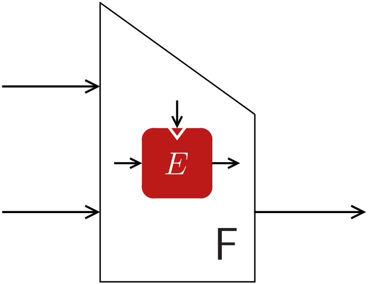
Hash Functions Based on Three Permutations: A Generic Security Analysis

Bart Mennink and Bart Preneel
KU Leuven

CRYPTO 2012 — August 21, 2012

Motivation

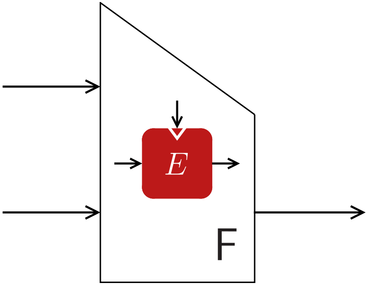
- Hash functions based on block ciphers
  - Davies-Meyer '84, PGV '93, Tandem-DM '92, ...
  - MD5 '92, SHA-1 '95, SHA-2 '01, Blake '08, Skein '08, ...



Motivation

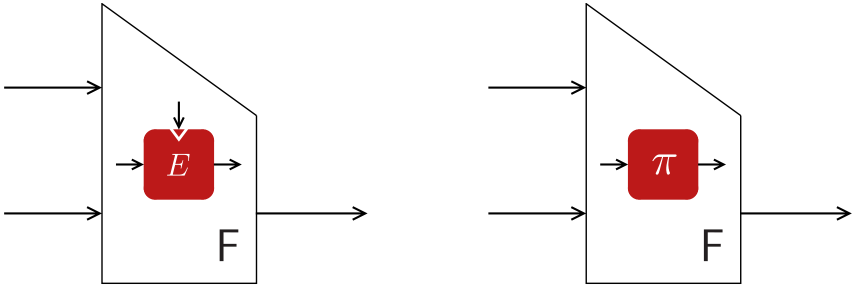
- Hash functions based on block ciphers
  - Davies-Meyer '84, PGV '93, Tandem-DM '92, ...
  - MD5 '92, SHA-1 '95, SHA-2 '01, Blake '08, Skein '08, ...

- Re-keying $\longrightarrow$ related-key security, efficiency loss, ...



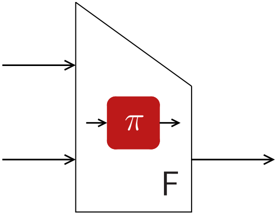
Motivation

- Hash functions based on block ciphers
  - Davies-Meyer '84, PGV '93, Tandem-DM '92, ...
  - MD5 '92, SHA-1 '95, SHA-2 '01, Blake '08, Skein '08, ...
- Re-keying $\longrightarrow$ related-key security, efficiency loss, ...
- Instead use fixed-key block ciphers, or permutations



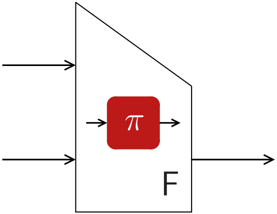
Motivation

- Black-Cochran-Shrimpton '05: no secure $2n$-to-n-bit function using 1 n-bit permutation call



Motivation

- Black-Cochran-Shrimpton '05: no secure $2n$-to-n-bit function using 1 n-bit permutation call

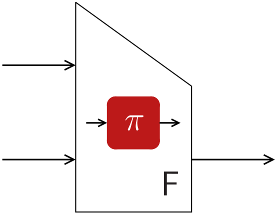


- Generalized by Rogaway-Steinberger '08, Stam '08, Steinberger '10
  - mn-to-rn-bit function using k n-bit permutations: collisions in $(2^n)^{1-(m-r+1)/(k+1)}$ queries (almost always)

F	2 π	3 π	4 π	5 π
$2n \to n$	$2^{n/3}$	$2^{n/2}$		
$\frac{5}{2}n \to n$	$2^{n/6}$	$2^{3n/8}$	$2^{n/2}$	
$4n \to 2n$	1	$2^{n/4}$	$2^{2n/5}$	$2^{n/2}$

Motivation

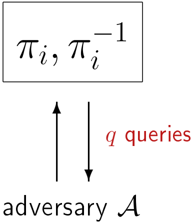
- Black-Cochran-Shrimpton '05: no secure $2n$-to-n-bit function using 1 n-bit permutation call



- Generalized by Rogaway-Steinberger '08, Stam '08, Steinberger '10
  - mn-to-rn-bit function using k n-bit permutations: collisions in $(2^n)^{1-(m-r+1)/(k+1)}$ queries (almost always)

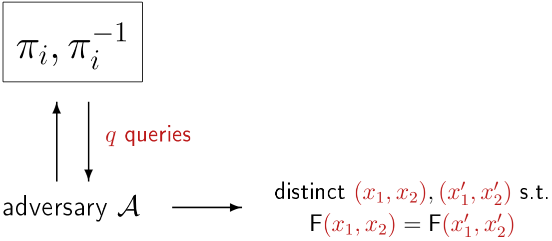
F	2 π	3 π	4 π	5 π
$2n \to n$	$2^{n/3}$	$2^{n/2}$		
$\frac{5}{2}n \to n$	$2^{n/6}$	$2^{3n/8}$	$2^{n/2}$	
$4n \to 2n$	1	$2^{n/4}$	$2^{2n/5}$	$2^{n/2}$

Security Model



- Ideal permutation model: π_i's randomly generated
- Adversary query access to π_i's

Security Model



- Ideal permutation model: π_i's randomly generated
- Adversary query access to π_i's

$$\mathbf{Adv}_{\mathsf{F}}^{\mathsf{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

Security Model

$$\boxed{\pi_i, \pi_i^{-1}}$$

q queries

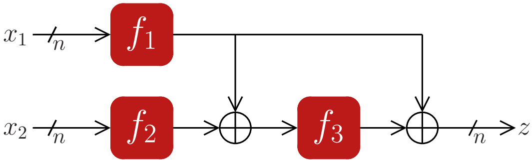
$$z \in \{0,1\}^n \longrightarrow \text{adversary } \mathcal{A} \longrightarrow (x_1, x_2) \text{ s.t. } \mathsf{F}(x_1, x_2) = z$$

- Ideal permutation model: π_i's randomly generated
- Adversary query access to π_i's

$$\mathbf{Adv}_{\mathsf{F}}^{\mathsf{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

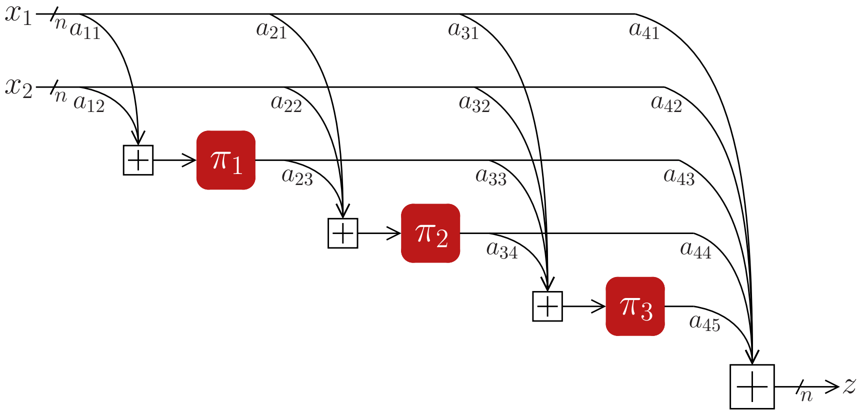
$$\mathbf{Adv}_{\mathsf{F}}^{\mathsf{epre}}(q) = \max_{\mathcal{A}} \max_{z \in \{0,1\}^n} \text{ success probability } \mathcal{A}$$

Prior Constructions — Shrimpton-Stam '08



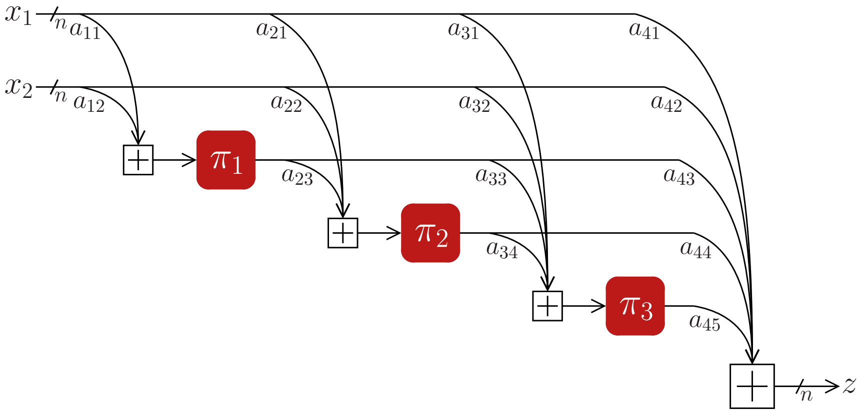
- $2n$-to-n-bit function using 3 one-way functions
- Optimal collision security
- Collision security if $f_i(x) = \pi_i(x) \oplus x$ (showed by automated analysis)

Prior Constructions — Rogaway-Steinberger '08



- $2n$-to-n-bit function (over $\mathbb{F}_{2^n}$) using 3 permutations

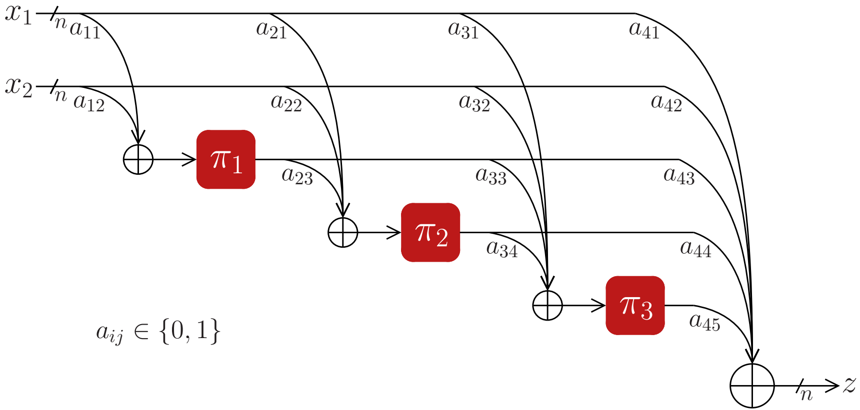
Prior Constructions — Rogaway-Steinberger '08



- $2n$-to-n-bit function (over $\mathbb{F}_{2^n}$) using 3 permutations
- Collision/preimage security if a_{ij} satisfy "independence criterion"
  $\longrightarrow$ Excludes binary a_{ij}

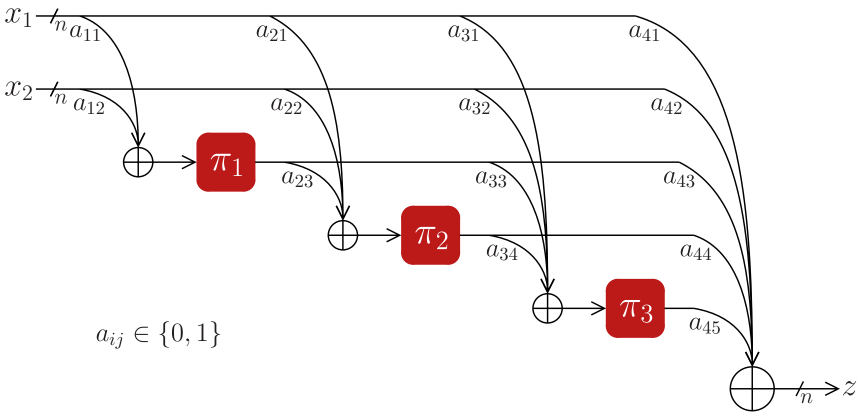
Our Compression Function Design

- $2n$-to-n compression function using permutations and $\bigoplus$-operators

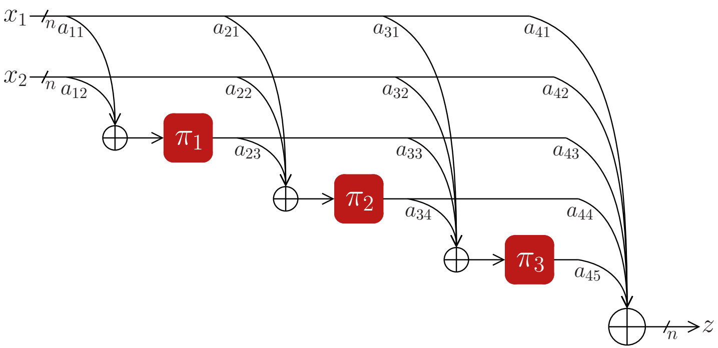


Our Compression Function Design

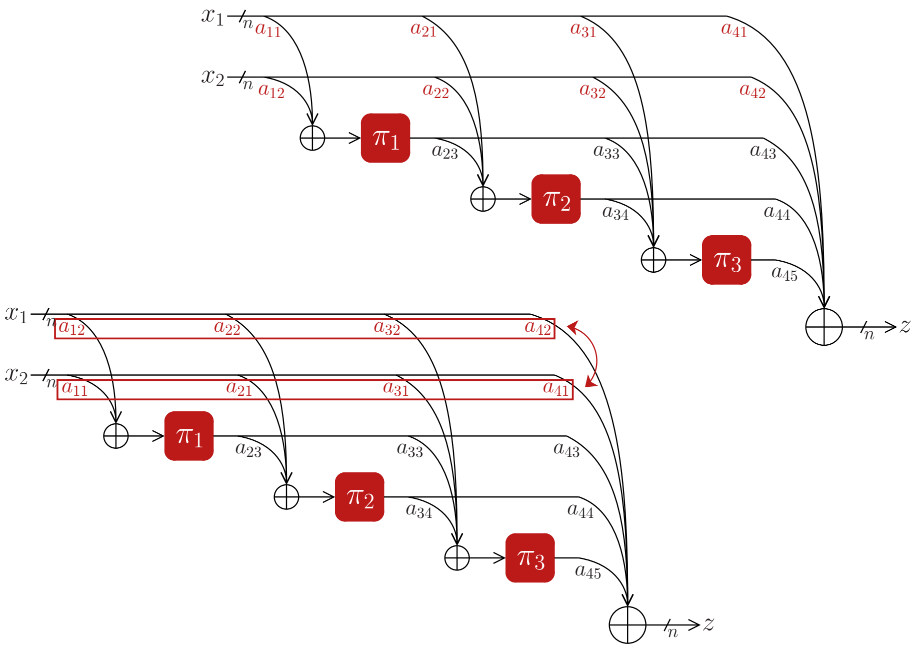
- $2n$-to-n compression function using permutations and $\bigoplus$-operators

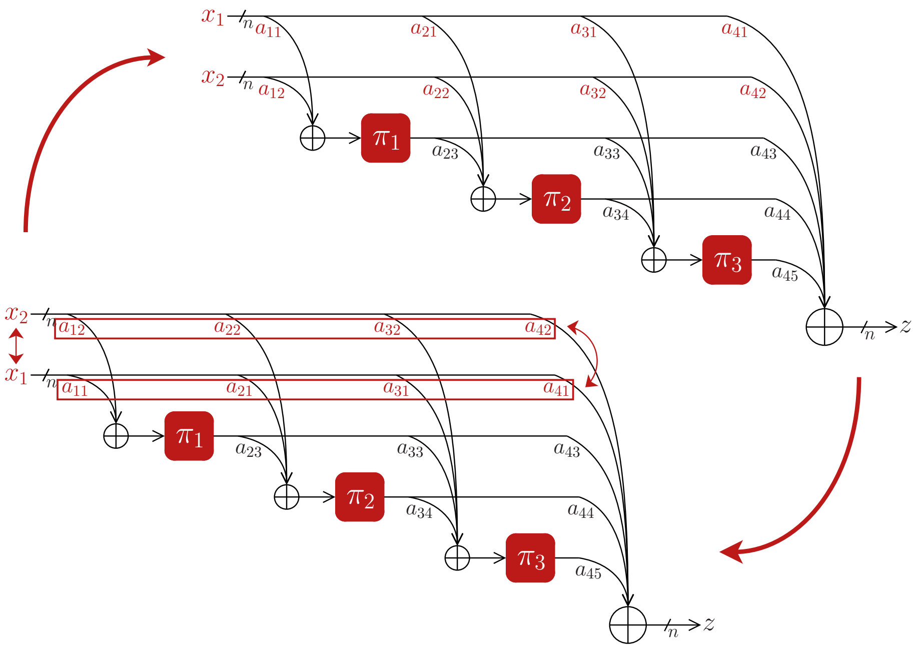


- Multi-permutation setting: π_i's all different
- Single-permutation setting: $\pi_1 = \pi_2 = \pi_3$



x_1
x_2
n
n
a_{11}
a_{21}
a_{31}
a_{41}
a_{12}
a_{22}
a_{32}
a_{42}
π_1
a_{23}
a_{33}
a_{43}
π_2
a_{34}
a_{44}
π_3
a_{45}
n
z


x_1
x_2
n
a_{11} a_{21} a_{31} a_{41}
a_{12} a_{22} a_{32} a_{42}
π_1 a_{23} a_{33} a_{43}
π_2 a_{34} a_{44}
π_3 a_{45}
z
x_1
x_2
n
a_{12} a_{22} a_{32} a_{42}
a_{11} a_{21} a_{31} a_{41}
π_1 a_{23} a_{33} a_{43}
π_2 a_{34} a_{44}
π_3 a_{45}
z


x_1
x_2
n
a_11
a_21
a_31
a_41
a_12
a_22
a_32
a_42
π_1
π_2
π_3
a_23
a_33
a_43
a_34
a_44
a_45
z

Equivalence Classes

Definition: Equivalence Class

Compression functions F and F' are equivalent if for both collision and preimage security there exists a tight bi-directional reduction

- Intuition: F and F' equivalent $\longrightarrow$ 'equally secure'

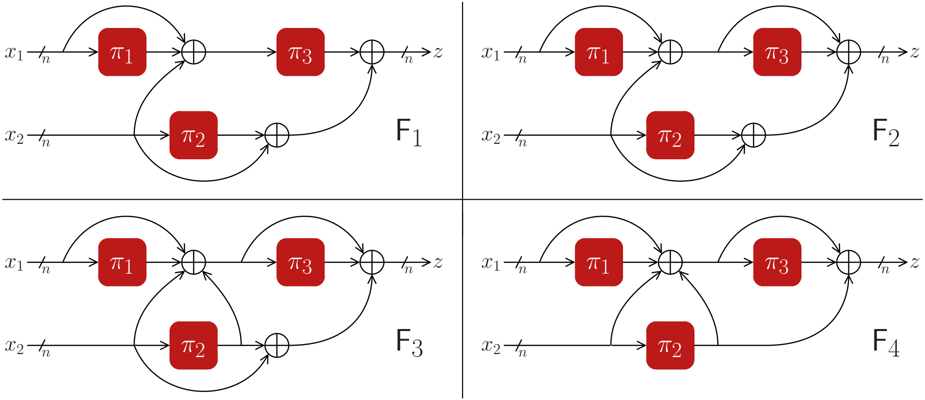
Equivalence Classes

Definition: Equivalence Class

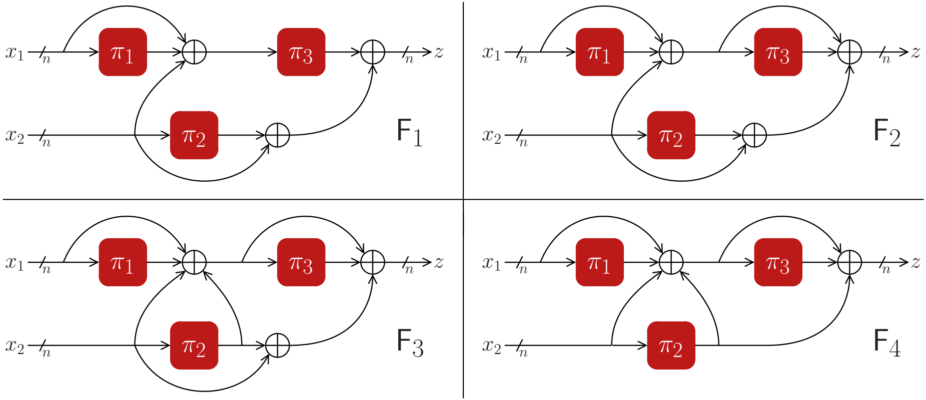
Compression functions F and F′ are equivalent if for both collision and preimage security there exists a tight bi-directional reduction

- Intuition: F and F′ equivalent $\longrightarrow$ 'equally secure'
- We identify 4 equivalence reductions
  - Example reduction of previous slide
  - 3 extra reductions
- We restrict to equivalence w.r.t. these reductions only

Multi-Permutation Setting — Main Result

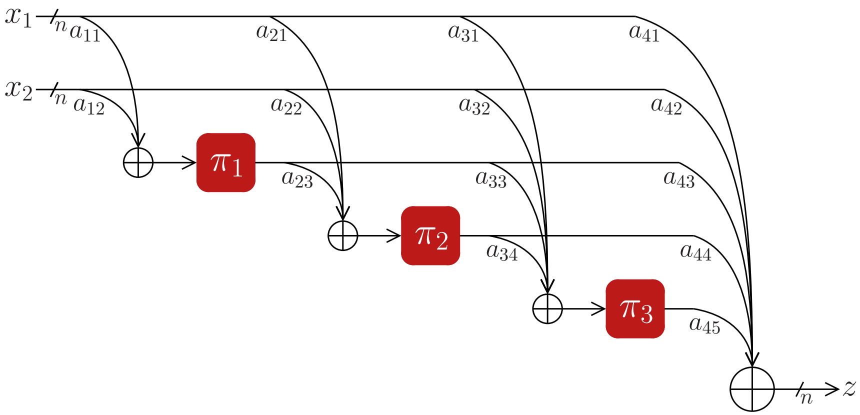


Multi-Permutation Setting — Main Result

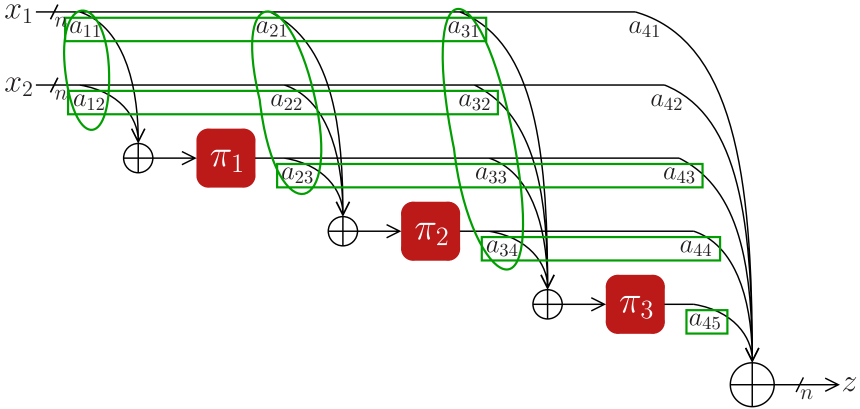


F equivalent to:	collision	preimage
$\mathsf{F}_1, \mathsf{F}_4$	✓[c]	✗
F_2	✓[c]	✓[c]
F_3	✓	✗
none of these	✗	?

Multi-Permutation Setting — Proof Idea (1)

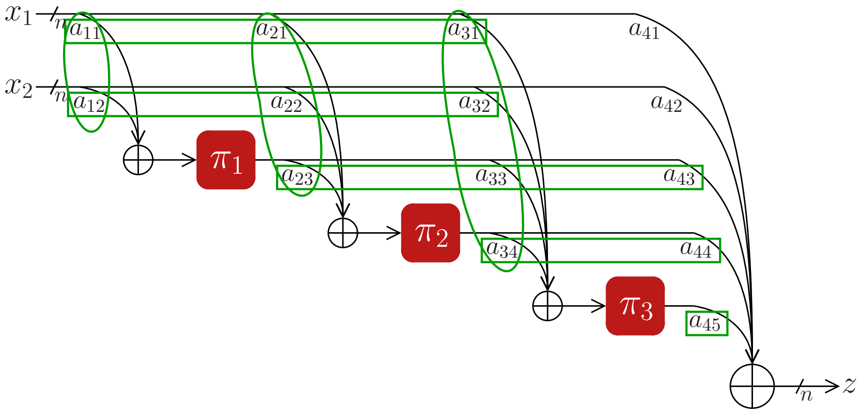


Multi-Permutation Setting — Proof Idea (1)

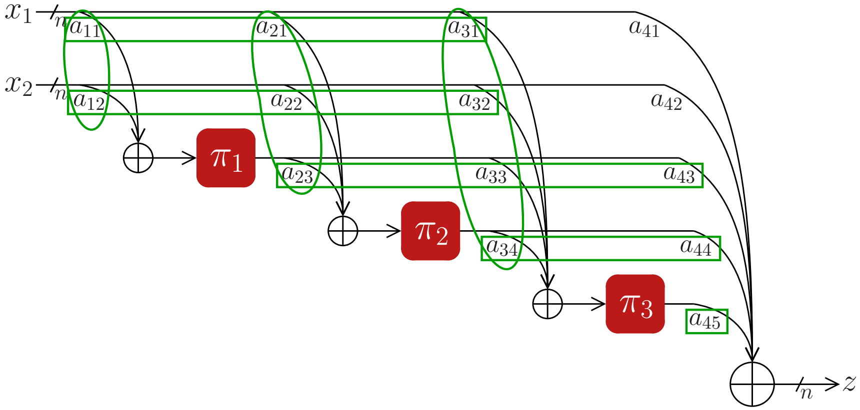


- In total 2^{14} schemes, but many trivially insecure
- Function is "valid" if each green set contains a 1
- We consider valid compression functions only

Multi-Permutation Setting — Proof Idea (2)



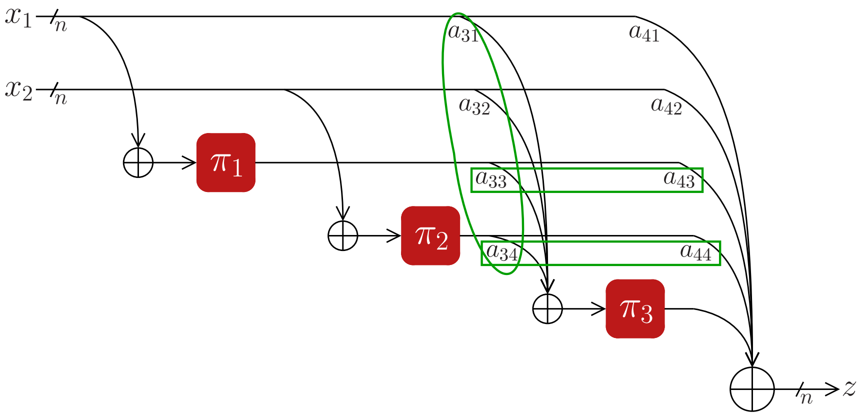
Multi-Permutation Setting — Proof Idea (2)



- Any valid F equivalent to some F′ with

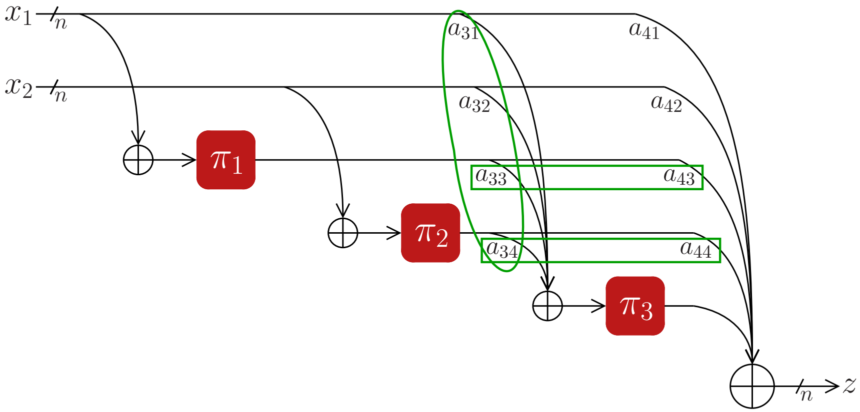
$$(a_{11}, a_{12}) = (1, 0) \text{ and } (a_{21}, a_{22}, a_{23}) = (0, 1, 0)$$

Multi-Permutation Setting — Proof Idea (2)

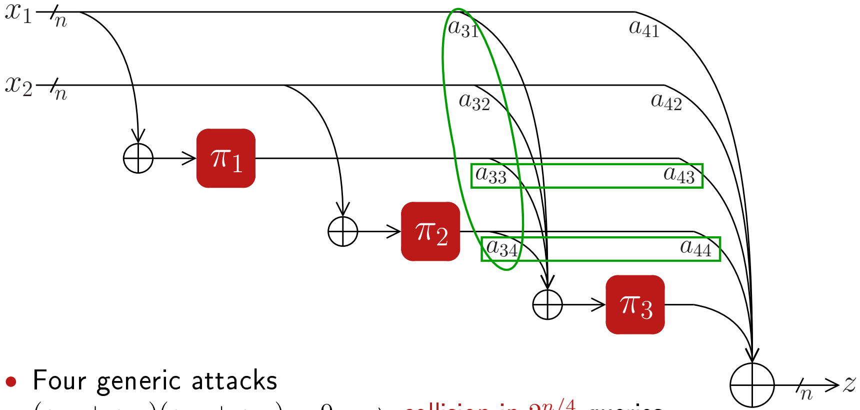


- Any valid F equivalent to some F′ with
  $$(a_{11}, a_{12}) = (1, 0) \text{ and } (a_{21}, a_{22}, a_{23}) = (0, 1, 0)$$
- It suffices to consider these functions only

Multi-Permutation Setting — Proof Idea (3)



Multi-Permutation Setting — Proof Idea (3)



- Four generic attacks

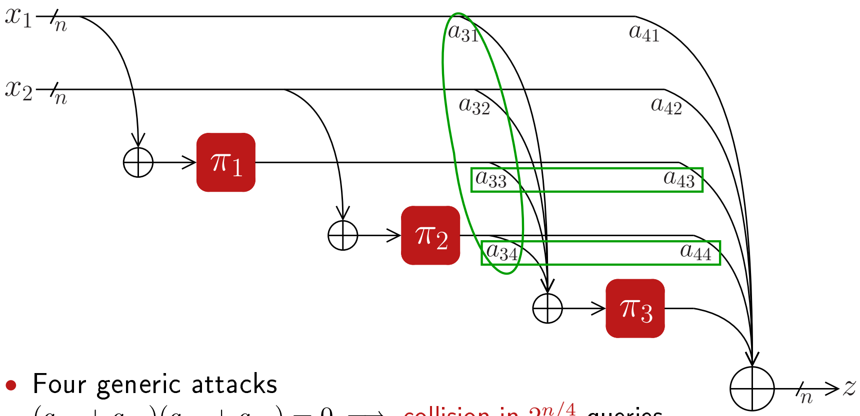
  $(a_{31} + a_{33})(a_{32} + a_{34}) = 0 \implies$ collision in $2^{n/4}$ queries

  $\vee_{j=1}^{4} a_{3j} = a_{4j} = 0 \implies$ collision in $2^{n/3}$ queries

  $\wedge_{j=1}^{2} a_{3j} a_{4,j+2} \neq a_{3,j+2} a_{4j} \implies$ collision in $2^{n/3}$ queries

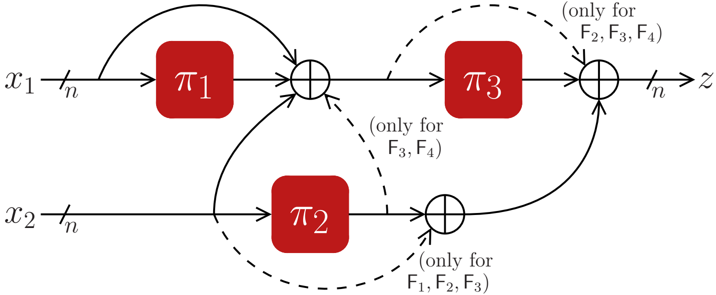
  $a_{41} + a_{42} + a_{43} + a_{44} = 1 \implies$ collision in $2^{2n/5}$ queries

Multi-Permutation Setting — Proof Idea (3)



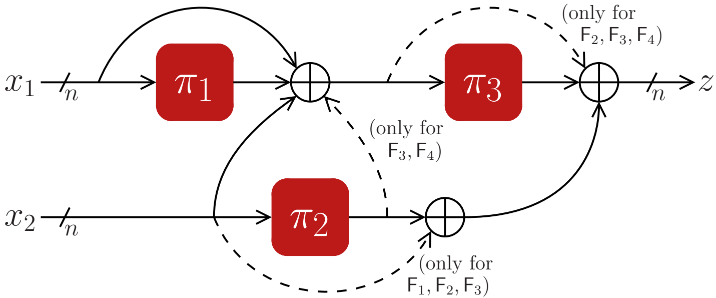
- Four generic attacks
  $(a_{31} + a_{33})(a_{32} + a_{34}) = 0 \implies$ collision in $2^{n/4}$ queries
  $\vee_{j=1}^{4} a_{3j} = a_{4j} = 0 \implies$ collision in $2^{n/3}$ queries
  $\wedge_{j=1}^{2} a_{3j} a_{4,j+2} \neq a_{3,j+2} a_{4j} \implies$ collision in $2^{n/3}$ queries
  $a_{41} + a_{42} + a_{43} + a_{44} = 1 \implies$ collision in $2^{2n/5}$ queries
- F is collision secure only if equivalent to $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{F}_4$

Multi-Permutation Setting — Proof Idea (4)



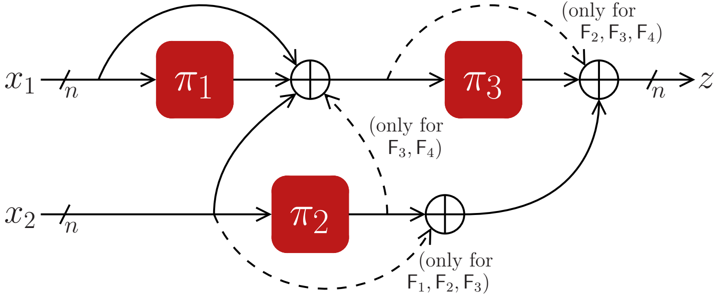
- F is collision secure only if it is equivalent to $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{F}_4$

Multi-Permutation Setting — Proof Idea (4)



- F is collision secure only if it is equivalent to $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{F}_4$
- Remains to prove: if-relation and preimage resistance

Multi-Permutation Setting — Proof Idea (4)



- F is collision secure only if it is equivalent to $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{F}_4$
- Remains to prove: if-relation and preimage resistance
- Hardest and most technical part
  - $\mathsf{F}_1, \ldots, \mathsf{F}_4$ collision resistant up to $2^{n/2}$ queries tight (asympt.)
  - F_2 preimage resistant up to $2^{2n/3}$ queries tight (asympt.)
  - $\mathsf{F}_1, \mathsf{F}_3, \mathsf{F}_4$ preimage resistant up to $2^{n/2}$ queries tight

Multi-Permutation Setting — Conjecture

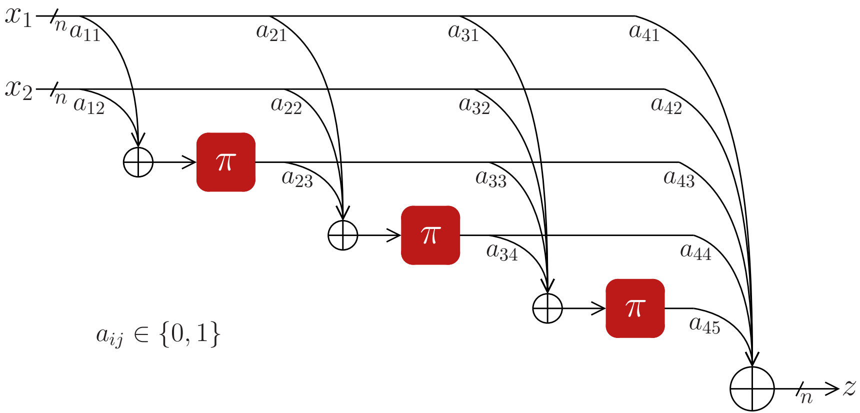
Z : set of q random elements from $\{0,1\}^n$ (duplicates may occur)
X, Y : any two sets of q elements from $\{0,1\}^n$ (no duplicates)

Conjecture

With high probability, there exist $O(q \log q)$ tuples $(x, y, z) \in X \times Y \times Z$ such that $x \oplus y = z$

- Conjecture relates to area of extremal graph theory
- Similar to (but more complex than) a longstanding problem of Zarankiewicz from 1951
- Detailed heuristical argument in paper

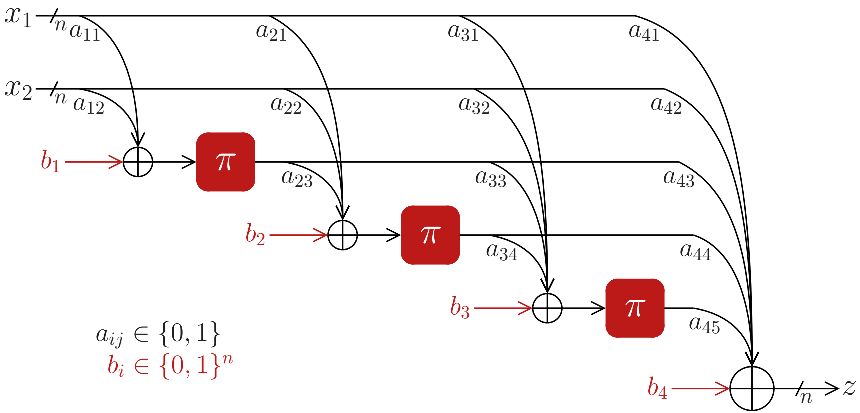
Single-Permutation Setting — Main Result



Theorem

For any compression function of this form, collisions can be found in $2^{2n/5}$ queries (proof is similar)

Single-Permutation Setting — Main Result



Theorem

For any compression function of this form, collisions can be found in $2^{2n/5}$ queries (proof is similar)

Conclusions

Complete classification of $2n$-to-n-bit compression functions solely based on three permutations and $\bigoplus$-operators

- Multi-permutation setting: analysis of 2^{14} functions
  - 216 functions optimally collision secure
  - 48 of which optimally preimage secure
- Single-permutation setting: non-existence of collision secure F
  - Attack on 2^{14} (or in fact $2^{4n}2^{14}$) functions

Conclusions

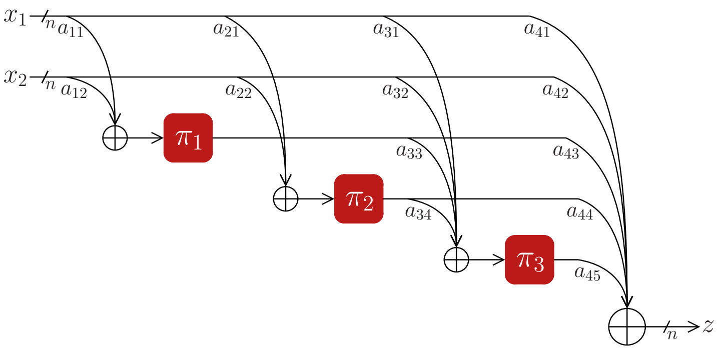
Complete classification of $2n$-to-n-bit compression functions solely based on three permutations and $\bigoplus$-operators

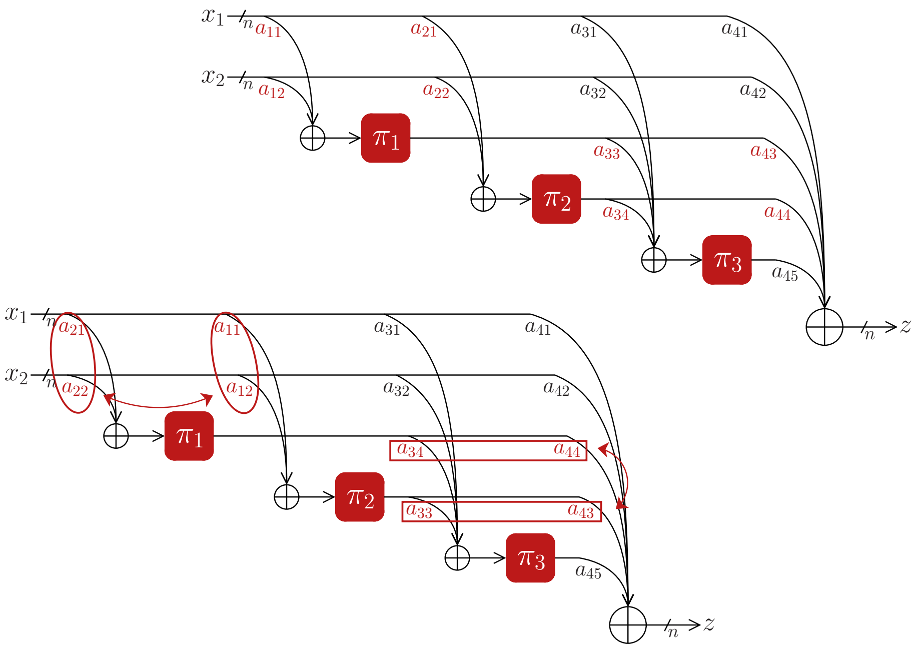
- Multi-permutation setting: analysis of 2^{14} functions
  - 216 functions optimally collision secure
  - 48 of which optimally preimage secure
- Single-permutation setting: non-existence of collision secure F
  - Attack on 2^{14} (or in fact $2^{4n}2^{14}$) functions

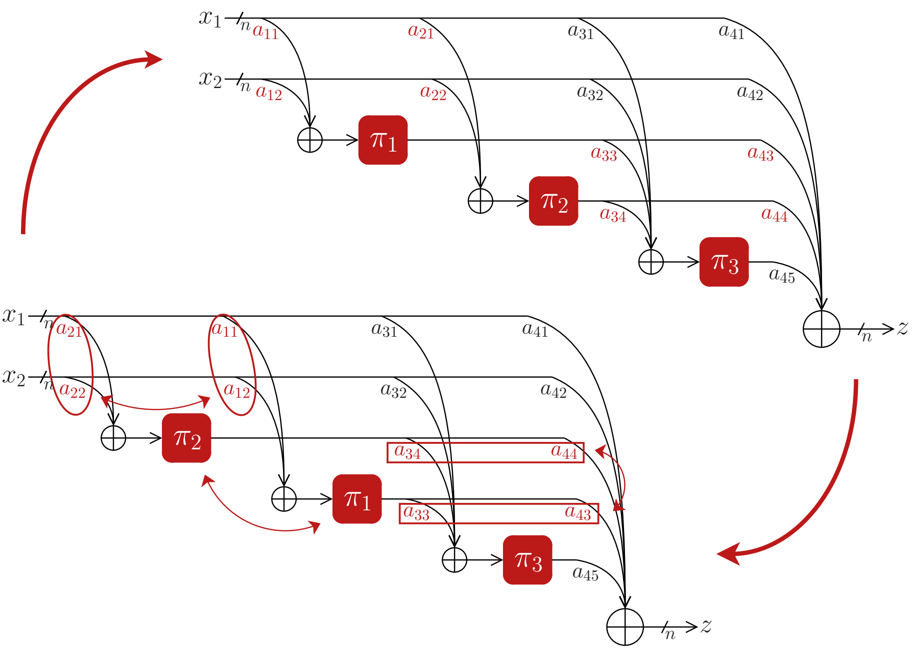
- Research directions:
  - Generalize to larger F's, and with different primitives
  - Generalize impossibility result in single-permutation setting
  - Conjecture

Thank you for your attention!

Supporting slides

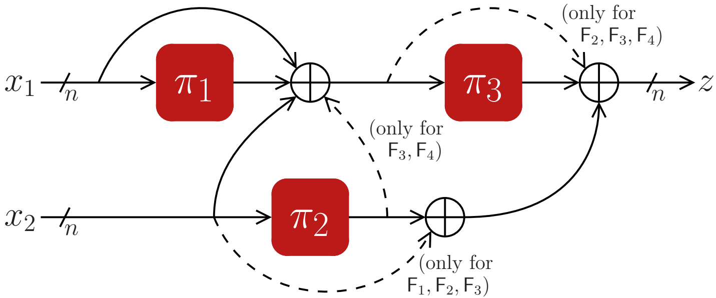

x_1
x_2
n
n
a_{11}
a_{21}
a_{31}
a_{41}
a_{12}
a_{22}
a_{32}
a_{42}
π_1
a_{33}
a_{43}
π_2
a_{34}
a_{44}
π_3
a_{45}
n
z


x_1
x_2
n
a_{11}
a_{21}
a_{31}
a_{41}
a_{12}
a_{22}
a_{32}
a_{42}
π_1
a_{33}
a_{43}
π_2
a_{34}
a_{44}
π_3
a_{45}
z
x_1
x_2
n
a_{21}
a_{11}
a_{31}
a_{41}
a_{22}
a_{12}
a_{32}
a_{42}
π_1
a_{34}
a_{44}
π_2
a_{33}
a_{43}
π_3
a_{45}
z



x_1
x_2
n
a_{11}
a_{21}
a_{31}
a_{41}
a_{12}
a_{22}
a_{32}
a_{42}
π_1
a_{33}
a_{43}
π_2
a_{34}
a_{44}
π_3
a_{45}
z
x_1
x_2
a_{21}
a_{11}
a_{31}
a_{41}
a_{22}
a_{12}
a_{32}
a_{42}
π_2
a_{34}
a_{44}
π_1
a_{33}
a_{43}
π_3
a_{45}
z

Summary of Our Results



	collision		preimage	
F equivalent to:	security	attack	security	attack
$\mathsf{F}_1, \mathsf{F}_4$	$2^{n/2}$ [c]	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
F_2	$2^{n/2}$ [c]	$2^{n/2}$	$2^{2n/3}$ [c]	$2^{2n/3}$
F_3	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
none of these	?	$2^{2n/5}$	?	?
any F in SP-setting	?	$2^{2n/5}$	?	?