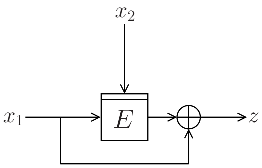
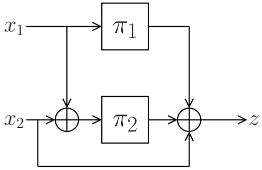
On the Impact of Known-Key Attacks on Hash Functions

Bart Mennink and Bart Preneel
KU Leuven (Belgium)

ASIACRYPT 2015
December 3, 2015

Introduction





- Hash functions classically built from:
  - Blockciphers: Davies-Meyer ('84), PGV ('93), ...
  - Permutations: Sponge ('07), Grøstl ('09), ...

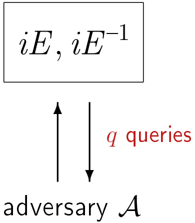
- Security classically in ideal cipher/permutation model

Ideal Cipher Model

- $\mathrm{Bloc}(\kappa, n)$: all blockciphers with κ-bit key and n-bit state
- iE is randomly drawn from $\mathrm{Bloc}(\kappa, n)$

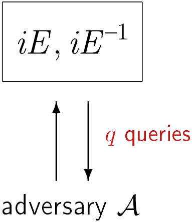
Ideal Cipher Model

- $\mathrm{Bloc}(\kappa, n)$: all blockciphers with κ-bit key and n-bit state
- iE is randomly drawn from $\mathrm{Bloc}(\kappa, n)$
- Adversary $\mathcal{A}$ has query access to iE and iE^{-1}



Ideal Cipher Model

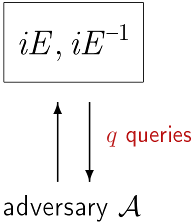
- $\mathrm{Bloc}(\kappa, n)$: all blockciphers with κ-bit key and n-bit state
- iE is randomly drawn from $\mathrm{Bloc}(\kappa, n)$
- Adversary $\mathcal{A}$ has query access to iE and iE^{-1}



- $\mathcal{A}$ tries to find collisions/preimages/... for F^{iE}

Ideal Cipher Model

- $\mathrm{Bloc}(\kappa, n)$: all blockciphers with κ-bit key and n-bit state
- iE is randomly drawn from $\mathrm{Bloc}(\kappa, n)$
- Adversary $\mathcal{A}$ has query access to iE and iE^{-1}



- $\mathcal{A}$ tries to find collisions/preimages/... for F^{iE}

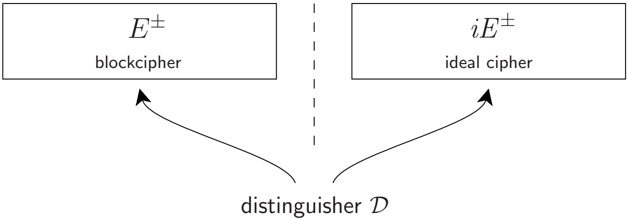
How realistic is this model?

Are Blockciphers Ideal Ciphers?

- Consider any blockcipher E (e.g. AES)
- E should look like an ideal cipher iE

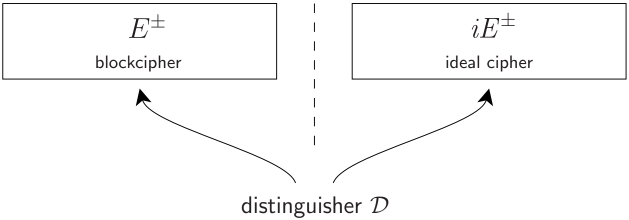
Are Blockciphers Ideal Ciphers?

- Consider any blockcipher E (e.g. AES)
- E should look like an ideal cipher iE



Are Blockciphers Ideal Ciphers?

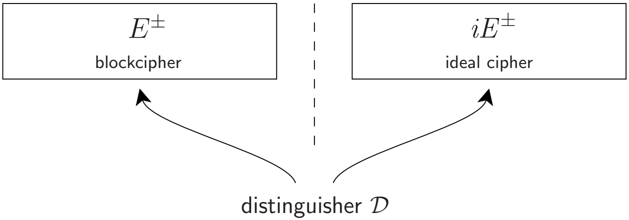
- Consider any blockcipher E (e.g. AES)
- E should look like an ideal cipher iE



- E is not a random system
- In theory, $\mathcal{D}$ always succeeds with probability 1

Are Blockciphers Ideal Ciphers?

- Consider any blockcipher E (e.g. AES)
- E should look like an ideal cipher iE



- E is not a random system
- In theory, $\mathcal{D}$ always succeeds with probability 1
- In practice, not trivial to demonstrate this

$\longrightarrow$ quest for open-key distinguishers

Known-(Related-)Key Distinguishers

- Known-(related-)key attacks distinguish E from iE:
  - $\text{Feistel}_7/\text{AES}_7$ (Knudsen-Rijmen, AC '07)
  - AES_7 (Mendel et al., FSE '09)
  - $\text{Threefish-512}_{35}$ (Aumasson et al., AC '09)
  - AES_8 (Gilbert-Peyrin, FSE '10)
  - Feistel_{11} (Sasaki-Yasuda, FSE '11)
  - BLAKE-32_8 (Biryukov et al., FSE '11)
  - RIPEMD-128_{52} (Sasaki-Wang, ACNS '12)
  - $\text{Threefish-512}_{36}$ (Yu et al., SAC '12)
  - ...

Known-(Related-)Key Distinguishers

Impact of Distinguishers Unclear

Known-(Related-)Key Distinguishers

Impact of Distinguishers Unclear

- "Banana attack" (Aumasson '10)

Known-(Related-)Key Distinguishers

Impact of Distinguishers Unclear

- "Banana attack" (Aumasson '10)
- (Knudsen-Rijmen, AC '07):

"In some cases block ciphers are used with a key that is known to the adversary, (...). Our attacks are quite relevant to this case."

Known-(Related-)Key Distinguishers

Impact of Distinguishers Unclear

- "Banana attack" (Aumasson '10)
- (Knudsen-Rijmen, AC '07):

  "In some cases block ciphers are used with a key that is known to the adversary, (...). Our attacks are quite relevant to this case."

- Attacks on E do not necessarily invalidate security of F^E

Known-(Related-)Key Distinguishers

Impact of Distinguishers Unclear

- “Banana attack” (Aumasson ’10)
- (Knudsen-Rijmen, AC ’07):

> *“In some cases block ciphers are used with a key that is known to the adversary, (...). Our attacks are quite relevant to this case.”*

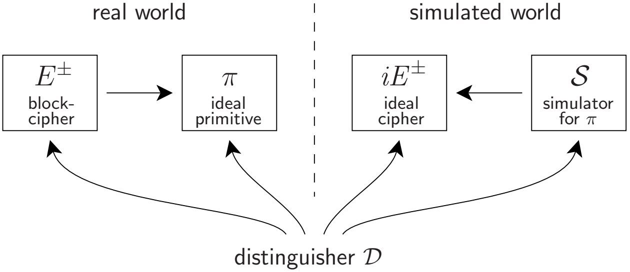
- Attacks on E do not necessarily invalidate security of F^E

Potential Solution

- Indifferentiability of blockciphers

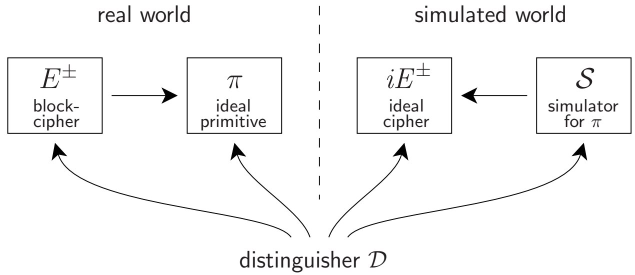
Indifferentiability of Blockciphers

Indifferentiability (Maurer et al. '04)



Indifferentiability of Blockciphers

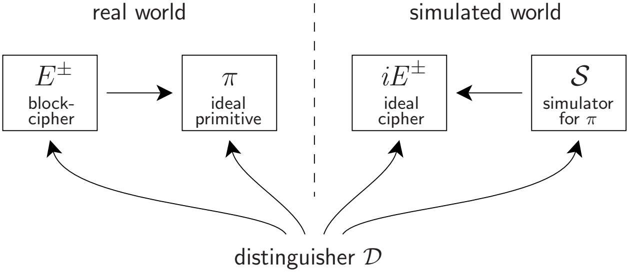
Indifferentiability (Maurer et al. '04)



- E based on π is indifferentiable from iE if for some simulator $\mathcal{S}$, distinguishability advantage is small

Indifferentiability of Blockciphers

Indifferentiability (Maurer et al. '04)

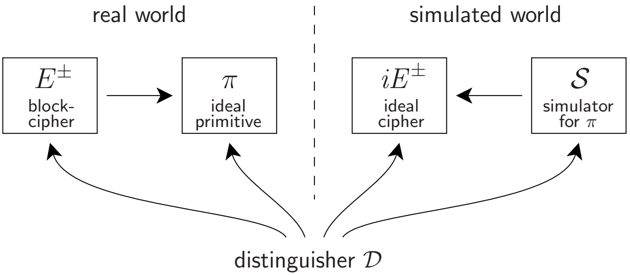


- E based on π is indifferentiable from iE if for some simulator $\mathcal{S}$, distinguishability advantage is small
- Blockcipher behaves like ideal cipher . . .

  . . . and can replace it in certain applications

Indifferentiability of Blockciphers

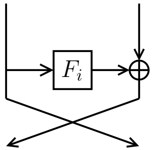
Indifferentiability (Maurer et al. '04)

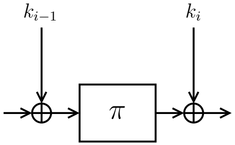


- E based on π is indifferentiable from iE if for some simulator $\mathcal{S}$, distinguishability advantage is small
- Blockcipher behaves like ideal cipher ...

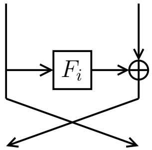
  ... and can replace it in certain applications
- Much (!!) harder to prove

Indifferentiability of Blockciphers

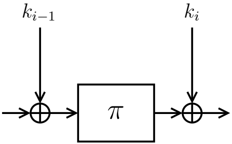




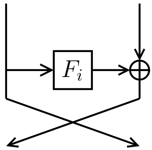
Indifferentiability of Blockciphers



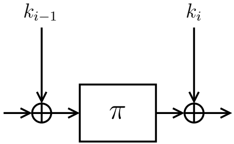
Feistel	bound	remark
Coron et al. '08	$2^{18} q^{8} / 2^n$	6 rnd (flawed)
Holenstein et al. '10	$2^{66} q^{10} / 2^n$	14 rnd
Guo and Lin '15	$2^{222} q^{30} / 2^n$	21 rnd (alter. key)
Dachman-Soled et al. '15	$2^{51} q^{12} / 2^n$	10 rnd
Dai and Steinberger '15	$2^{23} q^{8} / 2^n$	8 rnd



Indifferentiability of Blockciphers

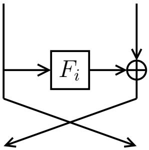


Feistel	bound	remark
Coron et al. '08	$2^{18}q^{8}/2^n$	6 rnd (flawed)
Holenstein et al. '10	$2^{66}q^{10}/2^n$	14 rnd
Guo and Lin '15	$2^{222}q^{30}/2^n$	21 rnd (alter. key)
Dachman-Soled et al. '15	$2^{51}q^{12}/2^n$	10 rnd
Dai and Steinberger '15	$2^{23}q^{8}/2^n$	8 rnd

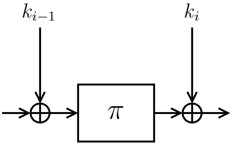


Even-Mansour	bound	remark
Andreeva et al. '13	$2^{34}q^{10}/2^n$	5 rnd (random kdf)
Lampe and Seurin '13	$2^{91}q^{12}/2^n$	12 rnd
Guo and Lin '15	$2^{11}q^{8}/2^n$	15 rnd (alter. key)

Indifferentiability of Blockciphers



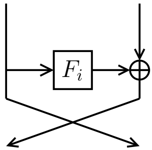
Feistel	bound	remark
Coron et al. '08	$2^{18}q^{8}/2^n$	6 rnd (flawed)
Holenstein et al. '10	$2^{66}q^{10}/2^n$	14 rnd
Guo and Lin '15	$2^{222}q^{30}/2^n$	21 rnd (alter. key)
Dachman-Soled et al. '15	$2^{51}q^{12}/2^n$	10 rnd
Dai and Steinberger '15	$2^{23}q^{8}/2^n$	8 rnd



Even-Mansour	bound	remark
Andreeva et al. '13	$2^{34}q^{10}/2^n$	5 rnd (random kdf)
Lampe and Seurin '13	$2^{91}q^{12}/2^n$	12 rnd
Guo and Lin '15	$2^{11}q^{8}/2^n$	15 rnd (alter. key)

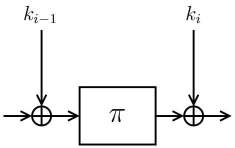
Extremely hard research question!

Indifferentiability of Blockciphers



Feistel	bound	remark
Coron et al. '08	$2^{18}\ q^{8}\ /2^n$	6 rnd (flawed)
Holenstein et al. '10	$2^{66}\ q^{10}/2^n$	14 rnd
Guo and Lin '15	$2^{222}q^{30}/2^n$	21 rnd (alter. key)
Dachman-Soled et al. '15	$2^{51}\ q^{12}/2^n$	10 rnd
Dai and Steinberger '15	$2^{23}\ q^{8}\ /2^n$	8 rnd

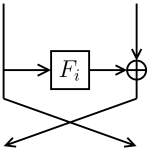
pointless for $n = 128$; security up to $q \lesssim 2$ for $n = 256$



Even-Mansour	bound	remark
Andreeva et al. '13	$2^{34}q^{10}/2^n$	5 rnd (random kdf)
Lampe and Seurin '13	$2^{91}q^{12}/2^n$	12 rnd
Guo and Lin '15	$2^{11}q^{8}\ /2^n$	15 rnd (alter. key)

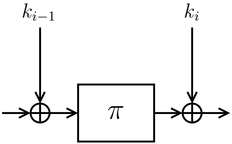
Extremely hard research question!

Indifferentiability of Blockciphers



Feistel	bound	remark
Coron et al. '08	$2^{18}\ q^{8}\ /2^n$	6 rnd (flawed)
Holenstein et al. '10	$2^{66}\ q^{10}/2^n$	14 rnd
Guo and Lin '15	$2^{222}q^{30}/2^n$	21 rnd (alter. key)
Dachman-Soled et al. '15	$2^{51}\ q^{12}/2^n$	10 rnd
Dai and Steinberger '15	$2^{23}\ q^{8}\ /2^n$	8 rnd

pointless for $n = 128$; security up to $q \lesssim 2$ for $n = 256$



Even-Mansour	bound	remark
Andreeva et al. '13	$2^{34}q^{10}/2^n$	5 rnd (random kdf)
Lampe and Seurin '13	$2^{91}q^{12}/2^n$	12 rnd
Guo and Lin '15	$2^{11}q^{8}\ /2^n$	15 rnd (alter. key)

security up to $q \lesssim 8$ for $n = 128$

Extremely hard research question!

Weak Cipher Model

Weak Cipher Model: Idea

Blockciphers behave like ideal ciphers, except for
a particular property that can be exploited

Weak Cipher Model: Idea

Blockciphers behave like ideal ciphers, except for a particular property that can be exploited

- Consider a predicate Φ
- $\mathrm{Bloc}[\Phi](\kappa, n)$: all (κ, n)-blockciphers that comply with Φ

Weak Cipher Model: Idea

Blockciphers behave like ideal ciphers, except for a particular property that can be exploited

- Consider a predicate Φ
- $\text{Bloc}[\Phi](\kappa, n)$: all (κ, n)-blockciphers that comply with Φ
- iE is randomly drawn from $\text{Bloc}[\Phi](\kappa, n)$

Weak Cipher Model: Idea

Blockciphers behave like ideal ciphers, except for a particular property that can be exploited

- Consider a predicate Φ
- $\mathrm{Bloc}[\Phi](\kappa, n)$: all (κ, n)-blockciphers that comply with Φ
- iE is randomly drawn from $\mathrm{Bloc}[\Phi](\kappa, n)$

- Simple examples:

Φ	$\mathrm{Bloc}[\Phi](\kappa, n)$
true	all ciphers $\mathrm{Bloc}(\kappa, n)$
$\exists(k, m, c) : m = c$	all ciphers with a fixed point $m \mapsto m$
$\forall(k, m, c) : m = c$	identity mapping

Weak Cipher Model: Specific Predicate

- Core idea: analyze F in WCM instead of ICM
- Analysis in WCM depends on type of predicate
- Type of predicate depends on type of primitive attack

Weak Cipher Model: Specific Predicate

- Core idea: analyze F in WCM instead of ICM
- Analysis in WCM depends on type of predicate
- Type of predicate depends on type of primitive attack

- We focus on specific type of predicate

Weak Cipher Model: Specific Predicate

- Core idea: analyze F in WCM instead of ICM
- Analysis in WCM depends on type of predicate
- Type of predicate depends on type of primitive attack

- We focus on specific type of predicate

$\Phi = \Phi(A, B, \varphi)$: for each key k there exist A sets of B queries $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that comply with a certain condition φ

Weak Cipher Model: Specific Predicate

- Core idea: analyze F in WCM instead of ICM
- Analysis in WCM depends on type of predicate
- Type of predicate depends on type of primitive attack

- We focus on specific type of predicate

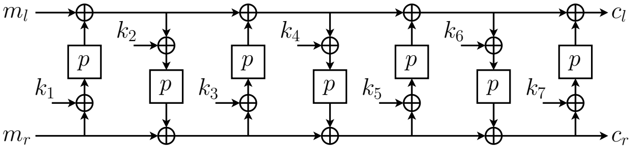
$\Phi = \Phi(A, B, \varphi)$: for each key k there exist A sets of B queries $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that comply with a certain condition φ

- General enough to cover many primitive attacks

Weak Cipher Model: Known-Key Distinguishers

Attack on Feistel$_7$ (Knudsen-Rijmen '07)

- Consider Feistel$_7$ based on $n/2$-bit permutation p

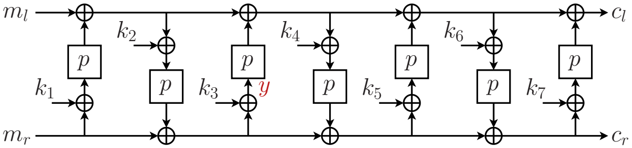


- Consider known key $k = (k_1, \ldots, k_7)$

Weak Cipher Model: Known-Key Distinguishers

Attack on Feistel$_7$ (Knudsen-Rijmen '07)

- Consider Feistel$_7$ based on $n/2$-bit permutation p

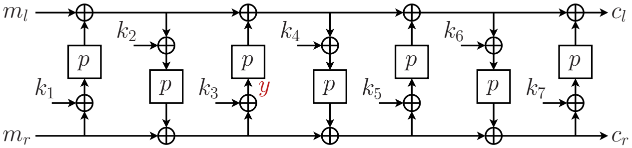


- Consider known key $k = (k_1, \ldots, k_7)$
- Choose $y \in \{0,1\}^{n/2}$

Weak Cipher Model: Known-Key Distinguishers

Attack on Feistel$_7$ (Knudsen-Rijmen '07)

- Consider Feistel$_7$ based on $n/2$-bit permutation p



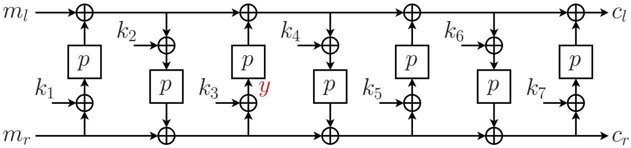
- Consider known key $k = (k_1, \ldots, k_7)$
- Choose $y \in \{0,1\}^{n/2}$
- Derive (m, c) and (m', c') satisfying

$$\text{Right}_{n/2}(m \oplus c \oplus m' \oplus c') = 0$$

Weak Cipher Model: Known-Key Distinguishers

Attack on Feistel$_7$ (Knudsen-Rijmen '07)

- Consider Feistel$_7$ based on $n/2$-bit permutation p



- Consider known key $k = (k_1, \ldots, k_7)$
- Choose $y \in \{0,1\}^{n/2}$
- Derive (m, c) and (m', c') satisfying

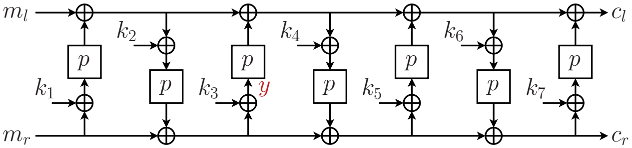
φ

$$\text{Right}_{n/2}(m \oplus c \oplus m' \oplus c') = 0$$

Weak Cipher Model: Known-Key Distinguishers

Attack on Feistel$_7$ (Knudsen-Rijmen '07)

- Consider Feistel$_7$ based on $n/2$-bit permutation p



- Consider known key $k = (k_1, \ldots, k_7)$
- Choose $y \in \{0,1\}^{n/2}$
- Derive (m, c) and (m', c') satisfying

φ

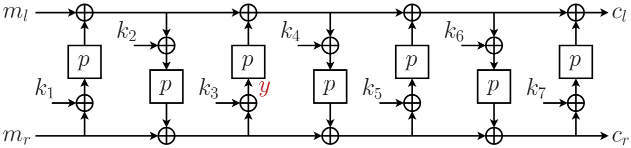
$$\text{Right}_{n/2}(m \oplus c \oplus m' \oplus c') = 0$$

$B = 2$

Weak Cipher Model: Known-Key Distinguishers

Attack on Feistel$_7$ (Knudsen-Rijmen '07)

- Consider Feistel$_7$ based on $n/2$-bit permutation p



- Consider known key $k = (k_1, \ldots, k_7)$
- Choose $y \in \{0,1\}^{n/2}$ $\longleftarrow$ $A = 2^{n/2}$
- Derive (m, c) and (m', c') satisfying

φ

$$\text{Right}_{n/2}(m \oplus c \oplus m' \oplus c') = 0$$

$B = 2$

Weak Cipher Model: Known-Key Distinguishers

Generalization

- For $C \in \{1, \ldots, n\}$, define φ as[1]

$$\mathsf{Right}_C \left(x^1 \oplus z^1 \oplus \cdots \oplus x^B \oplus z^B\right) = 0$$

[1] simplified for sake of presentation

Weak Cipher Model: Known-Key Distinguishers

Generalization

- For $C \in \{1, \dots, n\}$, define φ as[1]

$$\text{Right}_C\left(x^1 \oplus z^1 \oplus \cdots \oplus x^B \oplus z^B\right) = 0$$

- Covers virtually all existing known-key attacks

attack	A	B	C
Feistel$_7$ (Knudsen-Rijmen '07)	$= 2^{n/2}$	2	$n/2$
AES$_8$ (Gilbert-Peyrin '10)	$\lesssim 2^{n/8}$	2	$10n/16$
Threefish-512$_{36}$ (Yu et al. '12)	$\lesssim 2^{n/8}$	4	n
$\vdots$	$\vdots$	$\vdots$	$\vdots$

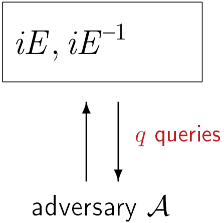
[1] simplified for sake of presentation

Random Weak Cipher

- $\mathrm{Bloc}[\Phi](\kappa, n)$: all (κ, n)-blockciphers that comply with Φ
- iE is randomly drawn from $\mathrm{Bloc}[\Phi](\kappa, n)$

Random Weak Cipher

- $\mathrm{Bloc}[\Phi](\kappa, n)$: all (κ, n)-blockciphers that comply with Φ
- iE is randomly drawn from $\mathrm{Bloc}[\Phi](\kappa, n)$
- Adversary $\mathcal{A}$ has query access to iE and iE^{-1}



Random Weak Cipher

- $\mathrm{Bloc}[\Phi](\kappa, n)$: all (κ, n)-blockciphers that comply with Φ
- iE is randomly drawn from $\mathrm{Bloc}[\Phi](\kappa, n)$
- Adversary $\mathcal{A}$ has query access to iE and iE^{-1}
- It has additional query access to iE^{Φ}
  - Returns tuples $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ satisfying φ

$$\boxed{iE, iE^{-1}, iE^{\Phi}}$$

$\updownarrow$ q queries

adversary $\mathcal{A}$

Random Weak Cipher

iE and iE^{-1} as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \backslash \text{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \backslash \text{dom}(P_k)$

Random Weak Cipher

iE and iE^{-1} as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \setminus \mathrm{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \setminus \mathrm{dom}(P_k)$

iE^{Φ}

- Σ_k: list of potential responses $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that
  - satisfy φ
  - are consistent with P_k

Random Weak Cipher

iE and iE^{-1} as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \backslash \text{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \backslash \text{dom}(P_k)$

iE^{Φ}

- Σ_k: list of potential responses $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that
  - satisfy φ
  - are consistent with P_k
- New query: random response from Σ_k

Random Weak Cipher

iE and iE^{-1} as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \backslash \text{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \backslash \text{dom}(P_k)$

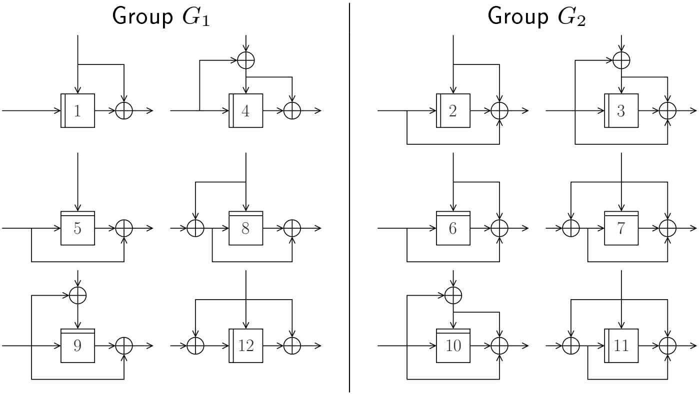
iE^{Φ}

- Σ_k: list of potential responses $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that
  - satisfy φ
  - are consistent with P_k
- New query: random response from Σ_k

Notes

- Behavior of (iE, iE^{-1}) detached from iE^{Φ}
- Works reasonably well as long as $|\Sigma_k| \gg 0$
- Thanks to Damian Vizár for pointing this out

PGV in WCM



PGV (Preneel et al. '93)

- 12 blockcipher-based compression functions
- Optimally secure in ICM (Black et al. '02)
- Attacks beyond ICM are often fixed-key differential attacks

PGV in WCM

B	C	collision	preimage
ideal model		$2^{n/2}$	2^n
1	arbitrary		
2	$\leq n/2$		
	$> n/2$		
≥ 3	arbitrary		

PGV in WCM

B	C	collision	preimage
ideal model		$2^{n/2}$	2^n
1	arbitrary		
2	$\leq n/2$	$2^{n/2}$	2^n
	$> n/2$		
≥ 3	arbitrary	$2^{n/2}$	2^n

- $B \geq 3$ or $(B = 2 \wedge C \leq n/2)$: ICM security bounds retained

PGV in WCM

B	C	collision	preimage
ideal model		$2^{n/2}$	2^n
1	arbitrary		
2	$\leq n/2$	$2^{n/2}$	2^n
	$> n/2$	2^{n-C}	2^n
≥ 3	arbitrary	$2^{n/2}$	2^n

- $B \geq 3$ or $(B = 2 \wedge C \leq n/2)$: ICM security bounds retained
- $(B = 2 \wedge C > n/2)$: any predicate query satisfies
  $x \oplus z \oplus x' \oplus z' = 0$ on $> n/2$ bits

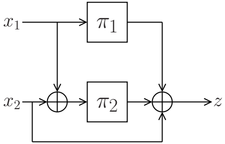
PGV in WCM

B	C	collision	preimage
ideal model		$2^{n/2}$	2^n
1	arbitrary	$2^{(n-C)/2}$	2^{n-C}
2	$\leq n/2$	$2^{n/2}$	2^n
	$> n/2$	2^{n-C}	2^n
≥ 3	arbitrary	$2^{n/2}$	2^n

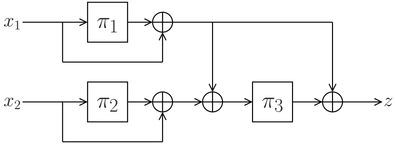
- $B \geq 3$ or $(B = 2 \wedge C \leq n/2)$: ICM security bounds retained
- $(B = 2 \wedge C > n/2)$: any predicate query satisfies $x \oplus z \oplus x' \oplus z' = 0$ on $> n/2$ bits
- $B = 1$: any predicate query satisfies $x \oplus z = 0$ on C bits

Grøstl and Shrimpton-Stam in WCM

Grøstl (Gauravaram et al. '09)



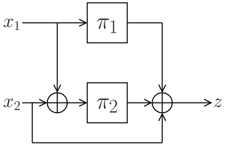
Shrimpton-Stam (Shrimpton-Stam '08)



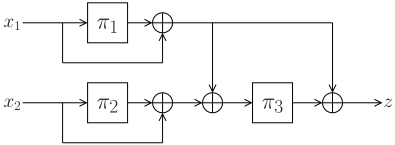
- Blockcipher with a fixed and known key is a permutation and can be used as such
- Understand impact of distinguishers on permutations

Grøstl and Shrimpton-Stam in WCM

Grøstl (Gauravaram et al. '09)



Shrimpton-Stam (Shrimpton-Stam '08)



- Blockcipher with a fixed and known key is a permutation and can be used as such
- Understand impact of distinguishers on permutations
- Similar security observations in ICM versus WCM

Conclusions

Weak Cipher Model

- Model to investigate impact of blockcipher weaknesses
- Application: existing known-key attacks have limited impact on PGV, Grøstl, and Shrimpton-Stam
- Approach generalizes to other functions and attacks

Conclusions

Weak Cipher Model

- Model to investigate impact of blockcipher weaknesses
- Application: existing known-key attacks have limited impact on PGV, Grøstl, and Shrimpton-Stam
- Approach generalizes to other functions and attacks

The Road Ahead

- First step to security beyond ideal model
- Still "controversial"
  - Also an idealized model
  - Simplification in random weak cipher
  - Abstraction of existing attacks
  - Only covers specific attacks

Thank you for your attention!

SUPPORTING SLIDES

Random Abortable Weak Cipher

iE and iE^{-1} as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \backslash \mathrm{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \backslash \mathrm{dom}(P_k)$

iE^{Φ}

- Σ_k: list of potential responses $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that
  - satisfy φ
  - may be inconsistent with P_k

Random Abortable Weak Cipher

$\boldsymbol{iE}$ and $\boldsymbol{iE^{-1}}$ as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \backslash \mathrm{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \backslash \mathrm{dom}(P_k)$

$\boldsymbol{iE^{\Phi}}$

- Σ_k: list of potential responses $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that
    - satisfy φ
    - may be inconsistent with P_k
- New query: random response from Σ_k
- Abort if response creates inconsistency with P_k

Random Abortable Weak Cipher

iE and iE^{-1} as usual

- P_k for all keys k: initially empty lists of iE_k-evaluations
- Query to iE: random response from $\{0,1\}^n \backslash \text{rng}(P_k)$
- Query to iE^{-1}: random response from $\{0,1\}^n \backslash \text{dom}(P_k)$

iE^{Φ}

- Σ_k: list of potential responses $\{(x^1, z^1), \ldots, (x^B, z^B)\}$ that
  - satisfy φ
  - may be inconsistent with P_k
- New query: random response from Σ_k
- Abort if response creates inconsistency with P_k

Notes

- Now: (iE, iE^{-1}) and iE^{Φ} behave somewhat independently
- RAWC aborts with probability $\mathcal{O}\left(\frac{(Bq)^2}{2^n}\right)$

All Results in WCM

		PGV		Grøstl		Shrimpton-Stam	
B	C	collision	preimage	collision	preimage	collision	preimage
ideal model		$2^{n/2}$	2^n	$2^{n/4}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
1	$\leq n/2$	$2^{(n-C)/2}$	2^{n-C}	$2^{(n-C)/4}$	$2^{(n-C)/2}$	$2^{(n-C)/2}$	$2^{n/2}$
	$> n/2$	$2^{(n-C)/2}$	2^{n-C}	$2^{(n-C)/4}$	$2^{(n-C)/2}$	$2^{(n-C)/2}$	2^{n-C}
2	$\leq n/2$	$2^{n/2}$	2^n	$2^{n/4}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
	$> n/2$	2^{n-C}	2^n	$2^{(n-C)/2}$	$2^{n/2}$	2^{n-C}	$2^{n/2}$
≥ 3	arbitrary	$2^{n/2}$	2^n	$2^{n/4}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$

- $B \geq 3$ or $(B = 2 \wedge C \leq n/2)$: ICM security bounds retained
- $(B = 2 \wedge C > n/2)$: any predicate query satisfies
  $x \oplus z \oplus x' \oplus z' = 0$ on $> n/2$ bits
- $B = 1$: any predicate query satisfies $x \oplus z = 0$ on C bits