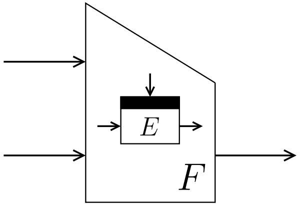
Optimal Collision Security in Double Block Length Hashing with Single Length Key

Bart Mennink
KU Leuven

ASIACRYPT 2012 — December 5, 2012

Introduction

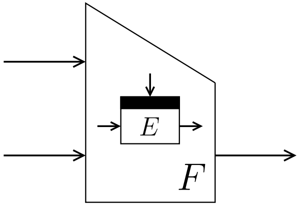
- Classical block cipher based hashing
  - $F : \{0,1\}^{2n} \to \{0,1\}^n$ using n-bit cipher
  - Davies-Meyer ('84), PGV ('93), MD5 ('92), SHA-1 ('95), ...



Introduction

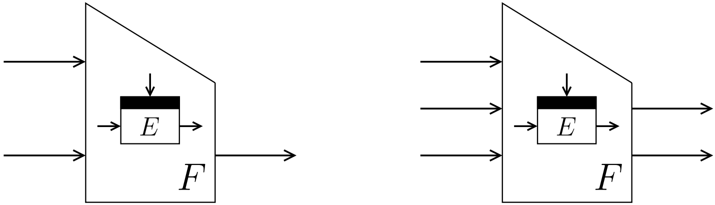
- Classical block cipher based hashing
  - $F : \{0,1\}^{2n} \to \{0,1\}^n$ using n-bit cipher
  - Davies-Meyer ('84), PGV ('93), MD5 ('92), SHA-1 ('95), ...

- Same underlying primitive but larger compression function?



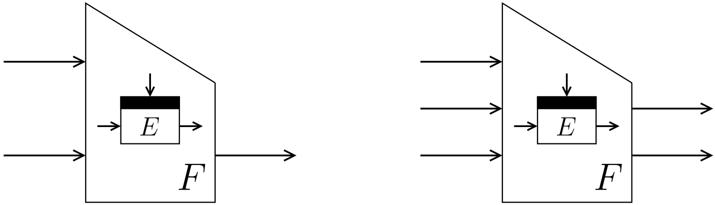
Introduction

- Classical block cipher based hashing
  - $F : \{0,1\}^{2n} \to \{0,1\}^n$ using n-bit cipher
  - Davies-Meyer ('84), PGV ('93), MD5 ('92), SHA-1 ('95), ...
- Same underlying primitive but larger compression function?
- Double block length hashing
  - $F : \{0,1\}^{3n} \to \{0,1\}^{2n}$ still using n-bit cipher
  - Security proofs typically harder



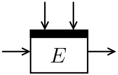
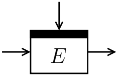
Introduction

- Classical block cipher based hashing
  - $F : \{0,1\}^{2n} \to \{0,1\}^n$ using n-bit cipher
  - Davies-Meyer ('84), PGV ('93), MD5 ('92), SHA-1 ('95), ...
- Same underlying primitive but larger compression function?
- Double block length hashing
  - $F : \{0,1\}^{3n} \to \{0,1\}^{2n}$ still using n-bit cipher
  - Security proofs typically harder

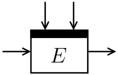


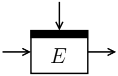
$F : \{0,1\}^{3n} \to \{0,1\}^{2n}$ from $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

Introduction

compression function	E-calls	collision security	preimage security	underlying cipher
				 $2n$-bit key
				 n-bit key

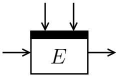
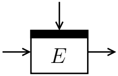
Introduction

compression function	E-calls	collision security	preimage security	underlying cipher
Stam's ('08 -'10)	1	2^n	2^n	
Tandem-DM ('92)	2	2^n	2^{2n}	
Abreast-DM ('92)	2	2^n	2^{2n}	
Hirose's ('06)	2	2^n	2^{2n}	
Hirose-class ('04)	2	2^n	2^n	$2n$-bit key
Özen-Stam-class ('09)	2	2^n	2^n	

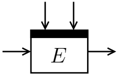
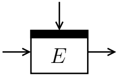


n-bit key

Introduction

compression function	E-calls	collision security	preimage security	underlying cipher
Stam's ('08 - '10)	1	2^n	2^n	
Tandem-DM ('92)	2	2^n	2^{2n}	
Abreast-DM ('92)	2	2^n	2^{2n}	
Hirose's ('06)	2	2^n	2^{2n}	
Hirose-class ('04)	2	2^n	2^n	$2n$-bit key
Özen-Stam-class ('09)	2	2^n	2^n	
MDC-2 ('88)	2	$2^{n/2}$	2^n	
MJH ('11)	2	$2^{n/2}$	2^n	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$	n-bit key

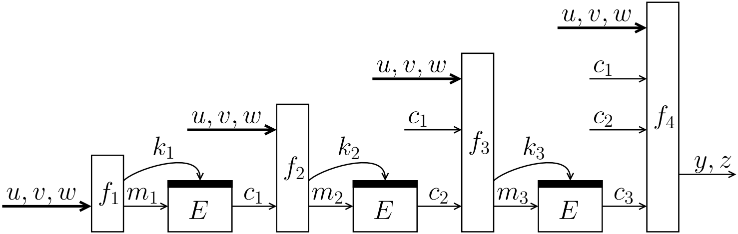
Introduction

compression function	E-calls	collision security	preimage security	underlying cipher
Stam's ('08 - '10)	1	2^n	2^n	
Tandem-DM ('92)	2	2^n	2^{2n}	
Abreast-DM ('92)	2	2^n	2^{2n}	
Hirose's ('06)	2	2^n	2^{2n}	
Hirose-class ('04)	2	2^n	2^n	$2n$-bit key
Özen-Stam-class ('09)	2	2^n	2^n	
MDC-2 ('88)	2	$2^{n/2}$	2^n	
MJH ('11)	2	$2^{n/2}$	2^n	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$	n-bit key
???	?	$\mathbf{2^n}$	$\mathbf{2^{2n}}$	

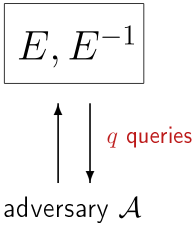
Our Goal

$$F^r : \{0,1\}^{3n} \to \{0,1\}^{2n} \text{ from } r$$

$$\text{calls to } E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$$



Security Model



- Ideal cipher model: E randomly generated
- Adversary query access to E

Security Model

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

q queries

adversary $\mathcal{A}$ $\longrightarrow$ distinct $(u, v, w), (u', v', w')$ s.t. $F^r(u, v, w) = F^r(u', v', w')$

- Ideal cipher model: E randomly generated
- Adversary query access to E

$$\mathbf{adv}_{F^r}^{\mathrm{coll}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

Security Model

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

q queries

$$(y,z) \in \{0,1\}^{2n} \longrightarrow \text{adversary } \mathcal{A} \longrightarrow (u,v,w) \text{ s.t. } F^r(u,v,w) = (y,z)$$

- Ideal cipher model: E randomly generated
- Adversary query access to E

$$\mathbf{adv}_{F^r}^{\mathrm{coll}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

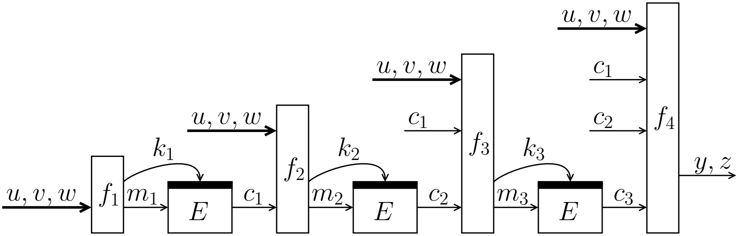
$$\mathbf{adv}_{F^r}^{\mathrm{pre}}(q) = \max_{\mathcal{A}} \max_{(y,z)} \text{ success probability } \mathcal{A}$$

Pigeonhole-Birthday Attack

- [Rogaway-Steinberger-EC08]: generic collision/preimage attack for permutation based compression functions

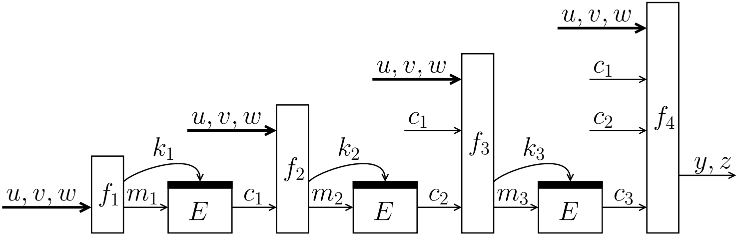
Pigeonhole-Birthday Attack

- [Rogaway-Steinberger-EC08]: generic collision/preimage attack for permutation based compression functions
- Straightforward to generalize to F^r



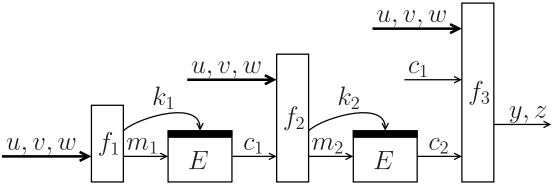
Pigeonhole-Birthday Attack

- [Rogaway-Steinberger-EC08]: generic collision/preimage attack for permutation based compression functions
- Straightforward to generalize to F^r

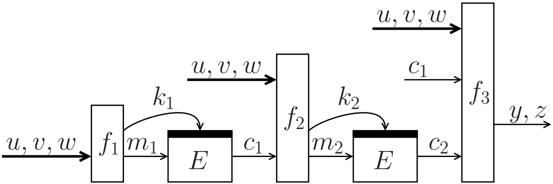


r (E-calls)	1	2	3	4	...
collision in	1	2^n	2^n	2^n	...
preimage in	2^n	$2^{3n/2}$	$2^{5n/3}$	$2^{7n/4}$	...

F^2: 2-Call Double Length Hashing



F^2: 2-Call Double Length Hashing



Theorem

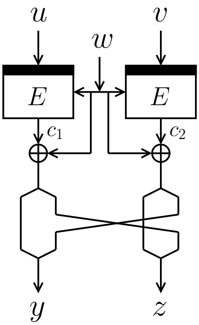
Suppose $\exists$ bijective L such that $\forall\, u, v, w, c_1, c_2$:

$$\text{left}_n \circ L \circ f_3(u, v, w; c_1, c_2) = \text{left}_n \circ L \circ f_3(u, v, w; c_1, 0)$$

Then, one expects collisions for F^2 in $2^{n/2}$ queries

F^2: Examples

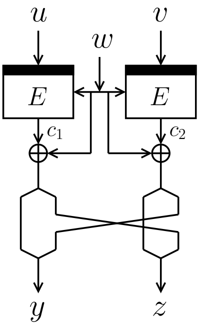
- Attack covers wide class of functions
  - Designs with linear finalization function f_3



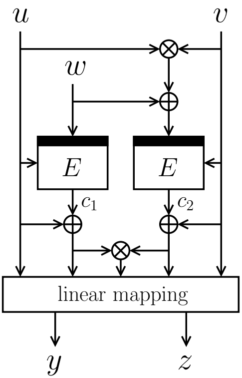
put $L(y, z) = (y^l \| z^r, z^l \| y^r)$

F^2: Examples

- Attack covers wide class of functions
  - Designs with linear finalization function f_3
  - Some functions with non-linear f_3 ...
    ... but Jetchev-Özen-Stam's construction unaffected



put $L(y, z) = (y^l \| z^r, z^l \| y^r)$



F^3: 3-Call Double Length Hashing

- Next step: 3 calls
- We propose the F^3_{A} double length hashing family

F^3: 3-Call Double Length Hashing

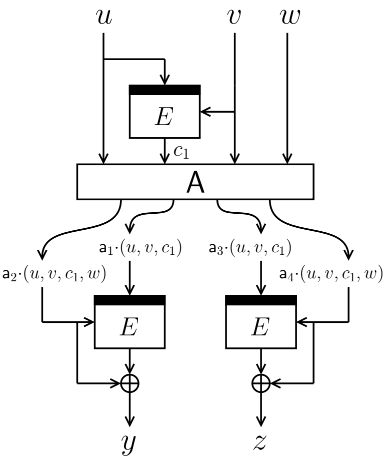
- Next step: 3 calls
- We propose the F^3_{A} double length hashing family

- Basic idea:
  - For $2n$-bit keyed hashing: one E-call compresses entire input
  - For n-bit keyed hashing: impossible to achieve!
    - Any E-call gets only $2n$ bits of info
  - Now: any two E evaluations define (inputs to) third one

F^3: 3-Call Double Length Hashing

- Next step: 3 calls
- We propose the F^3_{A} double length hashing family
- Basic idea:
  - For $2n$-bit keyed hashing: one E-call compresses entire input
  - For n-bit keyed hashing: impossible to achieve!
    - Any E-call gets only $2n$ bits of info
  - Now: any two E evaluations define (inputs to) third one
- Consider finite field $GF(2^n)$

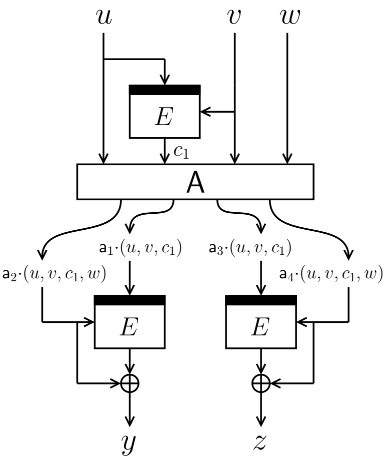
F^3_{A}: Our 3-Call Double Length Hashing Proposal



- F^3_{A} indexed by matrix A:

$$\mathsf{A} = \begin{pmatrix} \mathsf{a}_1 \\ \mathsf{a}_2 \\ \mathsf{a}_3 \\ \mathsf{a}_4 \end{pmatrix} = \begin{pmatrix} \mathsf{a}_{11} & \mathsf{a}_{12} & \mathsf{a}_{13} & 0 \\ \mathsf{a}_{21} & \mathsf{a}_{22} & \mathsf{a}_{23} & \mathsf{a}_{24} \\ \mathsf{a}_{31} & \mathsf{a}_{32} & \mathsf{a}_{33} & 0 \\ \mathsf{a}_{41} & \mathsf{a}_{42} & \mathsf{a}_{43} & \mathsf{a}_{44} \end{pmatrix}$$

F^3_{A}: Our 3-Call Double Length Hashing Proposal



- F^3_{A} indexed by matrix A:

$$\mathsf{A} = \begin{pmatrix} \mathsf{a}_1 \\ \mathsf{a}_2 \\ \mathsf{a}_3 \\ \mathsf{a}_4 \end{pmatrix} = \begin{pmatrix} \mathsf{a}_{11} & \mathsf{a}_{12} & \mathsf{a}_{13} & 0 \\ \mathsf{a}_{21} & \mathsf{a}_{22} & \mathsf{a}_{23} & \mathsf{a}_{24} \\ \mathsf{a}_{31} & \mathsf{a}_{32} & \mathsf{a}_{33} & 0 \\ \mathsf{a}_{41} & \mathsf{a}_{42} & \mathsf{a}_{43} & \mathsf{a}_{44} \end{pmatrix}$$

- If A invertible and $\mathsf{a}_{24}, \mathsf{a}_{44} \neq 0$, any two E evaluations define (inputs to) third one

F^3_{A}: Collision Resistance

$$\mathsf{A} = \begin{pmatrix} \mathsf{a}_{11} & \mathsf{a}_{12} & \mathsf{a}_{13} & 0 \\ \mathsf{a}_{21} & \mathsf{a}_{22} & \mathsf{a}_{23} & \mathsf{a}_{24} \\ \mathsf{a}_{31} & \mathsf{a}_{32} & \mathsf{a}_{33} & 0 \\ \mathsf{a}_{41} & \mathsf{a}_{42} & \mathsf{a}_{43} & \mathsf{a}_{44} \end{pmatrix}$$

Theorem

If A satisfies "`colreq`":

- A invertible
- $\mathsf{a}_{12}, \mathsf{a}_{13}, \mathsf{a}_{24}, \mathsf{a}_{32}, \mathsf{a}_{33}, \mathsf{a}_{44} \neq 0$
- $\mathsf{a}_{12} \neq \mathsf{a}_{32}$ and $\mathsf{a}_{13} \neq \mathsf{a}_{33}$

Then, for any $\varepsilon > 0$:

$$\mathbf{adv}^{\mathrm{coll}}_{F^3_{\mathsf{A}}}(2^{n(1-\varepsilon)}) \to 0 \text{ for } n \to \infty$$

- `colreq` easily satisfied

F^3_{A}: Collision Resistance

$$\mathsf{A} = \begin{pmatrix} \mathsf{a}_{11} & \mathsf{a}_{12} & \mathsf{a}_{13} & 0 \\ \mathsf{a}_{21} & \mathsf{a}_{22} & \mathsf{a}_{23} & \mathsf{a}_{24} \\ \mathsf{a}_{31} & \mathsf{a}_{32} & \mathsf{a}_{33} & 0 \\ \mathsf{a}_{41} & \mathsf{a}_{42} & \mathsf{a}_{43} & \mathsf{a}_{44} \end{pmatrix}$$

Theorem

If A satisfies "`colreq`":

- A invertible
- $\mathsf{a}_{12}, \mathsf{a}_{13}, \mathsf{a}_{24}, \mathsf{a}_{32}, \mathsf{a}_{33}, \mathsf{a}_{44} \neq 0$
- $\mathsf{a}_{12} \neq \mathsf{a}_{32}$ and $\mathsf{a}_{13} \neq \mathsf{a}_{33}$

Then, for any $\varepsilon > 0$:

$$\mathbf{adv}^{\mathrm{coll}}_{F^3_{\mathsf{A}}}(2^{n(1-\varepsilon)}) \to 0 \text{ for } n \to \infty$$

- `colreq` easily satisfied
- Basic proof idea similar to existing proofs
- New proof approach: apply idea of wish lists to collision resistance

F^3_{A}: Preimage Resistance

Theorem

If A satisfies "`prereq`":

- $\mathsf{A} - \begin{pmatrix} \mathsf{B}_1 & \begin{matrix} 00 \\ 00 \end{matrix} \\ \mathsf{B}_2 & \begin{matrix} 00 \\ 00 \end{matrix} \end{pmatrix}$ invertible $\forall\, \mathsf{B}_1, \mathsf{B}_2 \in \left\{ \binom{00}{00}, \binom{10}{00}, \binom{10}{01} \right\}$
- $\mathsf{a}_{12}, \mathsf{a}_{13}, \mathsf{a}_{24}, \mathsf{a}_{32}, \mathsf{a}_{33}, \mathsf{a}_{44} \neq 0$
- $\mathsf{a}_{12} \neq \mathsf{a}_{32}$, $\mathsf{a}_{13} \neq \mathsf{a}_{33}$, and $\mathsf{a}_{24} \neq \mathsf{a}_{44}$

Then, for any $\varepsilon > 0$:

$$\mathbf{adv}^{\mathrm{pre}}_{F^3_{\mathsf{A}}}(2^{3n(1-\varepsilon)/2}) \to 0 \text{ for } n \to \infty$$

- `prereq` $\Rightarrow$ `colreq`, easily satisfied

F^3_{A}: Preimage Resistance

Theorem

If A satisfies "prereq":

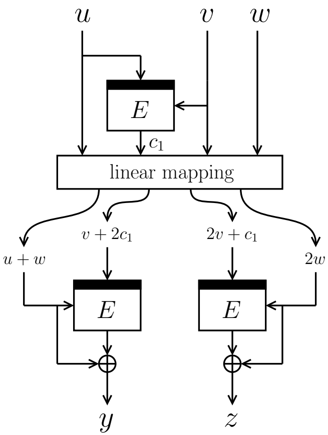
- $\mathsf{A} - \begin{pmatrix} \mathsf{B}_1 & \begin{matrix} 00 \\ 00 \end{matrix} \\ \mathsf{B}_2 & \begin{matrix} 00 \\ 00 \end{matrix} \end{pmatrix}$ invertible $\forall\, \mathsf{B}_1, \mathsf{B}_2 \in \left\{ \binom{00}{00}, \binom{10}{00}, \binom{10}{01} \right\}$
- $\mathsf{a}_{12}, \mathsf{a}_{13}, \mathsf{a}_{24}, \mathsf{a}_{32}, \mathsf{a}_{33}, \mathsf{a}_{44} \neq 0$
- $\mathsf{a}_{12} \neq \mathsf{a}_{32}$, $\mathsf{a}_{13} \neq \mathsf{a}_{33}$, and $\mathsf{a}_{24} \neq \mathsf{a}_{44}$

Then, for any $\varepsilon > 0$:

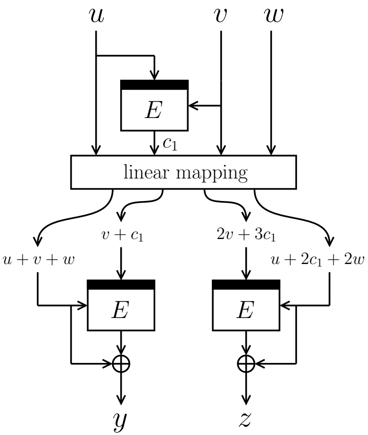
$$\mathbf{adv}^{\mathrm{pre}}_{F^3_{\mathsf{A}}}(2^{3n(1-\varepsilon)/2}) \to 0 \text{ for } n \to \infty$$

- `prereq` $\Rightarrow$ `colreq`, easily satisfied
- Bound non-optimal, but close to generic bound
- Bound is tight: attack in $O(2^{3n/2})$ queries

F^3_{A}: Example Functions

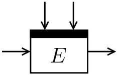
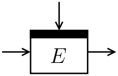


$$\mathsf{A} = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$



$$\mathsf{A} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & 3 & 0 \\ 1 & 0 & 2 & 2 \end{pmatrix}$$

Conclusions

compression function	E-calls	collision security	preimage security	underlying cipher
Stam's ('08 - '10)	1	2^n	2^n	
Tandem-DM ('92)	2	2^n	2^{2n}	
Abreast-DM ('92)	2	2^n	2^{2n}	
Hirose's ('06)	2	2^n	2^{2n}	$2n$-bit key
Hirose-class ('04)	2	2^n	2^n	
Özen-Stam-class ('09)	2	2^n	2^n	
MDC-2 ('88)	2	$2^{n/2}$	2^n	
MJH ('11)	2	$2^{n/2}$	2^n	
Jetchev-Özen-Stam's ('12)	2	$2^{2n/3}$	2^n	
MDC-4 ('88)	4	$2^{5n/8}$	$2^{5n/4}$	n-bit key
Our proposal	**3**	$\mathbf{2^n}$	$\mathbf{2^{3n/2}}$	

Conclusions

F^3_{A}: new family of double length hash functions

- Optimal collision security using n-bit keyed cipher
- Yet, 3 calls and non-parallelizable

Conclusions

F_{A}^3: new family of double length hash functions

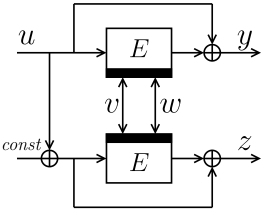
- Optimal collision security using n-bit keyed cipher
- Yet, 3 calls and non-parallelizable

- Open Problems
  - Optimally collision *and* preimage secure F^3 beyond F_{A}^3?
  - More efficient constructions?
  - F^3 with f_1, f_2, f_3, f_4 $\oplus$-only [M-Preneel-C12]?

Thank you for your attention!

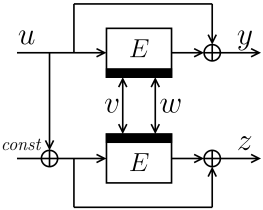
SUPPORTING SLIDES

Introduction: Hirose's Compression Function

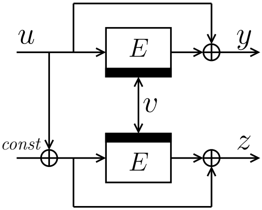


Hirose's $F(u, v, w) = (y, z)$

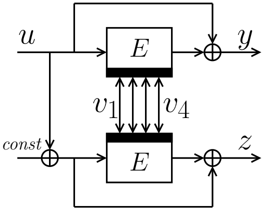
Introduction: Hirose's Compression Function



Hirose's $F(u, v, w) = (y, z)$



$F(u, v) = (y, z)$

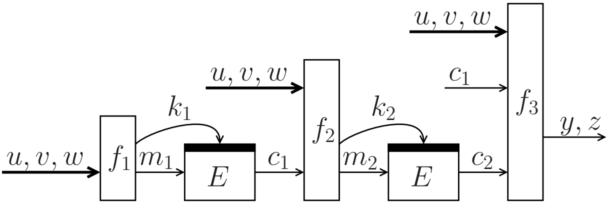


$F(u, v_1, v_2, v_3, v_4) = (y, z)$

F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:

$$\mathsf{left}_n \circ f_3(u, v, w; c_1, c_2) = \mathsf{left}_n \circ f_3(u, v, w; c_1, 0)$$

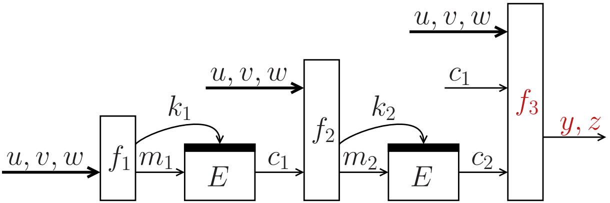


F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\ u, v, w, c_1, c_2$:

$$\text{left}_n \circ f_3(u, v, w; c_1, c_2) = \text{left}_n \circ f_3(u, v, w; c_1, 0)$$

- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$

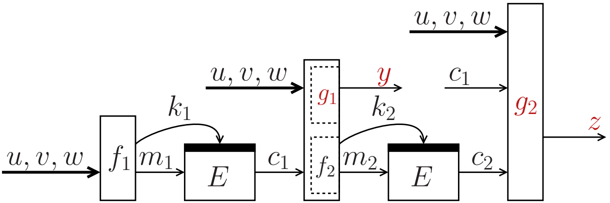


F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:

$$\mathsf{left}_n \circ f_3(u, v, w; c_1, c_2) = \mathsf{left}_n \circ f_3(u, v, w; c_1, 0)$$

- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$

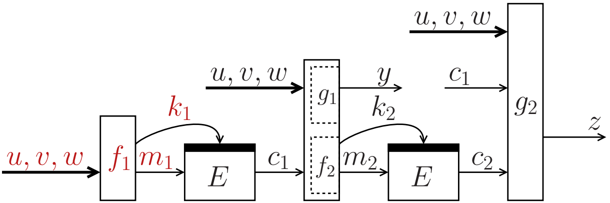


F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:

$$\mathsf{left}_n \circ f_3(u, v, w; c_1, c_2) = \mathsf{left}_n \circ f_3(u, v, w; c_1, 0)$$

- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$
- Greedy adversary: find $2^{n/2}$ (k_1, m_1) that cover $\geq 2^{3n/2}$ (u, v, w)

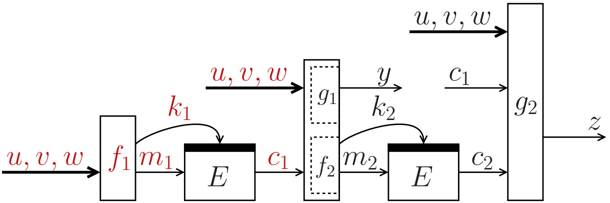


F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:

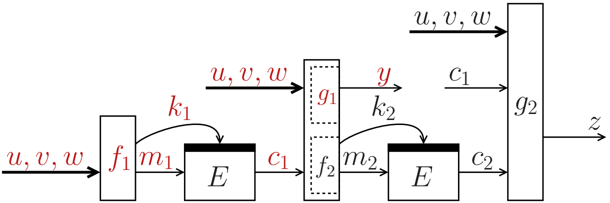
$$\mathsf{left}_n \circ f_3(u, v, w; c_1, c_2) = \mathsf{left}_n \circ f_3(u, v, w; c_1, 0)$$

- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$
- Greedy adversary: find $2^{n/2}$ (k_1, m_1) that cover $\geq 2^{3n/2}$ (u, v, w)
- Query these to find $\geq 2^{3n/2}$ tuples $(u, v, w; c_1)$



F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:
$$\mathsf{left}_n \circ f_3(u, v, w; c_1, c_2) = \mathsf{left}_n \circ f_3(u, v, w; c_1, 0)$$
- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$
- Greedy adversary: find $2^{n/2}$ (k_1, m_1) that cover $\geq 2^{3n/2}$ (u, v, w)
- Query these to find $\geq 2^{3n/2}$ tuples $(u, v, w; c_1)$
- For some y: $\geq 2^{n/2}$ tuples $(u, v, w; c_1)$ satisfy $g_1(u, v, w; c_1) = y$

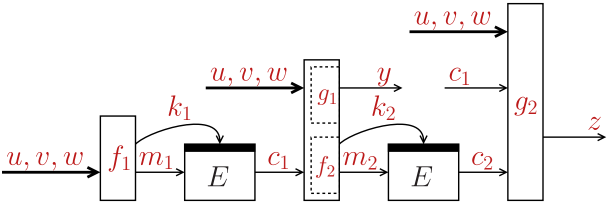


F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:

$$\text{left}_n \circ f_3(u, v, w; c_1, c_2) = \text{left}_n \circ f_3(u, v, w; c_1, 0)$$

- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$
- Greedy adversary: find $2^{n/2}$ (k_1, m_1) that cover $\geq 2^{3n/2}$ (u, v, w)
- Query these to find $\geq 2^{3n/2}$ tuples $(u, v, w; c_1)$
- For some y: $\geq 2^{n/2}$ tuples $(u, v, w; c_1)$ satisfy $g_1(u, v, w; c_1) = y$
- Vary over these to find a collision in g_2

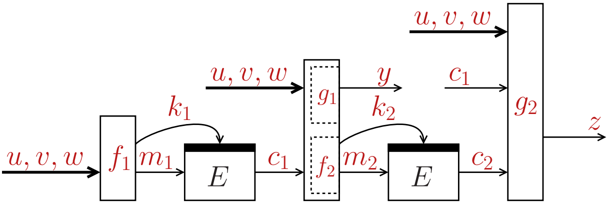


F^2: Extended Proof Idea

- First consider $L = id$, so suppose $\forall\, u, v, w, c_1, c_2$:

$$\text{left}_n \circ f_3(u, v, w; c_1, c_2) = \text{left}_n \circ f_3(u, v, w; c_1, 0)$$

- Write $f_3(u, v, w; c_1, c_2) = g_1(u, v, w; c_1) \| g_2(u, v, w; c_1, c_2)$
- Greedy adversary: find $2^{n/2}$ (k_1, m_1) that cover $\geq 2^{3n/2}$ (u, v, w)
- Query these to find $\geq 2^{3n/2}$ tuples $(u, v, w; c_1)$
- For some y: $\geq 2^{n/2}$ tuples $(u, v, w; c_1)$ satisfy $g_1(u, v, w; c_1) = y$
- Vary over these to find a collision in g_2



- Arbitrary bijective L: use idea of equivalence classes [M-Preneel-C12]