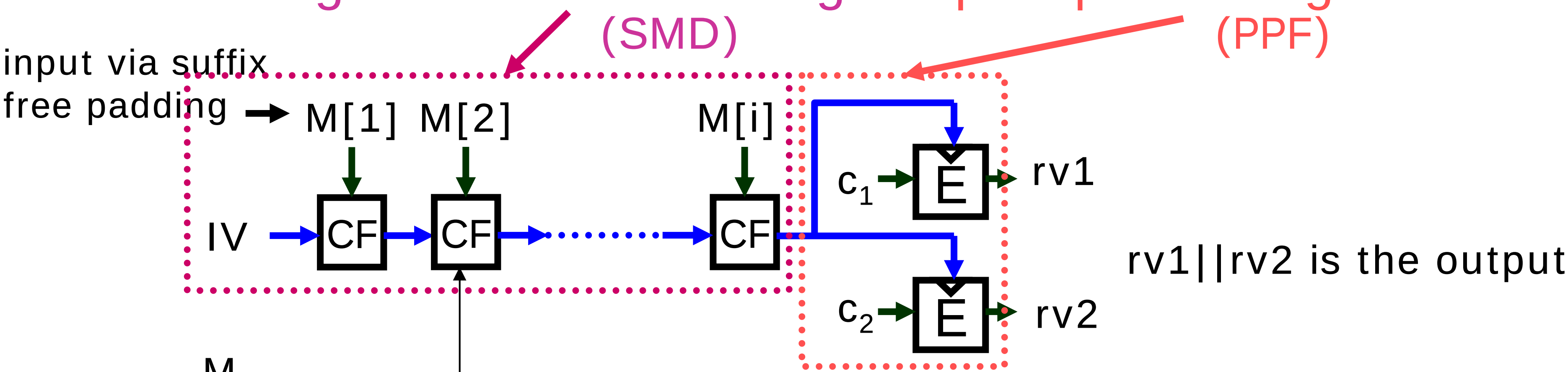
↑ The size is supported by AES-256

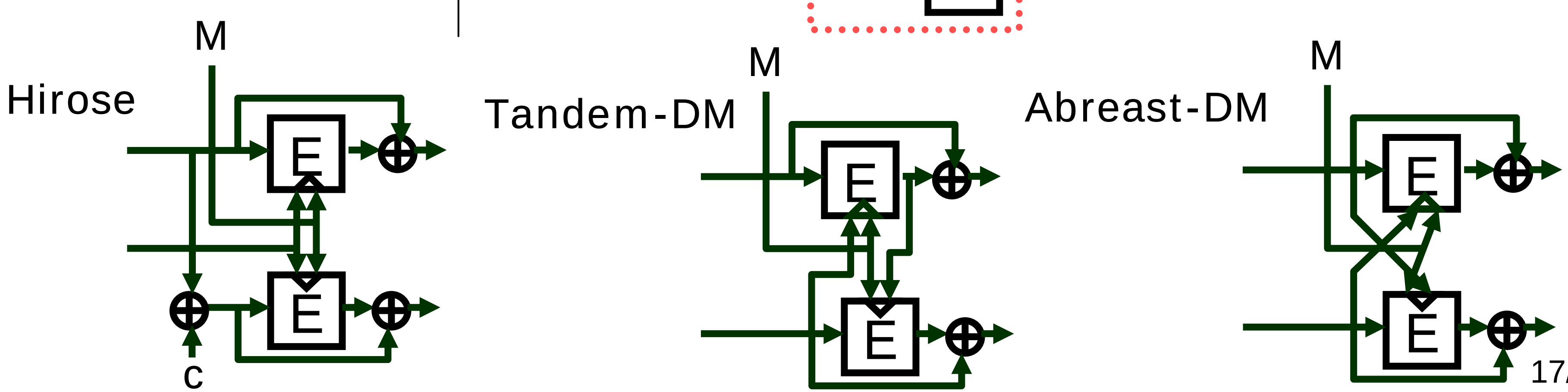
Our Double-Length Hash Functions

- Constructed from a single blockcipher such as AES-256

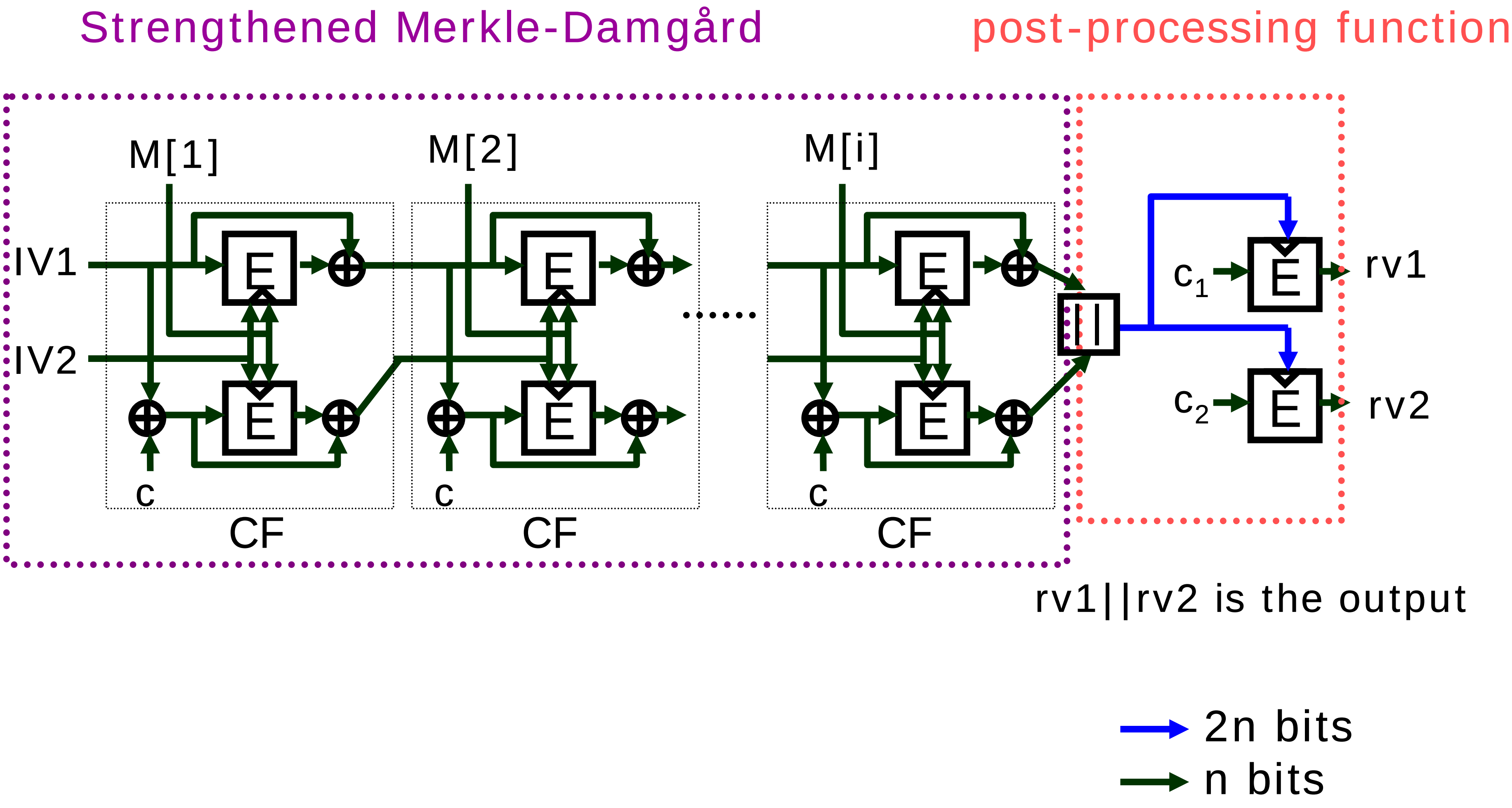


- Strengthened Merkle-Damgård+post-processing function





DLHF using Hirose's Scheme



Security Result

Theorem 3. There exists a simulator $S = (S_E, S_D)$ such that for any distinguisher $\mathcal{D}$ making at most (q_H, q_E, q_D) queries to three oracles, the PRO advantage is

$$\epsilon \leq \frac{2Q^2}{(2n-2Q)^2} + \frac{2Q}{2^n - 2Q} + \frac{4lqQ}{(2^n - Q)^2} + \frac{q_H + 2q}{2^n} + \frac{14Q}{2^n - Q}$$

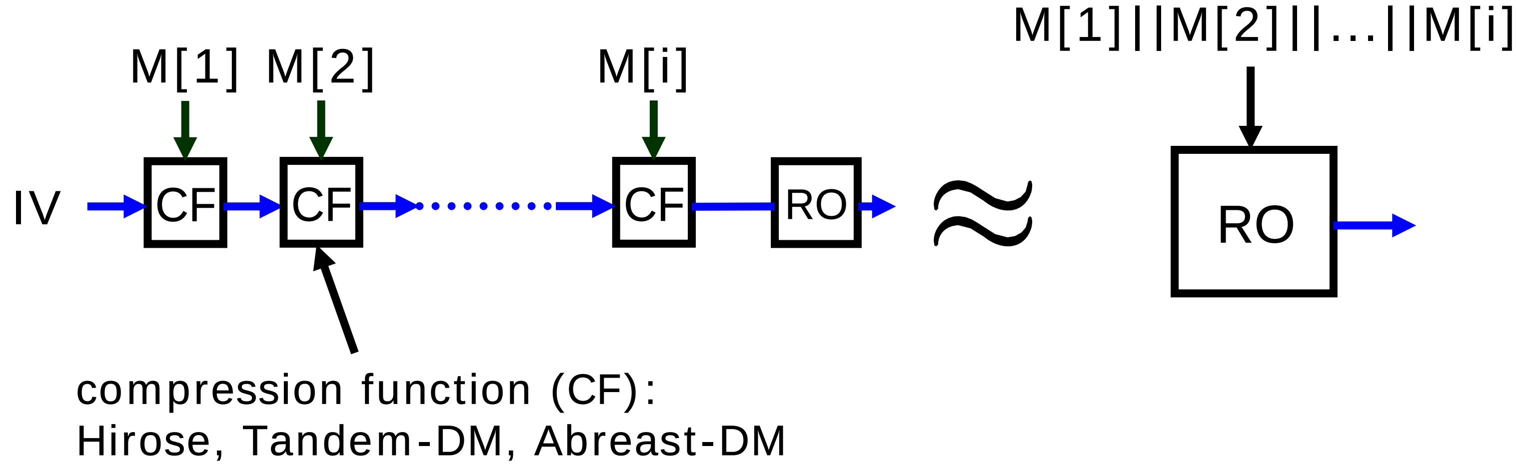
where S works in time $\mathcal{O}(q + 2lqQ + 2lq)$ and makes $2q$ queries to RO where $Q = 2l(q_H + 1) + q_E + q_D$ and $q = q_E + q_D$.

- The query complexity to be differentiable from RO with probability 1/2 is $O(2^n)$.

Our DLHFs achieve the birthday PRO-security!

Step 1

- Step 1:
  Compression functions of Hirose's scheme, Tandem-DM, and Abreast-DM are Preimage Aware (PrA)
  ⇒The following NMAC hash function is PRO



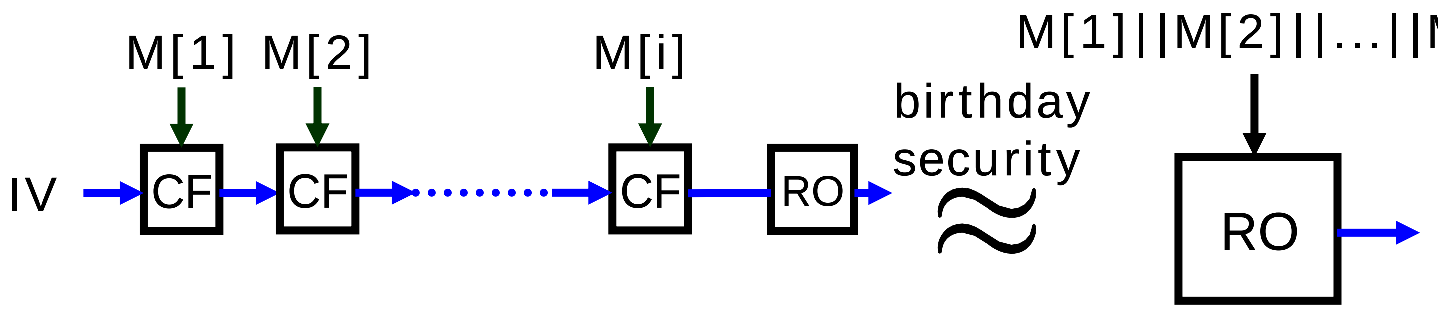
Step 1 (outline)

- The PrA security of Hirose, Tandem-DM, Abreast-DM= Collision Resistant (CR) + Preimage Resistant (PR)

birthday security ($O(2^n)$) beyond birthday security ($O(2^{2n})$)

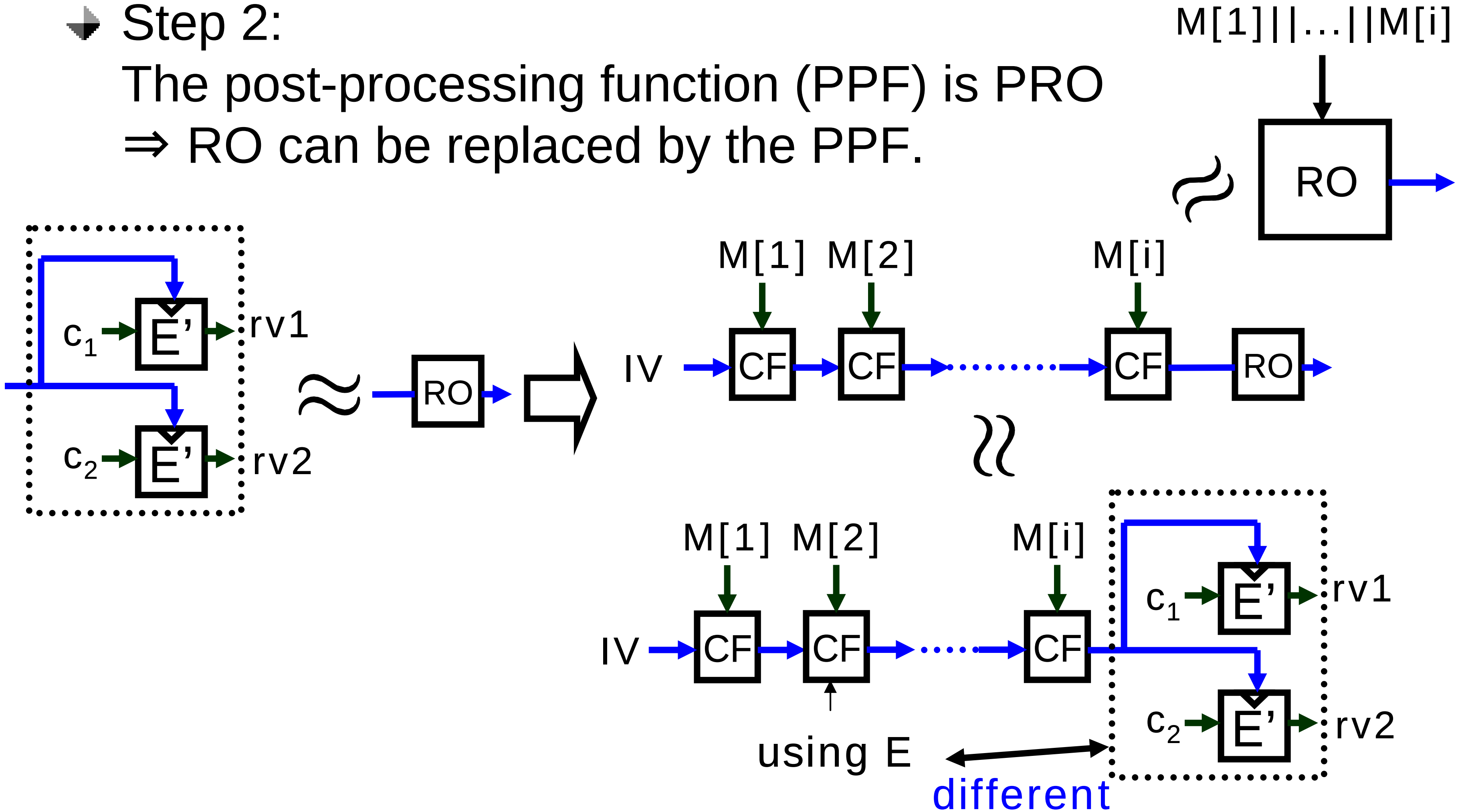
(Since the PrA notion is complex, the detail is skipped)

- The following NMAC hash functions satisfy birthday PRO security ($O(2^n)$)

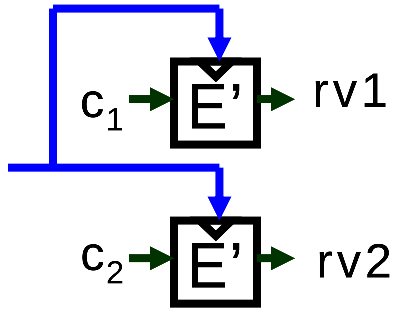


Step 2

- Step 2:
  The post-processing function (PPF) is PRO
  ⇒ RO can be replaced by the PPF.

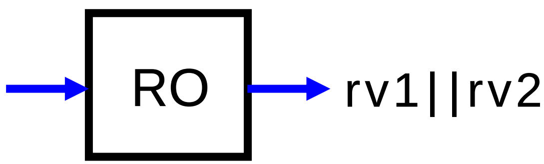


Step 2 (intuition)



rv1 is randomly chosen from $\{0,1\}^n$
rv2 is randomly chosen from $\{0,1\}^n \setminus \{rv1\}$

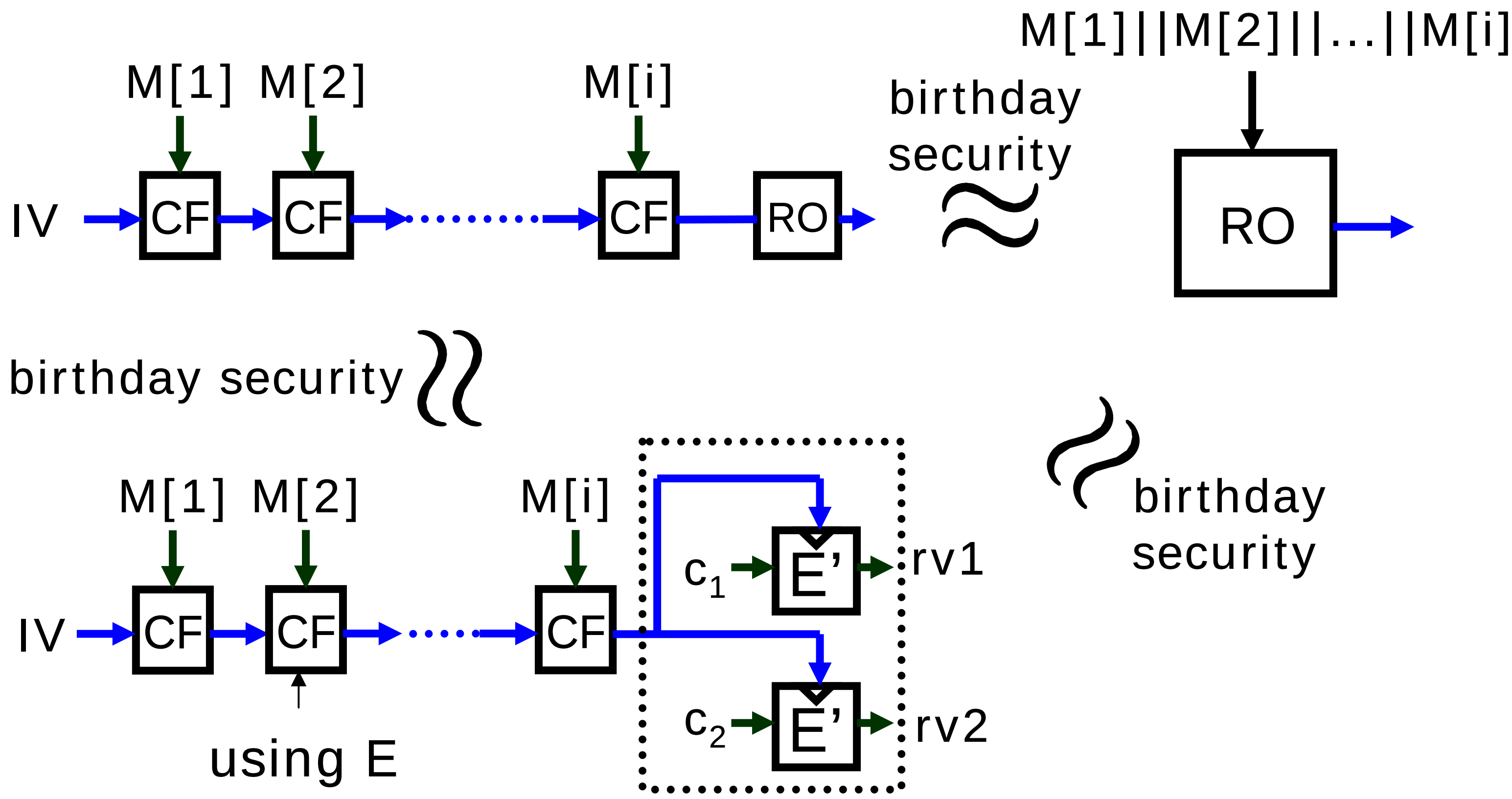
≈ birthday security



rv1 is randomly chosen from $\{0,1\}^n$
rv2 is randomly chosen from $\{0,1\}^n$

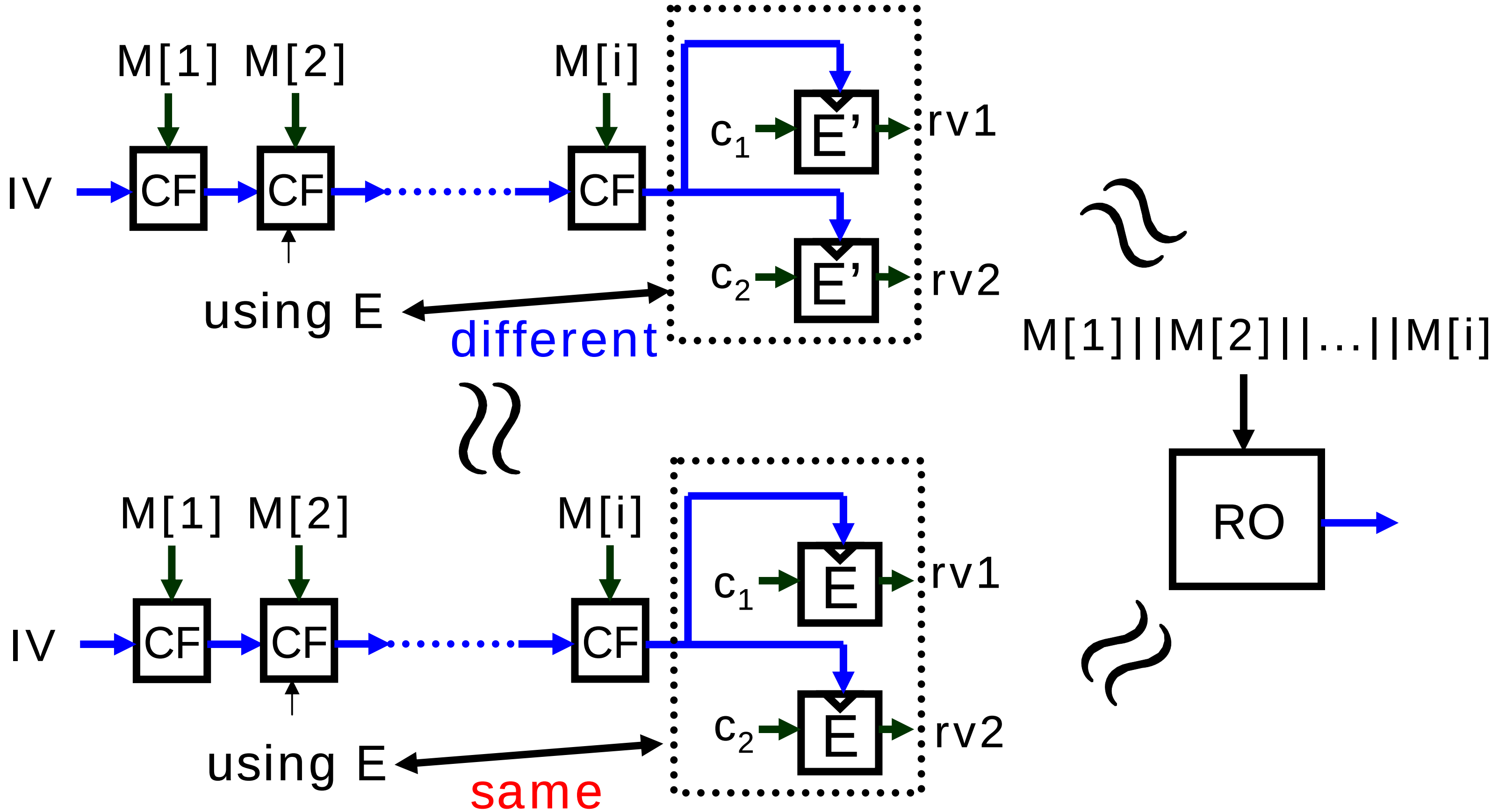
Since PPF: $rv1 \neq rv2$,
if RO: $rv1 \neq rv2$, then PPF is RO
$\Rightarrow$birthday PRO security ($O(2^n)$)

Result from Step 2

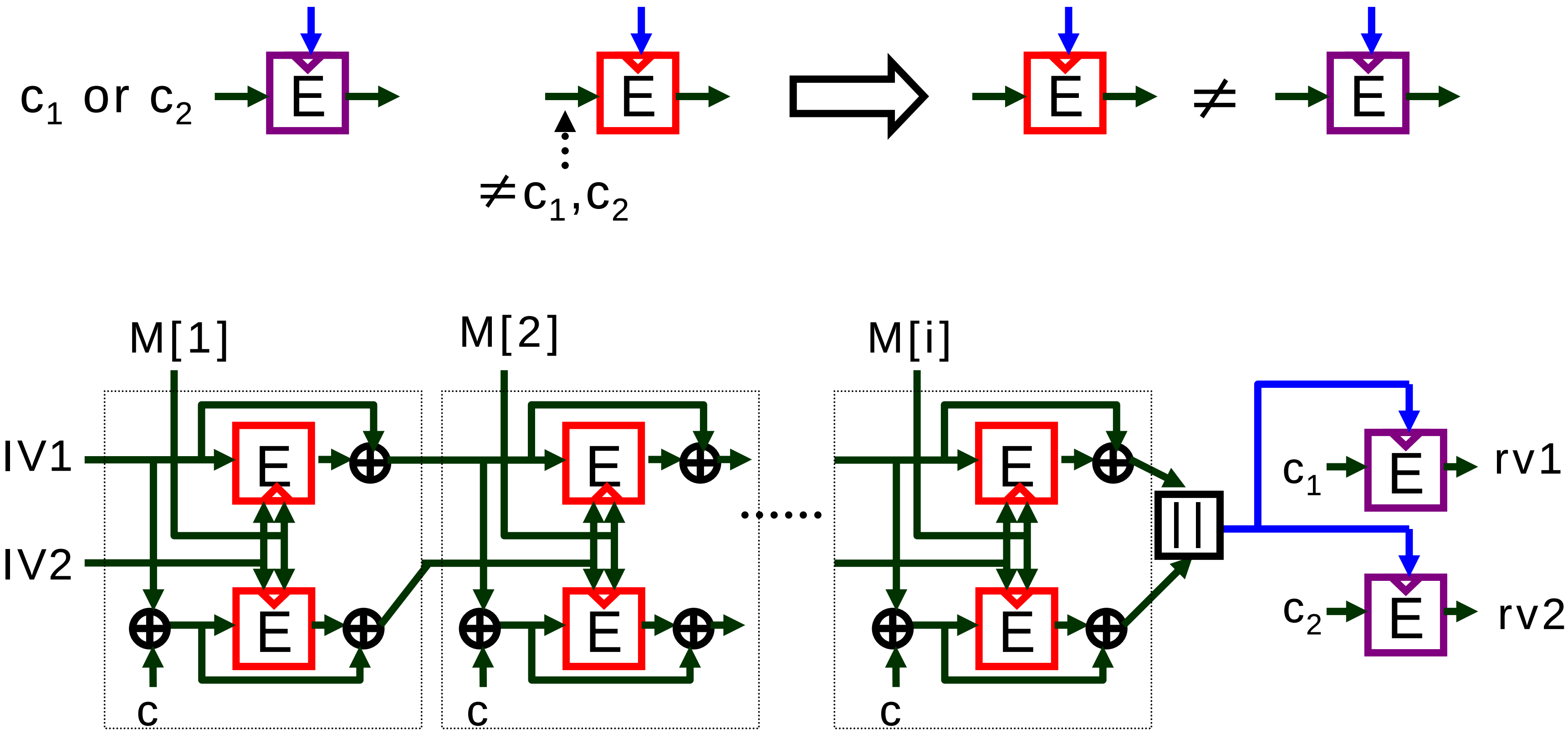


Step 3

- Step 3:
  The single-blockcipher based DLHF (our DLHF) is indifferentiable from two-blockcipher based DLHF

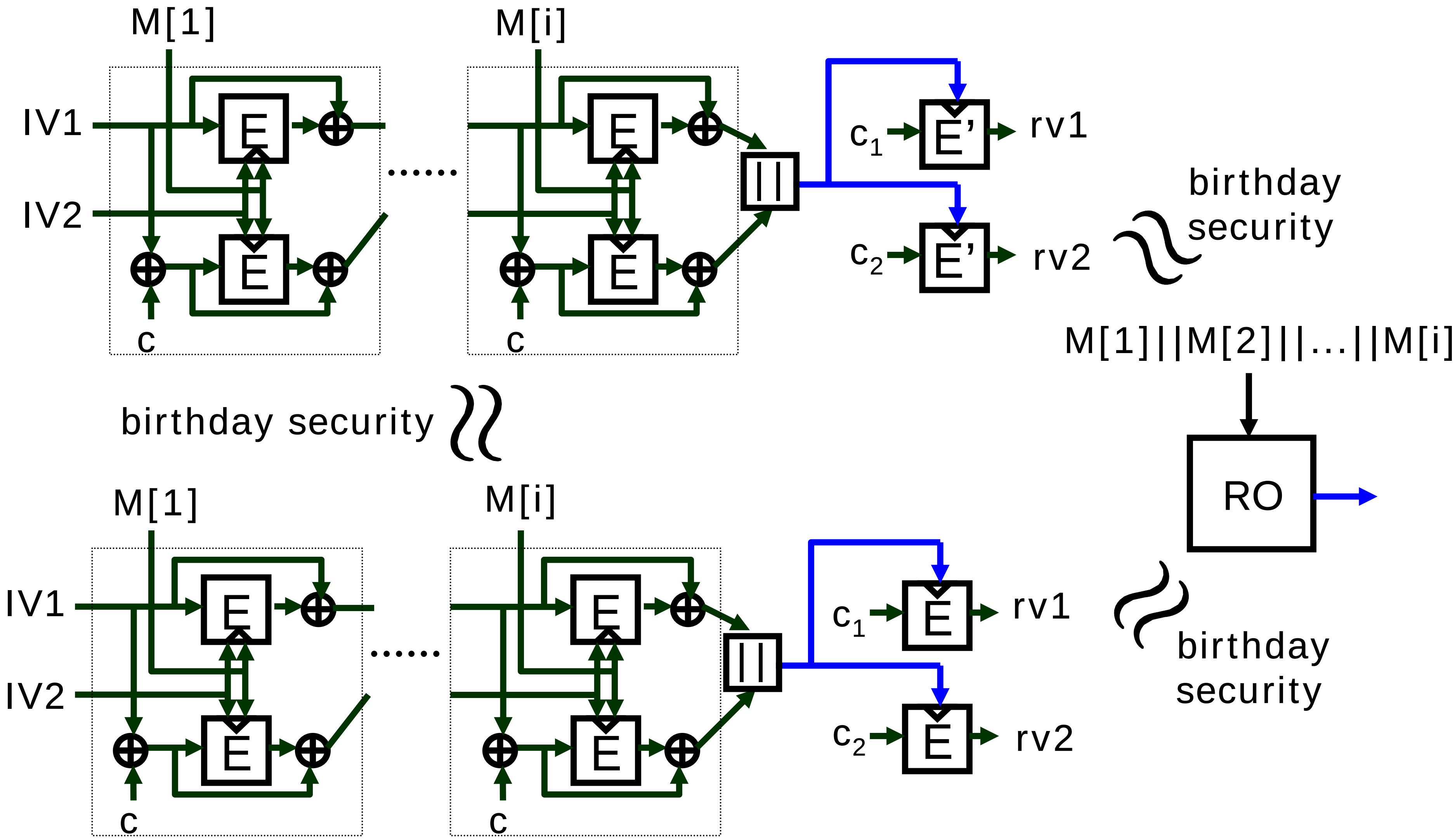


Step 3 (intuition)



Since the output of E is almost (n-bit) random,
the complexity that a random value is equal to c_1 or c_2 is $O(2^n)$

Result from Step 3



Conclusion

- First time DLHFs
  - achieve birthday PRO security
  - constructed from a single practical size blockcipher such as AES-256

Thank you for your attention!