Ideal-Cipher (Ir)reducibility for Blockcipher-Based Hash Functions

EUROCRYPT 2013

Paul Baecher, Pooya Farshim, Marc Fischlin, Martijn Stam

University of Bristol & Darmstadt University of Technology; supported by DFG Heisenberg and Center For Advanced Security Research Darmstadt (CASED)

CASED

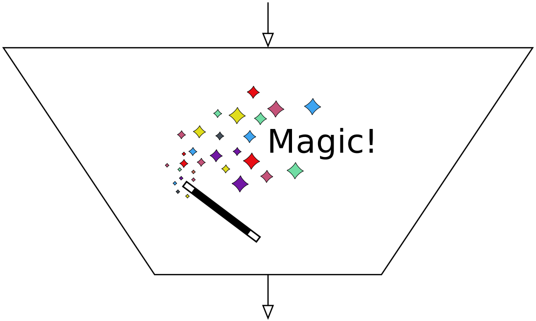
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Heisenberg-Programm
Deutsche Forschungsgemeinschaft

Introduction

Hash Functions in Real Life

$\{0,1\}^*$

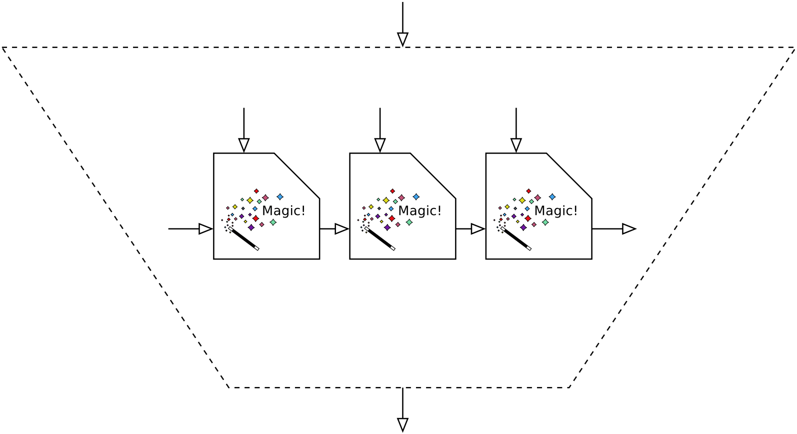


$\{0,1\}^n$

Hash Functions in Real Life

Zoom: 2x

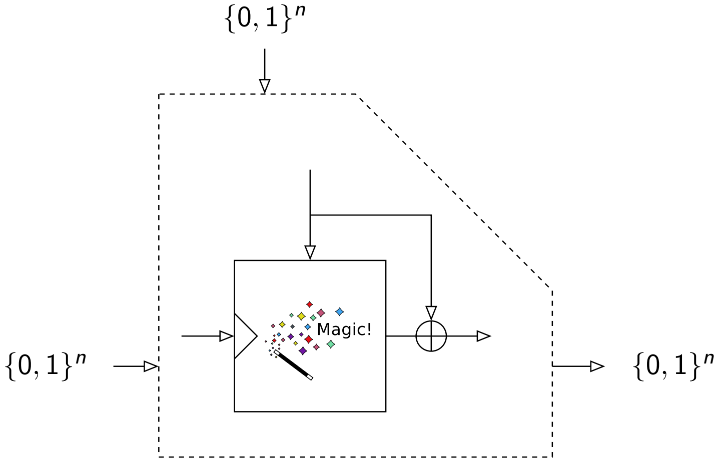
$\{0,1\}^{kn}$ for all $k \in \mathbb{N}$



$\{0,1\}^{n}$

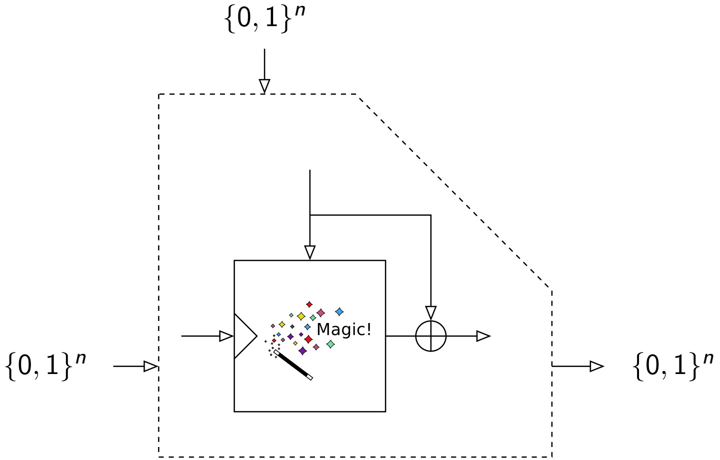
Hash Functions in Real Life

Zoom: 3x



Hash Functions in Real Life

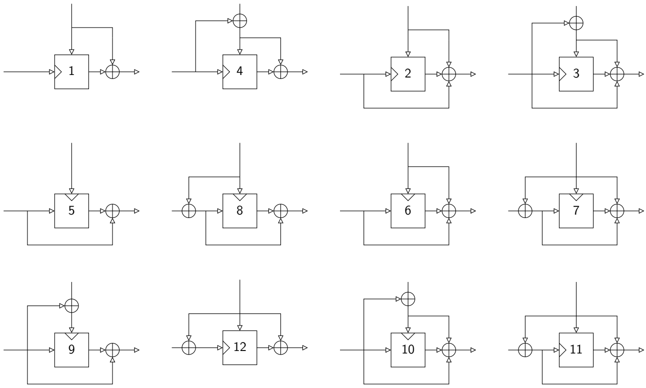
Zoom: 3x



scope of this paper: blockcipher-based compression functions

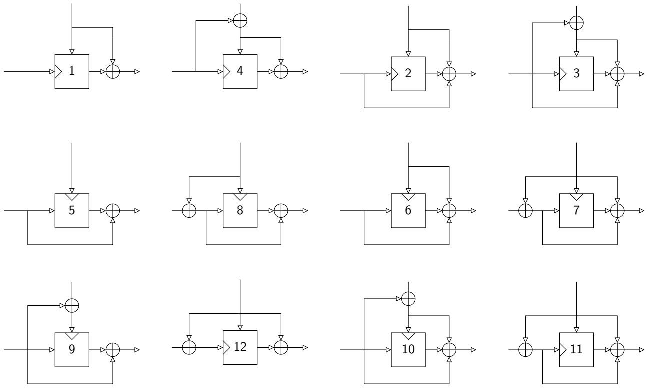
Blockcipher-Based Compression Functions

- 64 basic variants using XOR operations [PGV94]
  - 12 provably secure: collision and preimage resistance [BRSS10]
  - . . . in the ideal-cipher model



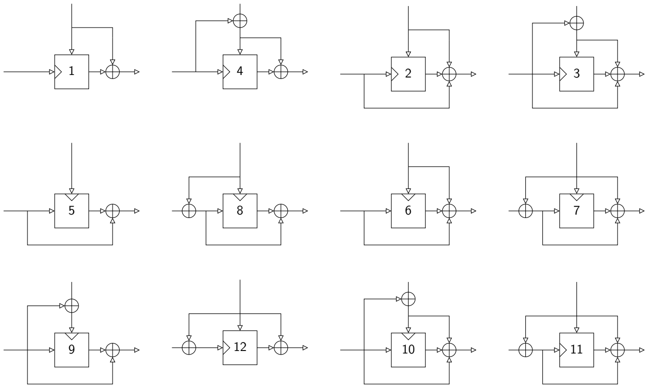
Blockcipher-Based Compression Functions

- 64 basic variants using XOR operations [PGV94]
  - 12 provably secure: collision and preimage resistance [BRSS10]
  - . . . in the ideal-cipher model



Blockcipher-Based Compression Functions

- 64 basic variants using XOR operations [PGV94]
  - 12 provably secure: collision and preimage resistance [BRSS10]
  - . . . in the ideal-cipher model



- only have AES, which function is good?

Ideal-Cipher Reducibility

Ideal-Cipher Reducibility

- based on (random-)oracle reducibility [BF11]

- relate compressions functions to each other w.r.t. to the blockcipher
- using a reductionist approach

Ideal-Cipher Reducibility

- based on (random-)oracle reducibility [BF11]
- relate compressions functions to each other w.r.t. to the blockcipher
- using a reductionist approach

"any blockcipher E that makes g^{E} secure also makes f^{E} secure"

or

"the blockcipher E in f reduces to the blockcipher E in g"

Ideal-Cipher Reducibility Defined

Def.: direct reducibility

"any blockcipher E that makes g^{E} secure also makes f^{E} secure"

Def.: free reducibility

"there exists T s.t. any blockcipher E that makes g^{E} secure also makes $f^{T^{E}}$ secure"

Ideal-Cipher Reducibility Defined

Def.: direct reducibility

"any blockcipher E that makes g^{E} secure also makes f^{E} secure"

$\Longrightarrow$

T := id

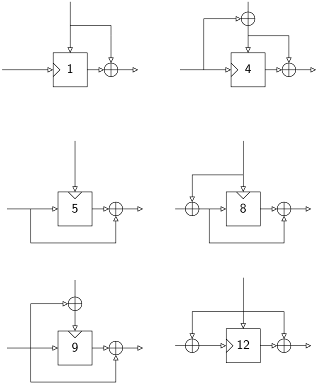
Def.: free reducibility

"there exists T s.t. any blockcipher E that makes g^{E} secure also makes $f^{\mathsf{T}^{\mathsf{E}}}$ secure"

- transformation T should be
  - simple (efficient, deterministic, stateless)
  - explicitly given in a proof
- note: simplified for exposition (E is actually a distribution)

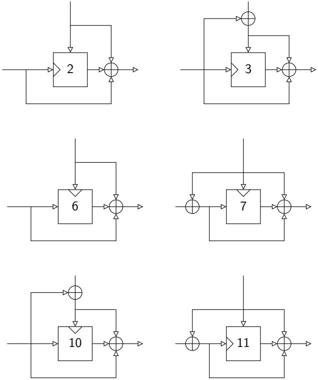
Revisiting the 12 PGV Functions

PGV_1-group



direct reducibility within

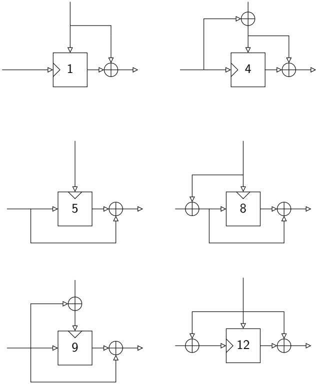
PGV_2-group



direct reducibility within

Revisiting the 12 PGV Functions

PGV_1-group

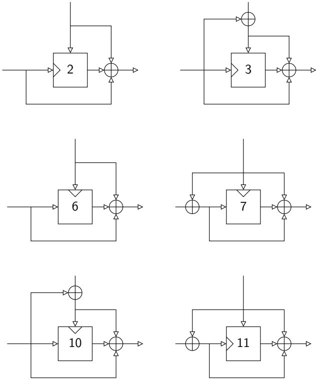


reducibility
(free)

↭

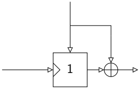
separation
(direct)

PGV_2-group



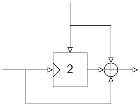
Revisiting the 12 PGV Functions

PGV$_1$-group

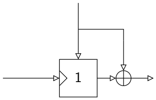


reducibility
(free)

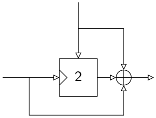
PGV$_2$-group



(Freely) Reducing PGV_2 to PGV_1



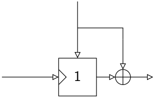
$\mathsf{E}(K, M) \oplus M$



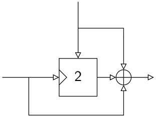
$\mathsf{E}(K, M) \oplus M \oplus K$

- there exists T^{E} s.t. for any E $\quad \mathsf{PGV}_1^{\mathsf{E}}$ secure $\Rightarrow \mathsf{PGV}_2^{\mathsf{T}^{\mathsf{E}}}$ secure

(Freely) Reducing PGV_2 to PGV_1

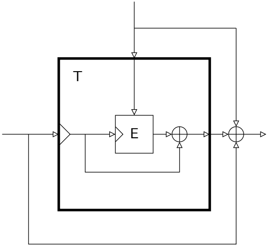


$E(K, M) \oplus M$



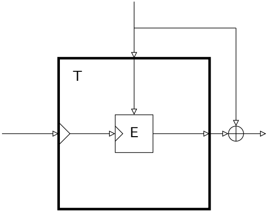
$E(K, M) \oplus M \oplus K$

- there exists T^E s.t. for any E $\quad PGV_1^E$ secure $\Rightarrow PGV_2^{T^E}$ secure
- $T^E(K, M) := E(K, M) \oplus K$



$T^E(K, M) \oplus M \oplus K$

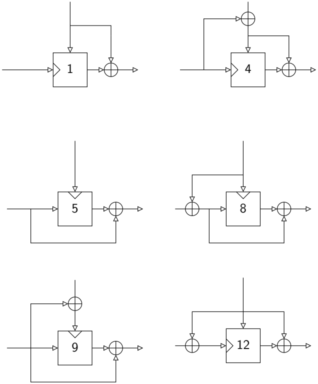
$\equiv$



$E(K, M) \oplus M$

Revisiting the 12 PGV Functions

PGV_1-group

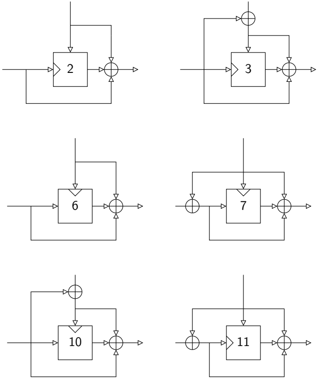


reducibility
(free)

$\leftrightsquigarrow$

separation
(direct)

PGV_2-group



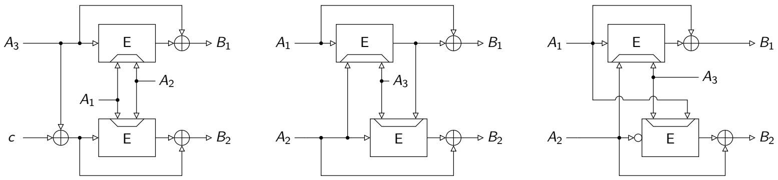
PGV Groups are Incomparable

- no direct reduction from PGV_1 to PGV_2 (or vice versa)
  - there exist blockciphers that make one secure but not the other
- groups are incomparable, no clear "winner"

Beyond PGV

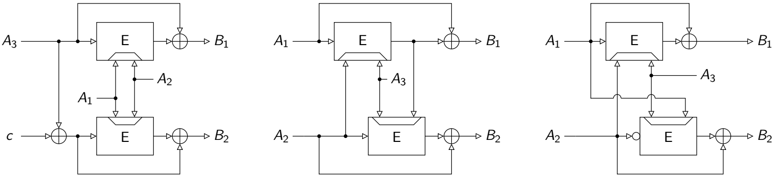
Double-Block-Length (DBL) Compression Functions

- compression functions $\{0,1\}^{3n} \to \{0,1\}^{2n}$
- two blockcipher invocations, double key lengths ($2n$)



Double-Block-Length (DBL) Compression Functions

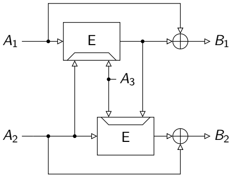
- compression functions $\{0,1\}^{3n} \to \{0,1\}^{2n}$
- two blockcipher invocations, double key lengths ($2n$)



- upper part $\equiv$ PGV$_1$
- hence direct reducibility (only!) for collision resistance

Double-Block-Length (DBL) Compression Functions

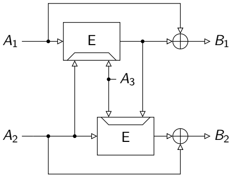
- compression functions $\{0,1\}^{3n} \rightarrow \{0,1\}^{2n}$
- two blockcipher invocations, double key lengths ($2n$)



- upper part $\equiv$ PGV_1
- hence direct reducibility (only!) for collision resistance

Double-Block-Length (DBL) Compression Functions

- compression functions $\{0,1\}^{3n} \rightarrow \{0,1\}^{2n}$
- two blockcipher invocations, double key lengths ($2n$)



- upper part $\equiv$ PGV_1
- hence direct reducibility (only!) for collision resistance
  - preimage resistance: separation
  - idea: either output "leaks" one half of the preimage

Further Results on DBL Compression Functions

- no direct reducibility among any DBL compression function

- reducibility to PGV_1 under free transformations
  - key length extension via chaining
- no free reducibility from any PGV to any DBL
  - ... as expected?

- DBL constructions thus rely on weaker assumptions
  - i.e., not only better because of double output length

Further Results on DBL Compression Functions

- no direct reducibility among any DBL compression function

- reducibility to PGV_1 under free transformations
  - key length extension via chaining
- no free reducibility from any PGV to any DBL
  - . . . as expected?

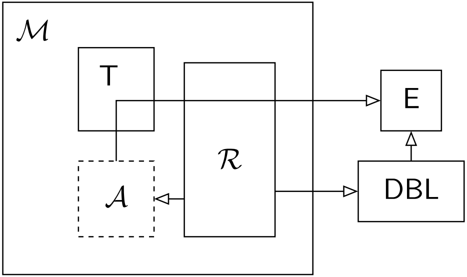
- DBL constructions thus rely on weaker assumptions
  - i.e., not only better because of double output length

Sketch: No Free Reducibility from PGV to DBL

- import techniques from [Pie08] on combiner impossibility
- meta reduction combined with generic bounds on attacking collision resistance [BK04]
- rule out existence of $(\mathsf{T}, \mathcal{R})$
  - $\mathcal{R}$ breaks DBL given PGV adversary:

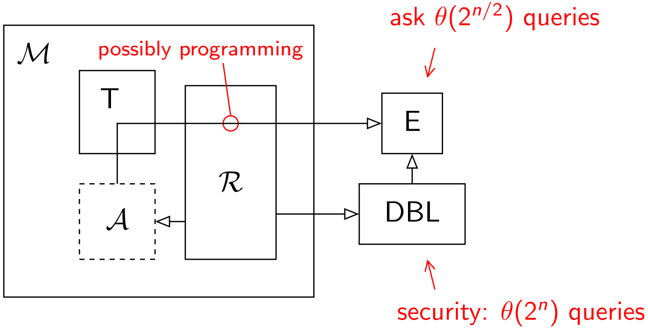
Sketch: No Free Reducibility from PGV to DBL

- import techniques from [Pie08] on combiner impossibility
- meta reduction combined with generic bounds on attacking collision resistance [BK04]
- rule out existence of $(\mathsf{T}, \mathcal{R})$
  - $\mathcal{R}$ breaks DBL given PGV adversary:



Sketch: No Free Reducibility from PGV to DBL

- import techniques from [Pie08] on combiner impossibility
- meta reduction combined with generic bounds on attacking collision resistance [BK04]
- rule out existence of $(\mathsf{T}, \mathcal{R})$
  - $\mathcal{R}$ breaks DBL given PGV adversary:



note: restrictions and fees apply

The End

Thank you!

?

References

Paul Baecher and Marc Fischlin.
Random oracle reducibility.
In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 21–38, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Berlin, Germany.

Mihir Bellare and Tadayoshi Kohno.
Hash function balance and its impact on birthday attacks.
In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 401–418, Interlaken, Switzerland, May 2–6, 2004. Springer, Berlin, Germany.

John Black, Phillip Rogaway, Thomas Shrimpton, and Martijn Stam.
An analysis of the blockcipher-based hash functions from PGV.
Journal of Cryptology, 23(4):519–545, October 2010.

Bart Preneel, René Govaerts, and Joos Vandewalle.
Hash functions based on block ciphers: A synthetic approach.
In Douglas R. Stinson, editor, *Advances in Cryptology – CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378, Santa Barbara, CA, USA, August 22–26, 1994. Springer, Berlin, Germany.

Krzysztof Pietrzak.
Compression from collisions, or why CRHF combiners have a long output.
In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 413–432, Santa Barbara, CA, USA, August 17–21, 2008. Springer, Berlin, Germany.